



Pakiet informacji na rok 2006

Programy dotyczące bezpieczeństwa informacji

w UE:

analiza i wskazówki dla państw członkowskich

Wrzesień 2006 r.

Adnotacja prawna:

Europejskiej Agencji Bezpieczeństwa Sieci i Informacji (ENISA)

Należy zwrócić uwagę, że informacje zawarte w niniejszym Pakiecie informacji zostały zebrane przez pracowników ENISA również na podstawie informacji przedstawionych Agencji przez odpowiednie organizacje państw członkowskich UE lub powszechnie dostępnych. Niniejszy Pakiet informacji nie musi zawierać najnowszych informacji i może być od czasu do czasu aktualizowany.

Ani ENISA, ani żadna osoba działająca w jej imieniu nie jest odpowiedzialna za wykorzystanie informacji zawartych w niniejszej publikacji. ENISA nie ponosi odpowiedzialności za treść zewnętrznych stron internetowych, których adresy zamieszczono w niniejszej publikacji.

Zabronione jest publikowanie jakichkolwiek fragmentów niniejszego Pakietu informacji w jakichkolwiek środkach przekazu bez pisemnej zgody i podania źródła.

© Europejska Agencja Bezpieczeństwa Sieci i Informacji (ENISA), 2006 r.

Wszelkie prawa zastrzeżone

Spis treści

Adnotacja prawna:	3
Spis treści	4
Streszczenie	9
Wstęp	11
Zakres	12
Założenia	14
Docelowi odbiorcy	17
Podsumowanie odpowiedzi	19
Informacje ogólne	23
ENISA	25
Podziękowania	26
Glosariusz	27
Profile grup	29
Użytkownik prywatny	30
MŚP	33
Media	38
ISP (Dostawcy usług internetowych)	40
Władze lokalne	42
Katalog dobrych praktyk	43
Dobre praktyki w poszczególnych krajach	48
1. Austria	48
Bieżąca sytuacja	48
Rząd jako partner przedsiębiorstw i przemysłu	49
Kampanie	52
2. Belgia	53
Kampanie	53
3. Cypr	55
Rząd jako twórca prawnych, regulacyjnych i instytucjonalnych uregulowań służących poszerzaniu wiedzy	55
Kampanie	56
4. Czechy	57
Rząd jako twórca prawnych, regulacyjnych i instytucjonalnych rozwiązań służących poszerzaniu wiedzy	57
Władze państwowe jako użytkownik systemów informacyjnych	58
Władze lokalne jako użytkownik systemów informacyjnych	58
5. Dania	59
Bieżąca sytuacja	59
Rząd jako twórca prawnych, regulacyjnych i instytucjonalnych uregulowań służących poszerzaniu wiedzy	59
Rząd jako partner przedsiębiorstw i przemysłu	62
Rząd jako partner społeczeństwa	62
Kampanie	63
6. Estonia	64
Rząd jako twórca prawnych, regulacyjnych i instytucjonalnych postanowień służących poszerzaniu wiedzy	64

Władze państwowe jako użytkownik systemów informacyjnych.....	67
Władze lokalne jako użytkownik systemów informacyjnych.....	67
Rząd jako partner przedsiębiorstw i przemysłu	67
Rząd jako partner społeczeństwa	69
Statystyki i kluczowe wskaźniki wydajności (KPI).....	69
7. Finlandia.....	70
Rząd jako partner przedsiębiorstw i przemysłu	70
Rząd jako partner społeczeństwa	71
Kampanie	72
8. Francja.....	74
Rząd jako twórca prawnych, regulacyjnych i instytucjonalnych postanowień służących poszerzaniu wiedzy	74
Rząd jako partner społeczeństwa	74
9. Niemcy.....	83
Rząd jako twórca prawnych, regulacyjnych i instytucjonalnych postanowień służących poszerzaniu wiedzy	83
Władze państwowe jako użytkownik systemów informacyjnych.....	88
Władze lokalne jako użytkownik systemów informacyjnych.....	88
Rząd jako partner przedsiębiorstw i przemysłu	88
Rząd jako partner społeczeństwa	92
Statystyki i kluczowe wskaźniki wydajności (KPI).....	93
10. Grecja	95
Bieżąca sytuacja	95
Kampanie	95
11. Węgry.....	97
Obecna sytuacja.....	97
Rząd jako twórca prawnych, regulacyjnych i instytucjonalnych postanowień służących poszerzaniu wiedzy	97
Władze państwowe jako użytkownik systemów informacyjnych.....	98
Władze lokalne jako użytkownik systemów informacyjnych.....	99
Rząd jako partner przedsiębiorstw i przemysłu	99
Rząd jako partner społeczeństwa	101
Statystyki i kluczowe wskaźniki wydajności (KPI).....	102
12. Islandia	104
Kampanie	104
13. Irlandia.....	110
Kampanie	110
14. Włochy.....	110
Rząd jako twórca prawnych, regulacyjnych i instytucjonalnych uregulowań służących poszerzaniu wiedzy	110
Władze państwowe jako użytkownik systemów informacyjnych.....	111
Władze lokalne jako użytkownik systemów informacyjnych.....	111
Rząd jako partner społeczny.....	112
Kampanie	113
15. Łotwa	115
Rząd jako twórca prawnych, regulacyjnych i instytucjonalnych postanowień służących poszerzaniu wiedzy	115

Władze państwowe jako użytkownik systemów informacyjnych.....	116
Władze lokalne jako użytkownik systemów informacyjnych.....	116
Rząd jako partner przedsiębiorstw i przemysłu	117
Rząd jako partner społeczeństwa	117
Statystyki i kluczowe wskaźniki wydajności (KPI).....	117
16. Liechtenstein	119
17. Litwa	120
Rząd jako twórca prawnych, regulacyjnych i instytucjonalnych uregulowań służących poszerzaniu wiedzy	120
Władze krajowe jako użytkownik systemów informacyjnych.....	123
Rząd jako partner przedsiębiorstw i przemysłu	123
Rząd jako partner dla społeczeństwa	125
18. Luksemburg	126
Rząd jako twórca prawnych, regulacyjnych i instytucjonalnych postanowień służących poszerzaniu wiedzy	126
Władze państwowe jako użytkownicy systemów informacyjnych.....	129
Władze lokalne jako użytkownik systemów informacyjnych.....	130
Rząd jako partner przedsiębiorstw i przemysłu	130
Rząd jako partner społeczeństwa	132
Statystyki i i kluczowe wskaźniki wydajności (KPI).....	133
Zdobyte doświadczenie	133
19. Malta	134
Rząd jako twórca prawnych, regulacyjnych i instytucjonalnych postanowień służących poszerzaniu wiedzy	134
Władze państwowe jako użytkownik systemów informacyjnych.....	135
Władze lokalne jako użytkownik systemów informacyjnych.....	135
Rząd jako partner przedsiębiorstw i przemysłu	135
Rząd jako partner społeczeństwa	138
Statystyki i kluczowe wskaźniki wydajności (KPI).....	139
20. Holandia	140
Rząd jako twórca prawnych, regulacyjnych i instytucjonalnych rozwiązań służących poszerzaniu wiedzy	140
Władze państwowe jako użytkownicy systemów informacyjnych.....	142
Władze lokalne jako użytkownicy systemów informacyjnych.....	143
Rząd jako partner przedsiębiorstw i przemysłu	143
Rząd jako partner społeczeństwa	145
21. Norwegia	149
Rząd jako twórca prawnych, regulacyjnych i instytucjonalnych ustaleń służących poszerzaniu wiedzy	149
Rząd jako partner przedsiębiorstw i przemysłu	150
Rząd jako partner społeczeństwa	152
22. Polska	153
Rząd jako twórca prawnych, regulacyjnych i instytucjonalnych regulacji służących poszerzaniu wiedzy	153
Władze państwowe jako użytkownik systemów informacyjnych.....	153
Władze lokalne jako użytkownik systemów informacyjnych.....	155
Rząd jako partner społeczeństwa	156

23. Portugalia	159
Rząd jako twórca prawnych, regulacyjnych i instytucjonalnych uregulowań służących poszerzaniu wiedzy	159
Władze państwowe jako użytkownik systemów informacyjnych	160
Władze lokalne jako użytkownik systemów informacyjnych	160
Rząd jako partner przedsiębiorstw i przemysłu	160
Rząd jako partner społeczeństwa	162
Statystyki i kluczowe wskaźniki wydajności (KPI)	162
24. Słowacja	164
Rząd jako twórca prawnych, regulacyjnych i instytucjonalnych uregulowań służących poszerzaniu wiedzy	164
Władze państwowe jako użytkownik systemów informacyjnych	164
Władze lokalne jako użytkownik systemów informacyjnych	165
Rząd jako partner przedsiębiorstw i przemysłu	165
Rząd jako partner społeczeństwa	166
Statystyki i kluczowe wskaźniki wydajności (KPI)	166
25. Słowenia	167
Obecna sytuacja	167
Rząd jako twórca prawnych, regulacyjnych i instytucjonalnych uregulowań służących poszerzaniu wiedzy	168
Władze państwowe jako użytkownik systemów informacyjnych	173
Władze lokalne jako użytkownik systemów informacyjnych	173
Rząd jako partner przedsiębiorstw i przemysłu	174
Rząd jako partner społeczeństwa	174
Statystyki i kluczowe wskaźniki wydajności (KPI)	176
26. Hiszpania	177
27. Szwecja	178
Obecna sytuacja	178
Rząd jako twórca prawnych, regulacyjnych i instytucjonalnych uregulowań służących poszerzaniu wiedzy	179
Władze państwowe jako użytkownik systemów informacyjnych	181
Władze lokalne jako użytkownik systemów informacyjnych	182
Rząd jako partner przedsiębiorstw i przemysłu	183
Rząd jako partner społeczeństwa	185
Statystyki i kluczowe wskaźniki wydajności (KPI)	190
Zdobyte doświadczenia	191
Inicjatywy w ramach kampanii	194
28. Wielka Brytania	197
Obecna sytuacja	197
Rząd jako twórca prawnych, regulacyjnych i instytucjonalnych uregulowań służących poszerzaniu wiedzy	198
Władze państwowe jako użytkownik systemów informacyjnych	200
Administracja lokalna jako użytkownik systemów informacyjnych	201
Administracja jako partner przedsiębiorstw i przemysłu	202
Rząd jako partner społeczeństwa	208
Statystyki i i kluczowe wskaźniki wydajności (KPI)	208
Kampanie	209

Dobre praktyki w grupach docelowych	213
Użytkownik prywatny	213
MŚP	221
Media	236
ISP	238
Władze lokalne	241
Wytyczne dotyczące dobrych praktyk	247
Zalecenia	247
Listy kontrolne	251
Statystyki / wskaźniki KPI	256
Plan działań	262
Inne materiały	265
Polecane materiały	265
Pliki elektroniczne	266

Streszczenie

Liczba użytkowników technologii informacyjnych i komunikacyjnych (ICT, Information Communication Technology) wciąż rośnie we wszystkich państwach członkowskich. Tak jak miało to miejsce w przeszłości, korzyściom dla przedsiębiorstw i obywateli, wynikającym z postępu w technologiach i coraz większego ich zasięgu, towarzyszyła coraz większa ilość naruszeń bezpieczeństwa informacji. Z tego względu obecna sytuacja wymaga, aby państwa członkowskie kontynuowały promowanie i rozwój „kultury bezpieczeństwa”.

Dzisiaj w dziedzinie technik informacyjnych ciągle powszechne jest porzekadło twierdzące, że o wytrzymałości łańcucha decyduje jego najsłabsze ogniwo. Podczas wdrażania każdego skutecznego i solidnego systemu bezpieczeństwa krytycznym czynnikiem jest wciąż czynnik ludzki. Europejska Agencja Bezpieczeństwa Sieci i Informacji (ENISA) wraz z państwami członkowskimi ponawiają próby wywarcia korzystnego wpływu na stosunek społeczeństwa do bezpieczeństwa informacji, a także zmianę nastawienia czynnika ludzkiego w celu osiągnięcia większej samoświadomości.

Niniejszy Pakiet informacji szczegółowo opisuje inicjatywy mające na celu poszerzanie wiedzy, podejmowane lub trwające w państwach członkowskich. Informacje opracowano na podstawie odpowiedzi poszczególnych państw na kwestionariusz ENISA i uzupełniono przy pomocy rozmów, badań i materiałów dodatkowych. Zakłada się, że zawarte w niniejszym dokumencie szczegółowe informacje mogą zostać wykorzystane do pomocy w rozpowszechnianiu praktycznych informacji o dobrych praktykach; mogą one także zapewnić możliwość śledzenia postępu w sposobach podejścia różnych państw do kwestii dotyczących wiedzy o bezpieczeństwie informacji.

Analiza inicjatyw i akcji państw członkowskich wykazała kilka tendencji i cech wspólnych w działaniach przeprowadzonych do tej pory:

- Ogólna liczba inicjatyw w UE mających na celu poszerzanie wiedzy nieco wzrosła w ciągu ubiegłego roku
- Dwie trzecie przeprowadzonych programów poszerzających wiedzę miało miejsce w północnej Europie
- Tak jak w przeszłości, różnica w charakterze i liczbie inicjatyw poszerzających wiedzę spowodowana jest różnymi poziomami rozumienia i kultury bezpieczeństwa informacji w poszczególnych państwach
- Prawie każdy program państw członkowskich był skierowany do MŚP i użytkowników prywatnych
- Rozwija się współpraca z dostawcami usług internetowych w zakresie poszerzania wiedzy
- Tak jak w przeszłości, głównymi zagadnieniami są phishing, spam i ochrona przy pomocy zapory sieciowej – w ubiegłym roku prawie wszystkie inicjatywy poszerzające wiedzę włączyły do swoich tematów kradzież tożsamości

- Tematy dotyczące poszerzania wiedzy mają coraz większy zakres i obejmują wykorzystywanie urządzeń mobilnych i technologii WiFi
- Strony internetowe i szkolenia w dalszym ciągu są najczęściej wykorzystywanymi formami przekazywania informacji w ramach podnoszenia poziomu wiedzy
- Media nadal są traktowane jako kanał przekazywania informacji, a nie grupa docelowa. Potwierdzają to odpowiedzi państw członkowskich, szczegółowo omówione w Pakiecie informacji

Po przeanalizowaniu najskuteczniejszych programów, które zrealizowano i oparto na metodologii dobrych praktyk ENISA, możliwe jest określenie kilku kluczowych warunków wstępnych i działań, koniecznych dla osiągnięcia skuteczności inicjatywy poszerzającej wiedzę:

- Przekazywana wiadomość musi być interesująca i postrzegana jako „wartościowa” dla grupy docelowej – konieczna jest właściwa ocena odbiorców wraz z określeniem ich celów, potrzeb i wiedzy
- Kanały przekazywania informacji powinny zostać przeanalizowane w celu ustalenia optymalnego mechanizmu przekazywania, a następnie wykorzystania go – należy zbadać i zastosować kanały przekazywania informacji preferowane przez dane grupy docelowe
- Należy wykorzystać partnerstwo publiczno-prywatne dla zwiększenia współdziałania, co pomoże zapewnić inicjatywie zasoby i wiedzę potrzebne do przekazania właściwej wiadomości właściwym odbiorcom przy pomocy najskuteczniejszych kanałów
- Należy wykorzystywać jednostki rozpowszechniające wiedzę, np. nauczycieli i media, w celu zwiększenia możliwości i zakresu każdej inicjatywy poszerzającej wiedzę
- Do pomiaru skuteczności inicjatywy należy stosować statystyki i kluczowe wskaźniki wydajności (ang. *Key Performance Indicators*, KPI) – doświadczenia zdobyte poprzez analizę danych ilościowych i jakościowych mogą być wykorzystane do ulepszenia przyszłych kampanii

Wstęp

Żyjemy i pracujemy w wieku informacji, który wciąż daje wiele możliwości przedsiębiorstwom i obywatelom. Jednakże dalszy rozwój technologii informacyjnych i komunikacyjnych (ang. *Information Communication Technologies*, ICT) i ich stosowanie przez użytkowników w dalszym ciągu wiąże się z podatnością na zagrożenia. Przedsiębiorstwa i obywatele wciąż są narażeni na zagrożenia takie jak naruszenia bezpieczeństwa informacji. Analitycy nadal informują, że w dziedzinie bezpieczeństwa informacji czynnik ludzki jest najsłabszym ogniwem, co oznacza, że w dalszym ciągu konieczne są zmiany w podejściu użytkowników lub w kulturze organizacyjnej.

W ramach Programu prac ENISA na rok 2005 stworzono Information Package: „Raising Awareness in Information Security – Insight and Guidance for Member States” [Pakiet informacji: poszerzanie wiedzy na temat bezpieczeństwa informacji – analiza i wskazówki dla państw członkowskich].¹ Ten dokument, jak również program na płycie CD, opracowano w celu analizowania skutecznych praktyk przyjętych przez państwa członkowskie UE i aby zwrócić uwagę na już rozpoczęte działania w dziedzinie poszerzania wiedzy. Aby w dalszym ciągu ułatwiać poszerzanie wiedzy i promowanie dobrych praktyk, a także pomagać w tym zakresie, w tym roku Agencja ponownie pracowała nad Pakietem informacji z roku 2005, mając na celu szczegółowy opis obecnych tendencji i postępów państw członkowskich.

¹ Pełen tekst „Information Package: Raising Awareness in Information Security – Insight and Guidance for Members States” [Pakiet informacji: poszerzanie wiedzy na temat bezpieczeństwa informacji – analiza i wskazówki dla państw członkowskich] znajduje się pod adresem: http://www.enisa.europa.eu/pages/05_01.htm

Zakres

Pod koniec 2005 r. ENISA i OECD badały, w jaki sposób mogłyby współpracować w dziedzinie bezpieczeństwa informacji, ze szczególnym uwzględnieniem poszerzania wiedzy w tym zakresie.

Analiza skuteczności środków poszerzających wiedzę zwróciła uwagę na konieczność przyjęcia bardziej strategicznego podejścia. Skuteczniejszą strategią byłoby przekazanie wyników kampanii i ogólnych informacji o poszerzaniu wiedzy tylko jednej organizacji. Dlatego też Agencja i OECD dostrzegły potrzebę współpracy i unikania powielania się działań. Celem tego podejścia jest poprawa efektywności gromadzenia informacji dotyczących inicjatyw poszerzających wiedzę, co ma na celu zapewnienie skuteczności przewidywanych osiągnięć.

Na tej podstawie ENISA opracowała kwestionariusz skupiający się na kwestiach dotyczących poszerzania wiedzy, które nie zostały zbadane szczegółowo ani w Pakiecie Informacji ENISA z 2006 r., ani w kwestionariuszu „OECD questionnaire on practical initiative to promote a culture of security” [Kwestionariusz OECD dotyczący praktycznych inicjatyw promujących kulturę bezpieczeństwa]. Obejmowało to zebranie szczegółowych informacji o dwóch dodatkowych grupach docelowych: dostawcach usług internetowych (ISP) i władzach lokalnych. Kwestionariusz (przesłany państwom członkowskim i Stałej Grupie Przedstawicieli Branżowych (Permanent Stakeholders Group, PSG)²) miał na celu uzyskanie istotnych informacji w sposób odpowiadający respondentowi. Kwestionariusz ten skupiony był głównie na sektorze publicznym, ale przewidywał też odpowiedzi sektora prywatnego. Pytania i struktura w stylu narracji umożliwiały respondentom kontrolowanie formatu i rozmiaru odpowiedzi bez zbędnych ograniczeń. Chociaż głównym celem kwestionariusza było zgromadzenie materiałów na temat dobrych praktyk, przyjęte podejście umożliwiało respondentom przedstawienie swojego sposobu postrzegania inicjatyw dotyczących poszerzania wiedzy.

Zebrane informacje uzupełniono za pomocą rozmów, badań i materiałów dodatkowych.

Celem Pakietu informacji na rok 2006 jest, więc przedstawienie ogólnych zarysów programów UE dotyczących poszerzania wiedzy. Przegląd ten składa się przede wszystkim z tekstów dostarczonych przez państwa członkowskie lub inne organizacje. Agencja opracowała również zalecenia w zakresie dobrych praktyk, udziela ona także porad w kwestii kierowania kampaniami poszerzania wiedzy. Zalicza się do tego informacje o statystykach i kluczowych wskaźnikach wydajności (KPI).

² Stała Grupa Przedstawicieli Branżowych została utworzona 28 lutego 2005 r. przez Dyrektora Zarządzającego ENISA. W jej skład wchodzi eksperci reprezentujący odpowiednie osoby zainteresowane, na przykład przedsiębiorstwa zajmujące się technologiami informacyjnymi i komunikacyjnymi, stowarzyszenia konsumentów i specjalistów naukowych w dziedzinie bezpieczeństwa sieci i informacji. Stała Grupa Przedstawicieli Branżowych doradza Dyrektorowi Zarządzającemu w wykonywaniu obowiązków wynikających z tego rozporządzenia, sporządzaniu projektów dotyczących programu prac ENISA i zapewnianiu kontaktu z odpowiednimi osobami zainteresowanymi we wszystkich kwestiach związanych z programem prac.

Aby przedstawić całościowy rozwój inicjatyw poszerzania wiedzy, sporządzono także mapę.

Niniejszy Pakiet informacji nie powinien być postrzegany jako wyczerpujące źródło informacji na temat wszystkich realizowanych inicjatyw poszerzających wiedzę w dziedzinie bezpieczeństwa informacji. Zakres Pakietu informacji zależy od stopnia szczegółowości informacji przekazanych przez państwa członkowskie, organizacje i organy. Pakiet ten nie stanowi także wytycznych, co do rodzajów bądź treści wiadomości, które powinny być wykorzystane jako część każdej inicjatywy poszerzającej wiedzę, nie zawiera on również technicznych wytycznych dotyczących standardów lub rozwiązań w dziedzinie bezpieczeństwa informacji.

Założenia

Pakiet informacji ENISA na rok 2006 ma na celu:

- Szczegółowy opis postępu w krajowych podejściach do poszerzania wiedzy i pomoc w śledzeniu tego postępu
- Dostarczenie spisu dobrych praktyk z państw członkowskich i innych organizacji
- Dostarczenie ogólnych zaleceń na temat dobrych praktyk w dziedzinie poszerzania wiedzy
- Dostarczenie materiałów o dobrych praktykach, które można zmodyfikować i przedstawić państwom członkowskim w celu ułatwienia im pracy nad poszerzaniem wiedzy
- Udzielenie porad w zakresie kierowania skutecznymi kampaniami poszerzania wiedzy, a także stosowania statystyk i kluczowych wskaźników wydajności do śledzenia wyników inicjatyw
- Przedstawienie przykładu sposobu prowadzenia kampanii poszerzania wiedzy
- Wsparcie rozwoju kultury bezpieczeństwa informacji w państwach członkowskich

Aby osiągnąć te cele, a także łatwo rozpowszechniać informacje, przyjęto poniższą strukturę:

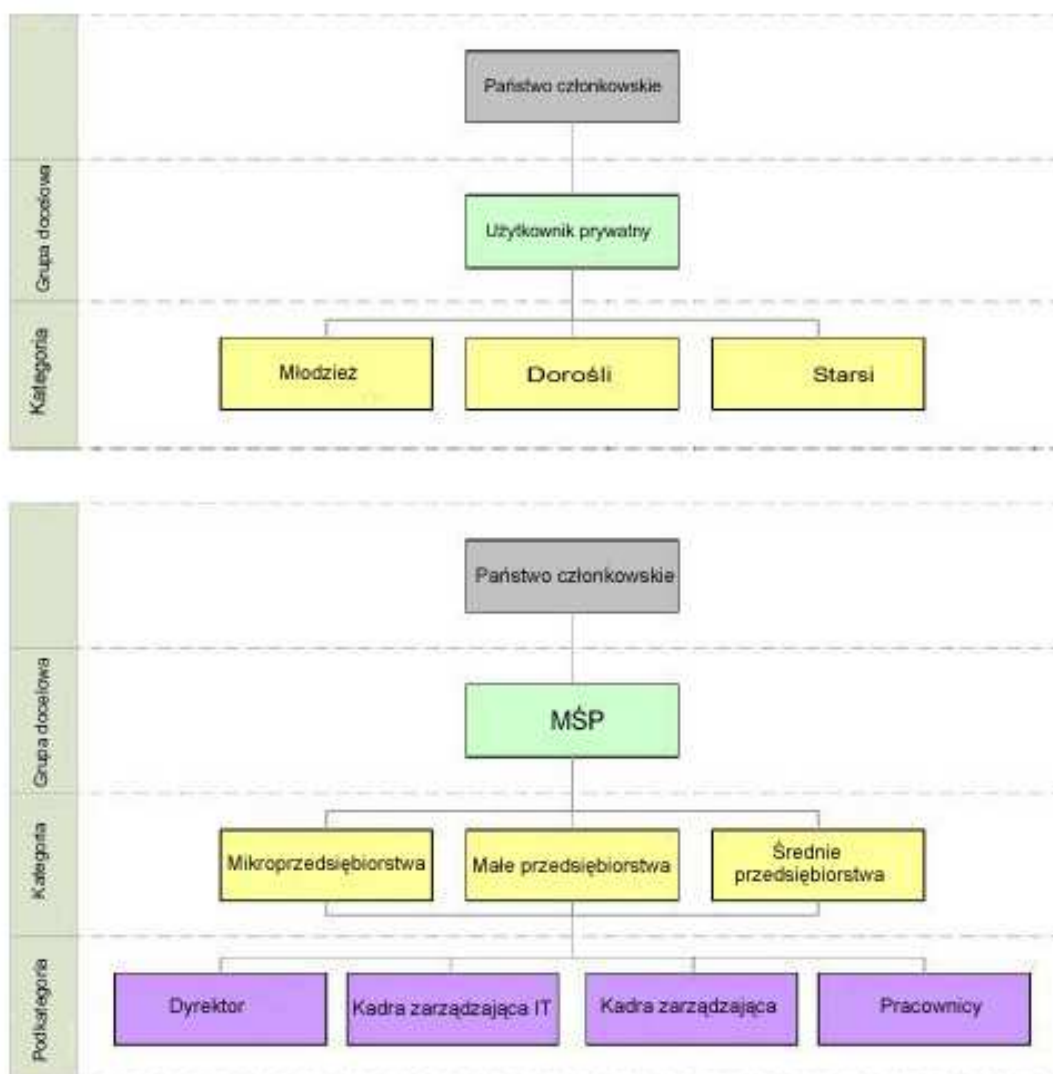
Część	Główny punkt	Wytyczne / Uwagi
Wstęp	Zakres	- Szczegółowe informacje o zakresie Pakietu informacji
	Założenia	- Szczegółowe informacje o założeniach Pakietu informacji
	Docelowi odbiorcy	- Szczegółowe informacje o docelowych odbiorcach
	Podsumowanie odpowiedzi	- Szczegółowe informacje o liczbie respondentów kwestionariusza
	Informacje ogólne	- Ogólne dane i spostrzeżenia w dziedzinie bezpieczeństwa informacji
	ENISA	- Informacje o organizacji ENISA
	Glosariusz	- Terminy i definicje stosowane w Pakiecie informacji
Profile grup	Użytkownik prywatny	- Profil grupy docelowej „użytkownik prywatny”
	MŚP	- Profil grupy docelowej „MŚP”
	Media	- Profil grupy docelowej „media”
	ISP	- Profil grupy docelowej „ISP”
	Władze lokalne	- Profil grupy docelowej „władze lokalne”
Katalog dobrych praktyk	Katalog dobrych praktyk	- Matryca państw członkowskich ze wskazaniem rodzaju informacji udzielonej w odpowiedzi na kwestionariusz

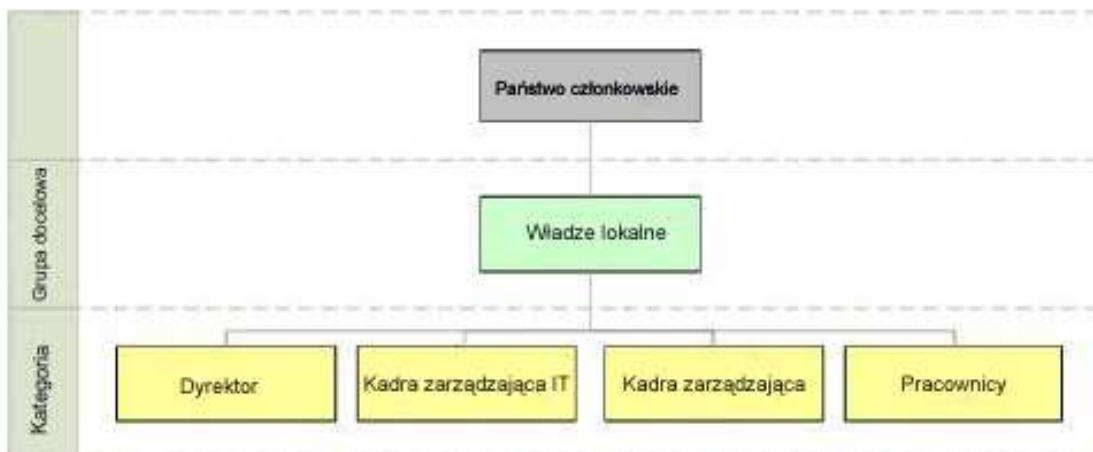
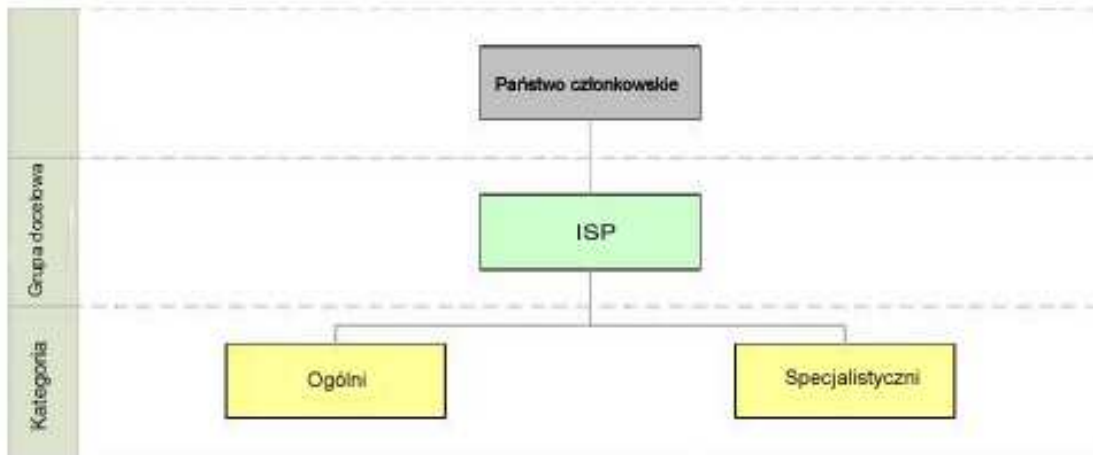
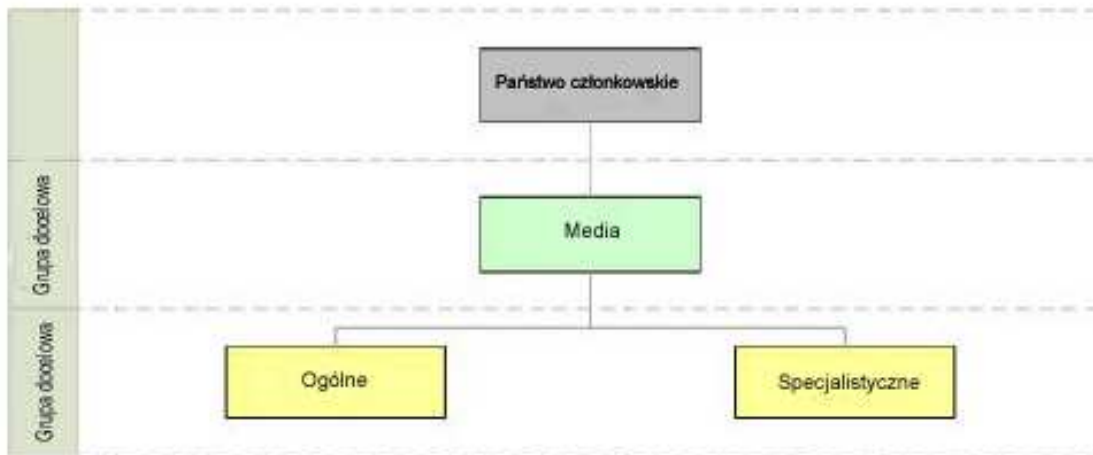
			<ul style="list-style-type: none"> - Zawiera wszystkie podane adresy URL dotyczące poszerzania wiedzy
Dobre praktyki w poszczególnych krajach	Państwo (państwo członkowskie)	Obecna sytuacja	<ul style="list-style-type: none"> - Informacje o obecnych warunkach / stanie sytuacji (jeżeli dostarczono informacje)
		Rząd jako twórca	<ul style="list-style-type: none"> - Informacje o krajowych strategiach poszerzania wiedzy (jeżeli dostarczono informacje do pytania) - Zawiera poczynione/planowane ustalenia prawne, regulacyjne i instytucjonalne
		Władze państwowe jako użytkownik	<ul style="list-style-type: none"> - Informacje o poszerzających wiedzę inicjatywach dla użytkowników systemów władz państwowych (jeżeli dostarczono informacje do pytania)
		Władze lokalne jako użytkownik	<ul style="list-style-type: none"> - Informacje o poszerzających wiedzę inicjatywach dla użytkowników systemów władz lokalnych (jeżeli dostarczono informacje do pytania)
		Rząd jako partner (przedsiębiorstw)	<ul style="list-style-type: none"> - Informacje o inicjatywach poszerzania wiedzy, skierowanych do MŚP, ISP i mediów lub inicjatywach partnerstwa publiczno-prywatnego (jeżeli dostarczono informacje do pytania)
		Rząd jako partner (społeczeństwa)	<ul style="list-style-type: none"> - Informacje o inicjatywach poszerzania wiedzy, skierowanych do społeczeństwa lub inicjatywach partnerstwa publiczno-prywatnego (jeżeli dostarczono informacje do pytania)
		Statystyki / wskaźniki KPI	<ul style="list-style-type: none"> - Informacje o stosowaniu statystyk / wskaźników KPI w inicjatywach poszerzania wiedzy (jeżeli dostarczono informacje do pytania)
		Zdobyte doświadczenia	<ul style="list-style-type: none"> - Informacje o wszelkich doświadczeniach zdobytych w ramach wprowadzania inicjatyw poszerzania wiedzy (jeżeli dostarczono informacje)
		Kampanie	<ul style="list-style-type: none"> - Ogólne informacje o inicjatywach poszerzania wiedzy (jeżeli dostarczono informacje wykraczające poza strukturę i format kwestionariusza)
Dobre praktyki w grupach docelowych	Grupa docelowa	Obecna sytuacja	<ul style="list-style-type: none"> - Ogólne informacje o obecnym stanie grupy docelowej (jeżeli informacje są dostępne)
		Dobre praktyki w poszczególnych krajach	<ul style="list-style-type: none"> - Krótkie podsumowanie inicjatyw poszerzania wiedzy przeprowadzanych w różnych państwach członkowskich - Odnosić do poszczególnych punktów w części <i>Dobre praktyki w poszczególnych krajach</i>
		Dobre praktyki innych organizacji	<ul style="list-style-type: none"> - Informacje o inicjatywach poszerzania wiedzy opisanych przez Stałą Grupę Przedstawicieli Branżowych i inne

			organizacje, które udzieliły odpowiedzi na kwestionariusz lub dostarczyły informacje
Wytyczne dotyczące dobrych praktyk	Zalecenia ENISA		- Zalecenia Agencji oparte na doświadczeniu i analizie informacji przekazanych przez państwa
	Lista kontrolna / wskazówki		- Główne kroki bądź działania wymagane w przypadku każdej inicjatywy poszerzającej wiedzę
	Statystyki kampanii / wskaźniki KPI		- Szczegółowe informacje o statystykach i kluczowych wskaźnikach wydajności, które mogą być stosowane w kampaniach
	Plan działań		- Przykład całościowego rozwoju w dziedzinie inicjatyw poszerzających wiedzę

Docelowi odbiorcy

Pakiet informacji na rok 2006 skierowany jest w szczególności do państw członkowskich w celu wykorzystania go przy realizacji kampanii poszerzania wiedzy. W Pakiecie skoncentrowano się na pięciu grupach docelowych: użytkownik prywatny, małe i średnie przedsiębiorstwa (MŚP), media, dostawca usług internetowych (ISP) i władze lokalne. Opis każdej grupy znajduje się w części *Profile grup*. Te pięć grup można przedstawić graficznie w następujący sposób:





Ponieważ najistotniejszym elementem każdej skutecznej kampanii jest zagwarantowanie dostosowania używanego kanału przekazywania informacji i danej wiadomości do potrzeb, celów i wiedzy odbiorców, niniejszy Pakiet informacji będzie skupiał się na tych pięciu wybranych grupach.

Podsumowanie odpowiedzi

Kwestionariusz użyty w Pakiecie informacji na rok 2006 został przesłany do:

- 28 państw członkowskich: 25 członków UE i 3 członków EOG
- Stałej Grupy Przedstawicieli Branżowych (PSG) ENISA
- Organizacji z sektora prywatnego i różnych innych organów

Diagram poniżej pokazuje, które części kwestionariusza wymagały wypełnienia przez państwa członkowskie lub Stałą Grupę Przedstawicieli Branżowych:

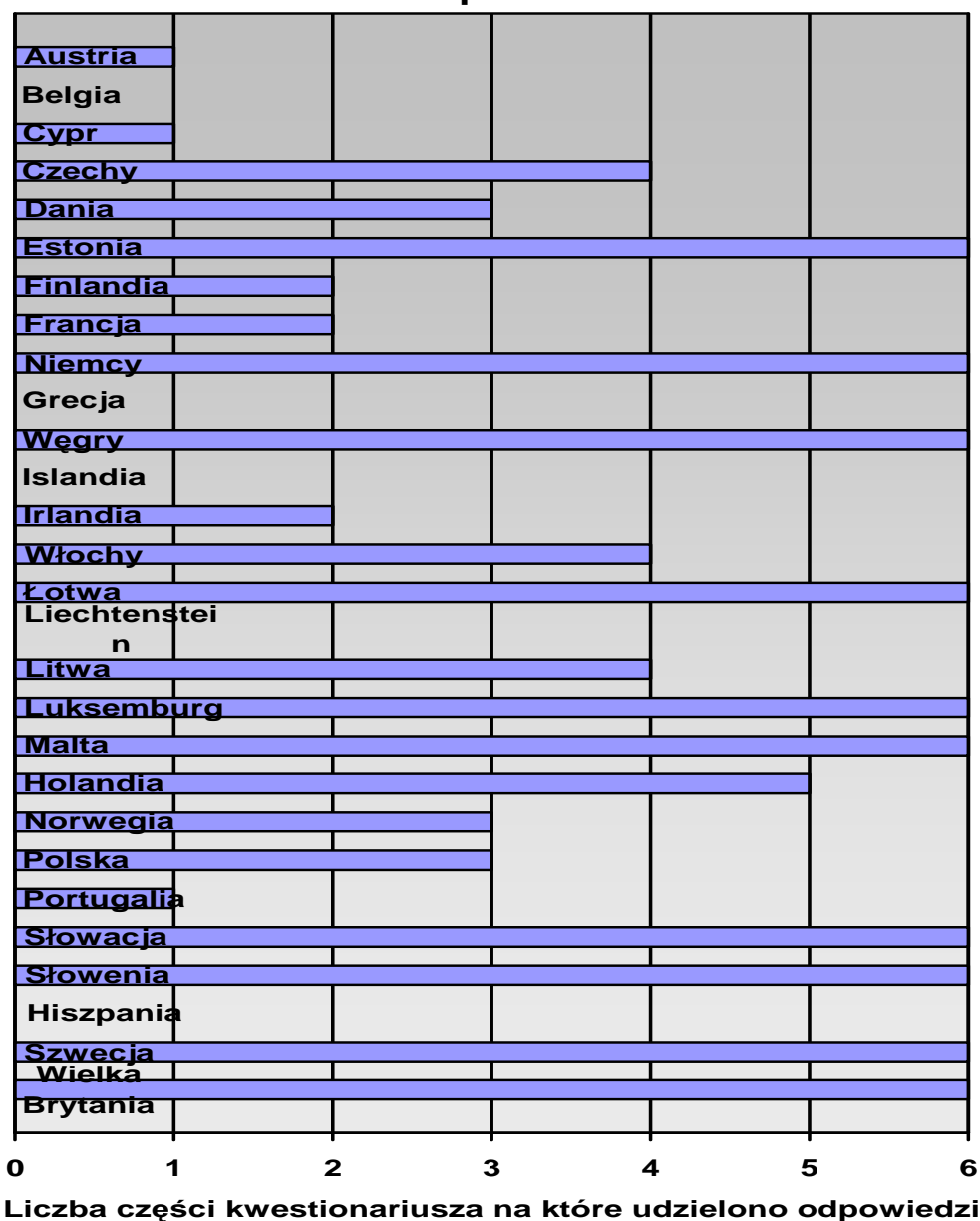
Część	Temat	Odpowiedzi	
		Państwa członkowskie	Stala Grupa Przedstawicieli Branżowych
Część 1	Rząd jako twórca rozwiązań ustawowych, regulacyjnych i instytucjonalnych uregulowań służących poszerzaniu wiedzy	✓	
Część 2	Rząd jako użytkownik systemów informacyjnych	✓	
Część 3	Władze lokalne jako użytkownik systemów informacyjnych	✓	
Część 4	Rząd jako partner przedsiębiorstw i przemysłu	✓	✓
Część 5	Rząd jako partner społeczeństwa	✓	✓
Część 6	Statystyki i kluczowe wskaźniki wydajności (KPI)	✓	✓

Poniższa tabela wskazuje, które państwa członkowskie udzieliły odpowiedzi na pytania zawarte w częściach kwestionariusza ENISA, a które przesłały informacje dodatkowe bądź uzupełniające:

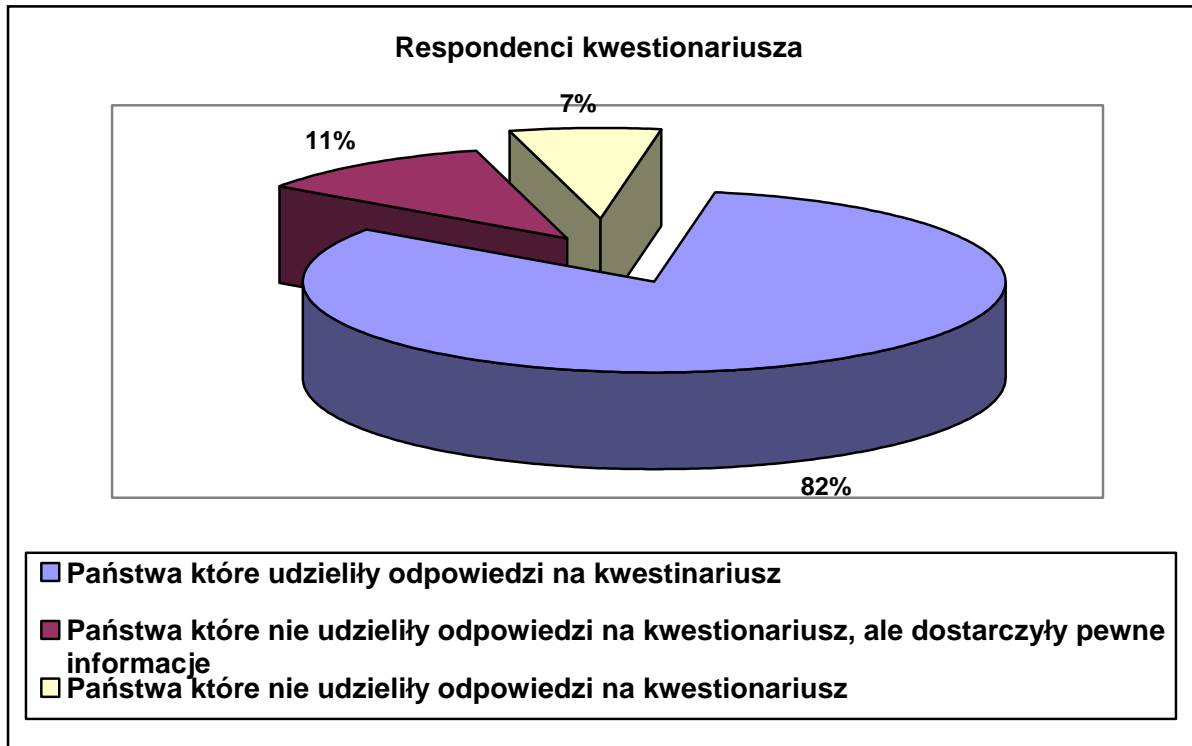
Państwo	Odpowiedzi na pytania kwestionariusza	Liczba części, na które udzielono odpowiedzi	Nie udzielono odpowiedzi na pytania kwestionariusza, ale dostarczono dodatkowe informacje i materiały
Austria	Tak	1	-
Belgia	Nie	0	Tak
Cypr	Tak	1	-
Czechy	Tak	4	-
Dania	Tak	3	-
Estonia	Tak	6	-
Finlandia	Tak	2	-
Francja	Tak	2	-
Niemcy	Tak	6	-
Grecja	Nie	0	Tak
Węgry	Tak	6	-
Irlandia	Tak	2	-
Włochy	Tak	4	-
Łotwa	Tak	6	-
Litwa	Tak	4	-
Luksemburg	Tak	6	-
Malta	Tak	6	-
Holandia	Tak	5	-
Polska	Tak	3	-
Portugalia	Tak	1	-
Słowacja	Tak	6	-
Słowenia	Tak	6	-
Hiszpania	Nie	0	Nie
Szwecja	Tak	6	-
Wielka Brytania	Tak	6	-
Norwegia	Tak	3	-
Islandia	Nie	0	Tak
Liechtenstein	Nie	0	Nie

Poniższa tabela przedstawia rozkład liczby części kwestionariusza, na które państwa członkowskie udzieliły odpowiedzi:

Analiza respondentów



Poniższy wykres przedstawia ogólne podsumowanie odpowiedzi państw członkowskich:



Informacje ogólne

Bezpieczeństwo informacji można zdefiniować jako ochronę informacji przed różnymi zagrożeniami w celu zapewnienia możliwości wykonania działań osobistych lub służbowych.

Zagrożenia dla bezpieczeństwa informacji lub naruszenia tego bezpieczeństwa mogą być rozmaite. Zalicza się do nich:

- Fizyczną kradzież technologii ICT zawierających informacje szczególnie chronione lub ważne
- Złośliwe kody wprowadzane do komputera
- Awarie sprzętu komputerowego lub oprogramowania
- Nieupoważnione uzyskanie dostępu lub niewłaściwe użytkowanie
- Zakłócenia sieciowe
- Fałszowanie tożsamości

Naruszenia te mogą objawiać się na rozmaite sposoby, na przykład jako:

- Utrata danych spowodowana złośliwym oprogramowaniem lub kradzieżą
- Kiepska wydajność spowodowana złośliwym kodem, awariami sprzętu lub oprogramowania
- Niezamówione wiadomości elektroniczne (spam) spowodowane niewłaściwym użytkowaniem
- Koszty finansowe spowodowane utratą funduszy na skutek fałszerstwa tożsamości, wykorzystania inżynierii społecznej lub przestojami systemów z powodu zakłóceń sieciowych

W raporcie firmy McAfee pt. "The threats within" [Zagrożenia wewnętrzne]³ zwraca się uwagę na to, że spośród 1500 specjalistów w 6 miastach europejskich:

- Niemal jedna czwarta wszystkich europejskich specjalistów używa służbowego laptopa do korzystania z Internetu w domu, pomimo tego, że 61% ma bardzo ograniczoną wiedzę o bezpieczeństwie IT
- Ponad połowa europejskich specjalistów posiada urządzenia lub przyrządy, które podłącza do komputera/sieci w miejscu pracy; z czego jedna czwarta robi tak codziennie
- 62% twierdzi, że nie ma pojęcia o bezpieczeństwie IT lub posiada w tej dziedzinie bardzo ograniczoną wiedzę

Według badań Information Security Breaches Survey na rok 2006, zleconych przez Ministerstwo Handlu i Przemysłu Wielkiej Brytanii, powszechnie uważa się, że znaczna większość naruszeń bezpieczeństwa spowodowana jest raczej błędem człowieka niż wadami technologicznymi. Zakładając, że większość incydentów dotyczących

³ Zob. [the threats english.pdf](#)

bezpieczeństwa informacji spowodowana jest błędem człowieka, ważne jest zrozumienie możliwych przyczyn tych błędów, ponieważ może to poprawić sytuację w tej dziedzinie. Biorąc pod uwagę informacje zgromadzone w badaniach, niektóre z przyczyn popełnianych błędów wiążą się z tym, że:

- Użytkownicy ICT są słabo wyszkoleni i na ogół mają małą wiedzę o bezpieczeństwie
- Ludzie wiedzą o niektórych kwestiach dotyczących bezpieczeństwa informacji, ale jako użytkownicy ICT podejmują błędne decyzje
- Istnieją ludzie złośliwi z natury i próbują umyślnie narazić firmę na niebezpieczeństwo.
- Ludzie nie są odpowiednio motywowani do wykonywania działań koniecznych dla zapewnienia bezpieczeństwa

Wytyczne OECD w zakresie bezpieczeństwa systemów i sieci informacyjnych (Guidelines for the Security of Information Systems and Networks) stwierdzają, że: „Świadomość ryzyka i dostępnych zabezpieczeń to pierwsza linia obrony bezpieczeństwa systemów i sieci informacyjnych.” Wytyczne podkreślają również, że obywatele muszą znać „... dobre praktyki, które mogą zastosować w celu zwiększenia bezpieczeństwa”. Organizacje powinny wdrażać odpowiednie programy, aby rozwinąć odpowiedni poziom świadomości i wiedzy, konieczne jest także zapewnienie regularnej analizy i aktualizacji przekazywanych wiadomości.

Dlatego też właściwe informowanie i przygotowanie ludzi ma decydujące znaczenie. Najskuteczniejszym sposobem przekazywania informacji masowemu odbiorcy są kampanie poszerzające wiedzę, a skuteczność takich kampanii w dużym stopniu zależy od wykorzystanych strategii.

ENISA

Europejska Agencja Bezpieczeństwa Sieci i Informacji (ENISA) jest agencją Unii Europejskiej stworzoną w celu usprawnienia funkcjonowania Rynku Wewnętrznego.

ENISA jest ośrodkiem doskonalenia dla państw członkowskich i instytucji unijnych w zakresie bezpieczeństwa sieci i informacji, ponadto udziela porad, wydaje zalecenia i służy jako centrum wymiany informacji na temat dobrych praktyk. Agencja ułatwia także kontakty między instytucjami unijnymi, państwami członkowskimi i uczestnikami sektora prywatnego i przemysłu.

Dane kontaktowe:

Kontakt z ENISA bądź uzyskanie ogólnych informacji na temat programów poszerzających wiedzę w państwach członkowskich możliwe są przez:

e-mail: Isabella Santa - awareness@enisa.europa.eu

Internet: <http://www.enisa.europa.eu/>

Podziękowania

Do niniejszej pracy na różne sposoby przyczyniło się wiele osób i organizacji, bezpośrednio lub pośrednio. Dane w niniejszym Pakiecie zawierają (z kilkoma wyjątkami) informacje przekazane przez państwa członkowskie, organy i organizacje.

Autorzy pragną podziękować za wysiłek OECD, a w szczególności pani Anne Carblanc i panu Laurentowi Bernatowi, których początkowa pomoc i współpraca wpłynęły na niektóre najważniejsze aspekty tego projektu, a także państwom członkowskim i Stałej Grupie Przedstawicieli Branżowych z ENISA, którzy dostarczyli cenne dane i materiały do opracowania Pakietu informacji.

Ponadto autorzy pragną podziękować za pomoc w przygotowaniu niniejszego dokumentu następującym organizacjom: CASPUR (Consortio Interuniversitario per le Applicazioni di Supercalcolato Per Università e Ricerca), miastu Sztokholm, FOURTH, Reuters, Krajowej Agencji ds. Poczty i Telekomunikacji w Szwecji, SAP, SAFT, Swiss Re, Uniwersytetowi 'La Sapienza' w Rzymie, VigiTrust. Wyjątkowe podziękowania należą się panu Jeremy'emu Hiltonowi za jego badania i cenne sugestie.

Na koniec pragniemy podziękować osobom, które przyczyniły się do powstania tego dokumentu poprzez nieformalne rozmowy, cenne spostrzeżenia, obserwacje, sugestie i rozwiązania. Chociaż niniejsza praca niewątpliwie nie stanowi kompletnej listy, zawartość jej byłaby niepełna i niepoprawna bez ich pomocy.

Glosariusz

W poniższej tabeli szczegółowo zdefiniowano terminy techniczne stosowane w niniejszym Pakiecie informacji. Definicje innych terminów oraz więcej szczegółowych informacji można znaleźć na stronie internetowej ENISA: http://www.enisa.europa.eu/pages/05_03.htm

Termin	Definicja
Adware	Program wyświetlający płatne reklamy, często instalowany bez wiedzy użytkownika na skutek takich czynności jak odwiedzanie stron internetowych lub pobieranie oprogramowania
Oprogramowanie antywirusowe	Oprogramowanie stosowane w celu ochrony komputera przed wirusami i innymi zagrożeniami ze strony złośliwego oprogramowania. Oprogramowanie to musi być regularnie aktualizowane i może być także używane w celach bezpieczeństwa, np. do filtrowania zawartości lub stron internetowych.
Botnet ("komputery zombie")	Sieć zainfekowanych komputerów, które mogą być zdalnie sterowane przez hakera. Połączone "komputery zombie" można wykorzystać do rozsyłania spamu lub przeprowadzenia ataków typu DoS (Denial of Service – odmowa usługi)
CERT	Zespół reagujący na naruszenia bezpieczeństwa w Internecie (Computer Emergency Response Team) – centrum koordynacji lub grupa, której zadaniem jest reagowanie na wszelkie nagłe incydenty związane z bezpieczeństwem komputerów i sieci i opanowywanie ich
Denial of Service (odmowa usługi)	Rodzaj ataku polegający na zalaniu sieci przedsiębiorstwa fałszywymi danymi w celu zablokowania strony internetowej/portalu
Zapora sieciowa (firewall)	Sprzęt komputerowy lub oprogramowanie mające na celu powstrzymanie nieupoważnionych osób przed uzyskaniem bez zezwolenia dostępu do komputera za pośrednictwem Internetu
Haker	Osoba, która bezprawnie uzyskuje dostęp do informacji zawartych w systemie komputerowym i potencjalnie w nie ingeruje
Kradzież (fałszerstwo) tożsamości	Kradzież danych osobowych i nielegalne ich wykorzystanie
System wykrywania włamań (Intrusion Detection System)	Oprogramowanie mające na celu monitorowanie przypadków nieupoważnionego uzyskania dostępu do komputera przez Internet i ostrzeganie użytkowników przed takim niebezpieczeństwem
ISP	Internet Service Provider – dostawca usług internetowych. Przedsiębiorstwo oferujące usługi internetowe
Złośliwe oprogramowanie	Złośliwe oprogramowanie (ang. <i>malware</i>) zawierające w swoim kodzie wirusy, robaki i konie trojańskie
Patch (łatka, poprawka)	Aktualizacja programu takiego jak oprogramowanie antywirusowe lub systemu operacyjnego np. Windows. Patche mogą być pobierane ręcznie lub automatycznie, w zależności od preferencji

	użytkownika
Pharming	Rodzaj ataku polegającego na fałszowaniu (spoofingu) nazwy domeny, co powoduje, że użytkownicy sądzą, że znajdują się na autentycznej stronie z właściwym adresem URL, a w rzeczywistości są przekierowani na stronę fałszywą
Phishing	Oszukanie użytkownika mające na celu pozyskanie informacji osobowych, np. szczegółowych danych o rachunku bankowym, poprzez udawanie rzeczywistego przedsiębiorstwa lub organizacji
SMS	Short Message Service - usługa przesyłania krótkich wiadomości tekstowych. Głównie wykorzystywana jako forma komunikacji tekstowej w telefonii komórkowej
Inżynieria społeczna	Rodzaj manipulacji polegający na tym, że dana osoba robi coś, czego mogłaby nie zrobić w innym przypadku
Spam	Niezamówione wiadomości elektroniczne, których odbiorca zazwyczaj nie chce otrzymywać. Spam może być nieszkodliwy lub stanowić formę złośliwego oprogramowania
Spyware	Program śledzący działania użytkownika w Internecie i wysyłający informacje na ten temat innej osobie
Koń trojański (trojan)	Program, który wydaje się być użyteczny, a w rzeczywistości w jakiś sposób szkodzi. Celem konia trojańskiego jest oszukanie użytkownika poprzez ukrycie szkodliwej działalności
Wirus	Program, który przyłącza się do innego programu lub pliku, aby rozprzestrzeniać się i powielać bez wiedzy użytkownika
Robak	Program, który samodzielnie powiela się w systemach komputerowych

Profile grup

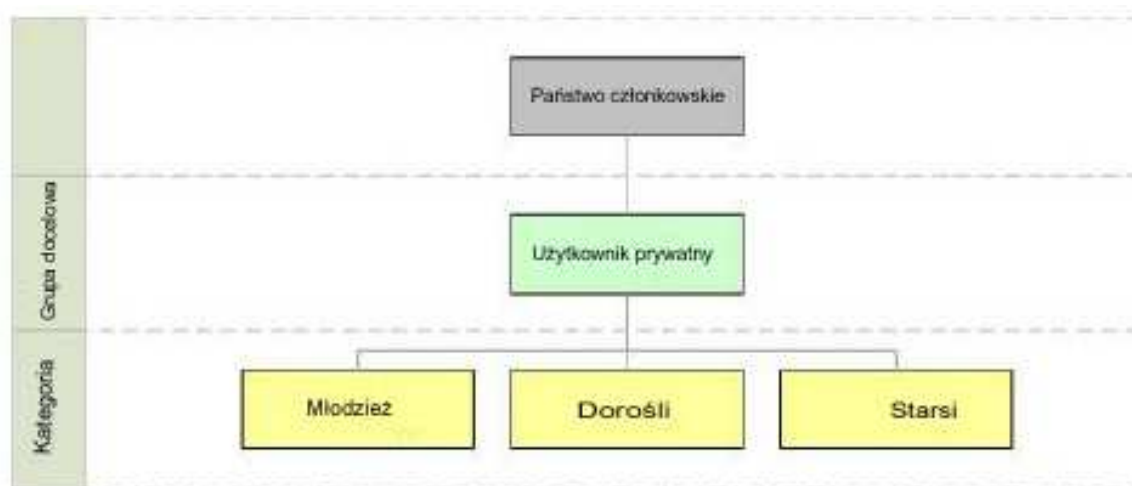
Przed przejściem do szczegółowego opisu profili pięciu grup docelowych, na których skupia się niniejszy Pakiet informacji, warto zapoznać się z niektórymi kluczowymi terminami, stosowanymi przy opisie tych grup:

Termin	Definicja
Grupa docelowa	Konkretni odbiorcy, do których skierowany jest dany program. Są to: użytkownicy prywatni, MŚP, media, ISP i władze lokalne
Kategoria	Klasyfikacja lub rodzaj grupy docelowej. Na przykład „dorośli” stanowią rodzaj „użytkowników prywatnych”
Podkategoria	Klasyfikacja lub rodzaj grupy docelowej, jeżeli możliwy jest dalszy podział kategorii. Na przykład „pracownik” należy do kategorii „małych przedsiębiorstw” w „MŚP”
Cele/potrzeby	Główne działania, do których grupa docelowa wykorzystuje technologie ICT. Przykładem może być osoba dorosła wykorzystująca Internet do bankowości internetowej
Wiedza	Poziom zdolności technicznych grupy docelowej. Może on być oceniony jako „żaden”, „niski”, „średni” lub „wysoki”
Kanał	Forma (lub środek) przekazywania informacji, używana do dostarczania wiadomości stanowiących część inicjatywy poszerzania wiedzy. Przykładem może być broszura

Na podstawie tych terminów możliwe jest określenie profili wszystkich pięciu grup docelowych:

Użytkownik prywatny

Grupę tę stanowią obywatele w różnym wieku i o różnych umiejętnościach technicznych, wykorzystujący ICT (technologie informacyjne i komunikacyjne) na potrzeby prywatne poza miejscem pracy. Tę grupę użytkowników można podzielić na trzy kategorie:



Młodzież

Są to obywatele w wieku zazwyczaj 7-15 lat, którzy dorośli w otoczeniu ICT, a poziom ich wiedzy podyktowany jest w znacznym stopniu stopniem rozwoju infrastruktury w każdym z państw członkowskich. Są oni niezwykle godni zaufania ze względu na ich młody wiek, mają ogromny potencjał przyswajania wiedzy i często eksperymentują z technologiami.

Główne zagadnienia

- Młodzież nie rozumie istniejących zagrożeń dla bezpieczeństwa informacji lub w najlepszym przypadku ma o nich mgliste pojęcie. Dlatego młodzież jest słabym ogniwem, które mogą wykorzystać hakerzy i oszuści
- Ponieważ w Internecie nie ma wyraźnych ustaleń (lub są one niezbyt jasne) w odniesieniu do np. granic prawnych, trzeba uczyć młodzież, „co jest dobre, a co złe”, podobnie jak ma to miejsce w rzeczywistości
- W kwestiach związanych z bezpieczeństwem w Internecie młodzież nie uczy się od rodziców
- Zazwyczaj młodzież jest jednocześnie ufna i dociekliwa

Cele / potrzeby

- Gry
- Rozmowy na czatach
- Surfowanie po Internecie w poszukiwaniu interesujących informacji
- Pobieranie plików muzycznych
- Telefony komórkowe
- Praca domowa

Dorośli

Są to obywatele urodzeni po latach 50-tych XX w., powyżej 16 roku życia – grupa, która częściowo dorastała w otoczeniu technologii ITC. Zakres umiejętności i znajomości ICT wśród tych użytkowników jest prawdopodobnie najbardziej zróżnicowany w porównaniu z innymi grupami, jako że sięga od całkowitej niewiedzy do ogromnego zasobu umiejętności. Obywatele ci mogą mieć lub nie mieć dzieci i pracować w różnorodnych zawodach.

Główne zagadnienia

- Choć niektórzy dorośli posiadają wystarczającą wiedzę w zakresie pewnych bardziej powszechnych typów zagrożeń dla bezpieczeństwa informacji, nie są oni świadomi stosunkowo nowych zagrożeń. Kwestie związane z bezpieczeństwem i prywatnością mają także wpływ na np. technologie wymiany danych, takie jak Bluetooth. Ludzie wciąż nie zdają sobie sprawy, że za pomocą technologii Bluetooth ktoś może uzyskać dostęp do ich książki adresowej lub wykonywać połączenia poprzez łączenie się z ich palmtopem lub telefonem komórkowym.
- Dorośli nie przeprowadzają internetowych transakcji finansowych (np. bankowych), ponieważ sądzą, że nie jest to bezpieczne
- Dorośli obawiają się lub nie rozumieją wszystkich terminów i definicji używanych w kampaniach i niepokoją się, że nie mają czasu na zrozumienie skomplikowanej wiadomości

Cele / potrzeby

- Zakupy przez Internet
- Pobieranie plików muzycznych i oprogramowania
- Płatności internetowe – zakupy, rachunki za telefon, transakcje itp.
- Oglądanie rozrywki w Internecie
- Surfowanie po stronach z informacjami – wiadomości, hobby itp.

Starsi użytkownicy

Są to obywatele urodzeni w latach 50-tych XX w. lub wcześniej, którzy nie dorastali w otoczeniu ICT. Ich poziom umiejętności jest niski lub żaden i, chociaż zazwyczaj nie orientują się w zagadnieniach technicznych, dość swobodnie korzystają z usług

(na przykład e-usług z telefonów komórkowych). Jako że nie dorastali w otoczeniu ICT, mogą mieć większe wątpliwości albo wręcz być nieufni wobec nowych technologii.

Główne zagadnienia

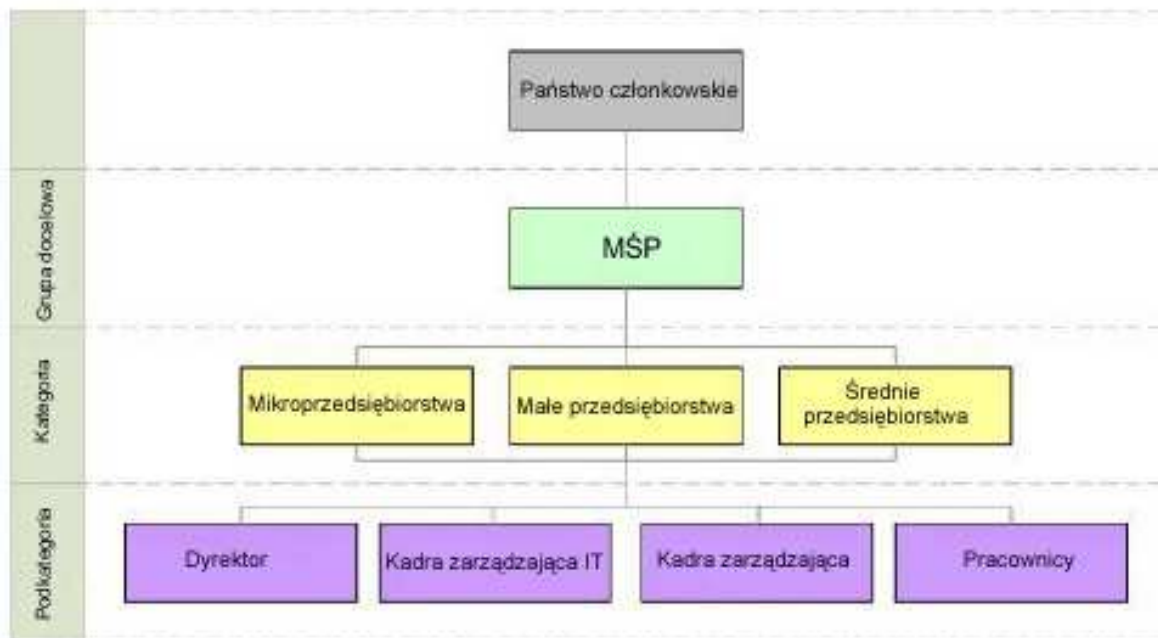
- Starsi użytkownicy muszą być informowani o zagrożeniach ekonomicznych i ich skutkach, a także o rozwiązaniach w zakresie bezpieczeństwa informacji, ponieważ nie dorastali oni w otoczeniu ITC
- Przeciętny starszy użytkownik jest ufny, chociaż ta kategoria użytkowników bardziej obawia się zagrożeń dla bezpieczeństwa

Cele / potrzeby

- Dostęp do komunikacji lub usług internetowych, np. opieki zdrowotnej
- Kontaktowanie się z rodziną – pozostawanie w kontakcie z najbliższymi dzięki poczcie elektronicznej itp.

MŚP

Grupa ta obejmuje zarówno pracodawców, jak i pracowników z mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw (firm). Za średnie przedsiębiorstwa Komisja Europejska uznaje firmy zatrudniające najwyżej 250 pracowników, za małe przedsiębiorstwa – najwyżej 50 pracowników, zaś za mikroprzedsiębiorstwa – najwyżej 10 pracowników⁴. Klasyfikacja rodzajów przedsiębiorstw w zależności od wielkości może być różna w poszczególnych państwach członkowskich. Ta grupa docelowa ma ogromne znaczenie, jako że stanowi 99% całkowitej liczby przedsiębiorstw w UE i zapewnia 65 mln miejsc pracy. Tę grupę użytkowników można podzielić na trzy kategorie, z których każda ma cztery podkategorie:



Mikroprzedsiębiorstwa – zatrudniające mniej niż 10 osób przedsiębiorstwa, których roczny obrót i/lub roczny bilans nie przekracza 2 mln euro. Ta grupa obywateli zazwyczaj nie posiada własnych specjalistów ds. IT czy bezpieczeństwa. W konkretnych państwach członkowskich wartości liczbowe mogą się różnić – na przykład w Wielkiej Brytanii mikroprzedsiębiorstwo składa się zazwyczaj z najwyżej 5 osób.

Małe przedsiębiorstwa – zatrudniające mniej niż 50 osób przedsiębiorstwa, których roczny obrót i/lub roczny bilans nie przekracza 10 mln euro. Państwa członkowskie stosują różne definicje małych przedsiębiorstw czy firm. Małe przedsiębiorstwo może mieć własnego specjalistę ds. IT, ale raczej nie ma specjalisty ds. bezpieczeństwa.

⁴ Rekomendacja 2003/361/WE, Dz.U. L 124 z dn. 20.05.2003 r., str. 36. Więcej informacji na temat definicji MŚP można znaleźć pod adresem: http://ec.europa.eu/enterprise/enterprise_policy/sme_definition/index_en.htm

Średnie przedsiębiorstwa – zatrudniające mniej niż 250 osób przedsiębiorstwa, których roczny obrót nie przekracza 50 mln euro i/lub roczny bilans nie przekracza 43 mln euro. Państwa członkowskie stosują różne definicje średnich przedsiębiorstw czy firm. Średnie przedsiębiorstwa mają zazwyczaj własnego specjalistę ds. IT i mogą mieć pracownika posiadającego wiedzę na temat bezpieczeństwa.

Kategoria przedsiębiorstwa	Liczba pracowników	Obrót	lub	Całkowity bilans
średnie	< 250	≤ 50 mln euro		≤ 43 mln euro
małe	< 50	≤ 10 mln euro		≤ 10 mln euro
mikroprzedsiębiorstwa	< 10	≤ 2 mln euro		≤ 2 mln euro

W każdej z trzech kategorii grupy docelowej można wyróżnić cztery podkategorie użytkowników:

Dyrektor / Właściciel

Osoba podejmująca kluczowe decyzje w zakresie inwestycji w bezpieczeństwo.

Główne zagadnienia

- Dyrektorzy lub właściciele firm często nie zdają sobie sprawy z możliwego wpływu poważnego naruszenia bezpieczeństwa informacji na ich firmy. Kilka przykładów rodzajów zagrożeń dla bezpieczeństwa, które mogą dotyczyć przedsiębiorstwa to:
 - Wirusy i szkodliwe oprogramowanie
 - Nadużycie systemów informacyjnych przez personel
 - Awarie systemu
 - Naruszenie integralności danych
 - Bezprawny dostęp przez osoby z zewnątrz, w tym konkurentów i hakerów
 - Atak DoS (*Denial of Service*)
 - Niezadowoleni pracownicy
 - Fałszerstwo, kradzież i oszustwo⁵
- Zarządzanie bezpieczeństwem informacji nie jest postrzegane jako coś, co pasuje do ogólnego zarządzania, zarządzania ryzykiem i inicjatyw zapewniania zgodności, ale raczej jako dodatkowy koszt finansowy i obciążenie. Powinno być ono postrzegane jak coś, co może pomóc zapobiec takim problemom jak zakłócenie działalności, wpływ na reputację czy wpływ na zaufanie klienta i dostawcy do firmy lub je zminimalizować.

⁵ DTI Information Security Breaches Survey 2004

- Duża liczba firm nie ma planów ciągłości działania (BCP) lub firmy, które je mają nie testują ich regularnie
- Bezpieczeństwo informacji nie jest postrzegane jako czynnik ułatwiający prowadzenie firmy, a raczej jako utrudniający działalność

Cele / potrzeby

- System bezpieczeństwa, który jest mocny i minimalizuje zakłócenia w firmie
- Wykorzystywanie Internetu i innych ICT w celu wspierania funkcji i działalności firmy
- Wykorzystywanie ICT jako wsparcia interesów zawodowych, w tym narzędzia analityczne, kwestie odpowiedzialności i działania organizacyjne
- Codzienne interesy i potrzeby są podobne do tych, które mają dorośli użytkownicy prywatni

Kadra zarządzająca IT

Grupa pracowników technicznych, którzy nie muszą być specjalistami w zakresie bezpieczeństwa, ale muszą rozumieć i wdrażać protokoły bezpieczeństwa informacji.

Główne zagadnienia

- Kierownicy lub personel IT mogą wpaść w pułapkę pomagania w projektowaniu i wdrażaniu systemu bezpieczeństwa w dużym stopniu opartych na sprzęcie i oprogramowaniu IT, ale mogą pominąć dwie rzeczy: potrzebę silnego zestawu strategii i procedur oraz potrzebę lepszego podejścia ludzi do kwestii bezpieczeństwa
- Ta grupa docelowa jest generalnie z natury techniczna, jednak określone komunikaty mogą zostać pominięte, ponieważ są postrzegane jako nietechniczne lub nieodpowiednie lub zbyt techniczne i skierowane do większych organizacji
- Firmy często nie mają systemu bezpieczeństwa lub, jeżeli go mają, nie jest on stale monitorowany czy aktualizowany. Niektóre firmy nie mają żadnego systemu zarządzania bezpieczeństwem informacji (ISMS)
- Krajowe i międzynarodowe standardy, takie jak ISO 17799 i inne uznane standardy, takie jak COBIT nie są wdrażane lub, jeżeli są, niektóre działania nadzorcze, takie jak poszerzanie wiedzy lub podział zadań i obowiązków nie są skutecznie komunikowane. Nadzór nad wprowadzaniem ulepszeń w zakresie monitorowania i zapobiegania także nie są wdrażane w wystarczającym stopniu.⁶

⁶ Achieving Best Practice in your Business - Information Security: BS 7799 and the Data Protection Act, DTI, 2004, http://www.dti.gov.uk/industries/information_security

Część grupy docelowej musi stosować metodologię zapobiegania, wykrywania, reagowania i uzdrawiania w ramach zarządzania ryzykiem bezpieczeństwa systemu, ale stosuje w tym celu nieodpowiednie kontrole.⁷

Cele / potrzeby

- Systemy bezpieczeństwa, które są mocne i minimalizują zakłócenia w firmie
- Wykorzystywanie Internetu i innych ICT w celu wspierania funkcji i działalności firmy
- Wykorzystywanie ICT jako wsparcia interesów zawodowych, w tym narzędzia analityczne, działania organizacyjne i podręcznik wspierające
- Codzienne interesy i potrzeby są podobne do tych, które mają dorośli użytkownicy prywatni

Kadra zarządzająca

Pracownicy często niezorientowani w kwestiach technicznych, którzy jednakże muszą być tak wyszkoleni, by rozumieli wagę bezpieczeństwa informacji. Umożliwi im to wdrożenie właściwych strategii bezpieczeństwa i kontroli w obszarach ich działań.

Główne zagadnienia

- Zarządzający często nie zdają sobie sprawy z konsekwencji naruszenia bezpieczeństwa informacji. Oprócz problemów związanych z danym zdarzeniem, inne konsekwencje (w zależności od rodzaju i powagi zdarzenia) mogą być następujące⁸:
 - Utrata ważnych informacji i brak możliwości funkcjonowania
 - Brak profesjonalizmu w oczach klienta
 - Utrata poufnych informacji o klientach
 - Utrata lub zniszczenie zaufania i relacji z personelem, klientami i dostawcami
 - Zniszczenie marki postrzeganej jako niepewna
 - Koszt związany z czasem poświęconym na uzdrawianie, naprawę szkód i zarządzanie
 - Koszt postępowania dyscyplinarnego
 - Zmniejszona skuteczność

⁷ The Management of Security Risks in Information (paper), Philippe Boozier, Thales Security Systems, 2004.

⁸ Achieving Best Practice in your Business - Information Security: Hard Facts, DTI, 2004, http://www.dti.gov.uk/industries/information_security

- Zarządzający często nie wspierają aktywnie i nie wdrażają polityki i procedur bezpieczeństwa w ich własnych obszarach
- W niektórych przypadkach wiedza personelu o jego obowiązkach oraz ogólnie kwestie bezpieczeństwa nie są skutecznie komunikowane
- Ochrona bezpieczeństwa informacji nie jest postrzegana jako szereg bieżących działań, ale jako coś, co może być wdrożone jednorazowo
- Kadra zarządzająca może spotkać się z podobnymi kwestiami jak te wymienione w poprzednim wyszczególnieniu Kadra zarządzająca IT

Cele / potrzeby

- Wykorzystywanie Internetu i innych ICT w celu wspierania funkcji i działalności firmy oraz zadań o charakterze administracyjnym
- Zapewnienie, że informacja wykorzystująca ICT jest poufna i prywatna
- Codzienne interesy i potrzeby są podobne do tych, które mają dorośli użytkownicy prywatni i inni użytkownicy MŚP

Pracownicy

Największa liczba użytkowników w grupie docelowej i prawdopodobnie najistotniejsza, jako że, jak sugerują badania, większość naruszeń bezpieczeństwa informacji wywołana jest błędem popełnionym przez człowieka.

Główne zagadnienia

- W większości przypadków pracownicy chcą zachować się zgodnie z zasadami bezpieczeństwa informacji, ale często nie wiedzą jak to zrobić
- Użytkownicy powinni stosować jasną i udokumentowaną politykę bezpieczeństwa informacji oraz procedury wspierające, jednak w wielu przypadkach nie mają jasności obrazu.
- Brakuje odpowiedniej wiedzy na temat tego, dlaczego należy czuwać nad bezpieczeństwem oraz świadomości pracowników dotyczącej konieczności podejmowania środków bezpieczeństwa

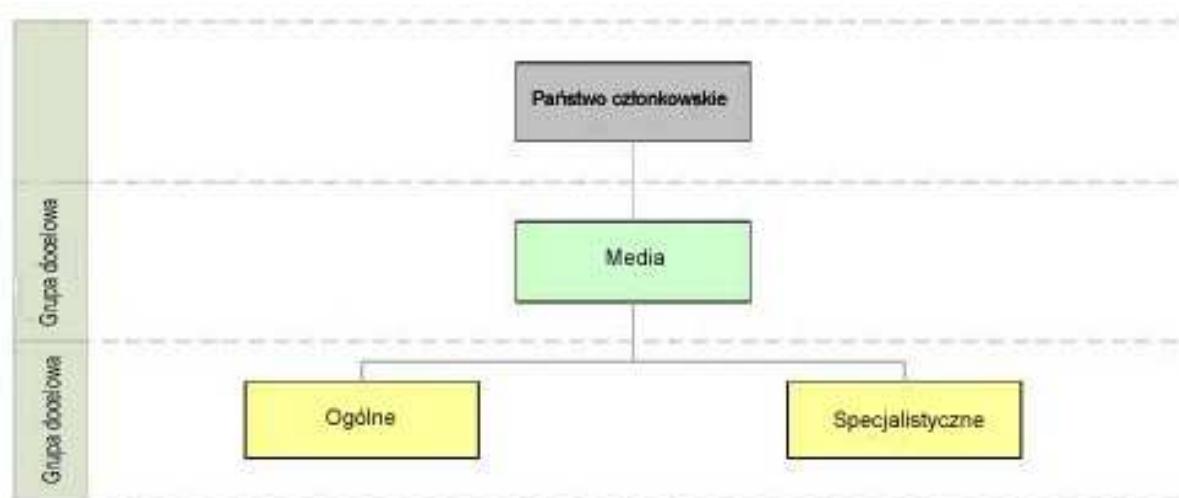
Cele / potrzeby

- Wykorzystywanie ICT do wykonywania pracy lub zadań administracyjnych
- Zapewnienie, że każde działanie online jest poufne i prywatne
- Codzienne interesy i potrzeby są podobne do tych, które mają dorośli użytkownicy prywatni

Dla celów niniejszego dokumentu mikroprzedsiębiorstwa oraz małe i średnie przedsiębiorstwa występują jako całość (MŚP), jako że te trzy kategorie traktowane są często w państwach członkowskich jako jedna.

Media

Ta grupa docelowa jest bardzo ważna, po pierwsze ze względu na wpływ, jaki wywiera na opinię publiczną. Kiedy pracownicy w świecie mediów są bardziej świadomi kwestii związanych z bezpieczeństwem informacji i odpowiednich rozwiązań nie tylko w codziennej pracy, ale także ogólnie, mogą lepiej informować swoich odbiorców. Ponadto uświadamianie odbiorców przekazu medialnego może spowodować, że oni sami będą kłaść większy nacisk na przekazywanie informacji. Tę grupę użytkowników można podzielić na dwie kategorie:



Ogólne

Składają się z dziennikarzy, asystentów dziennikarzy, prezenterów i personelu pomocniczego w środkach masowego przekazu, takich jak telewizja, Internet, radio czy prasa. Zazwyczaj ich odbiorcą docelowym jest przeciętny obywatel.

Główne zagadnienia

- Czas, zasoby i wysiłek, jakie można poświęcić na daną historię są ograniczone
- Jest wiele wiadomości dotyczących informacji i bezpieczeństwa, może to wpłynąć na liczbę materiałów poświęconych bezpieczeństwu informacji

Cele / potrzeby

- Podawanie sprawdzonych wiadomości
- Przekazywanie opinii publicznej i personelowi aktualnych informacji
- Pozytywny wpływ lub lepsze informowanie opinii publicznej (w zależności od materiału)

Specjalistyczne

Składają się z dziennikarzy, asystentów dziennikarzy, prezenterów i personelu pomocniczego w specjalnych środkach masowego przekazu koncentrujących się na określonej tematyce. Na przykład magazyny komputerowe czy tematyczne strony internetowe stanowią formy mediów specjalistycznych.

Główne zagadnienia

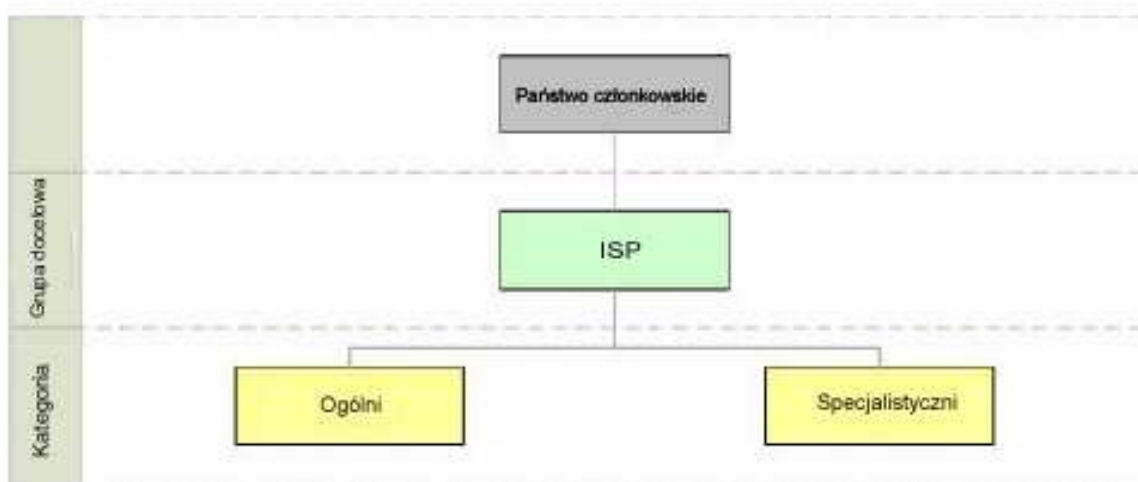
- Główne zagadnienia dotyczące mediów specjalistycznych są podobne do tych, które wymieniono w części poświęconej mediom ogólnym

Cele / potrzeby

- Główne interesy i potrzeby są podobne do tych, które wymieniono w części poświęconej mediom ogólnym

ISP (Dostawcy usług internetowych)

Ta grupa docelowa jest ważna przede wszystkim ze względu na to, że dla firm i opinii publicznej często stanowi pierwszą linię obrony i źródło wiedzy w zakresie bezpieczeństwa informacji. Dzieje się tak dlatego, że ISP zapewniają dostęp do Internetu. Kiedy pracownicy w ISP są bardziej świadomi kwestii związanych z bezpieczeństwem informacji i odpowiednich rozwiązań nie tylko w codziennej pracy, ale także ogólnie, może to przyczynić się do wzmocnienia bezpieczeństwa opinii publicznej. Tę grupę użytkowników można podzielić na dwie kategorie:



Ogólni

Składa się z firm sektora prywatnego, które oferują różne produkty i usługi; dotyczy to nie tylko zwykłej usługi podłączenia do Internetu. Poza dostępem do Internetu usługi mogą obejmować, e-mail, chat, portale internetowe opracowane dla indywidualnego klienta, hotspoty WiFi czy multimedia (video, muzyka). Dla ISP odbiorcami docelowymi są zarówno firmy jak i osoby.

Główne zagadnienia

- Stan technologii i standardy ciągle się zmieniają
- Egzekwowanie musi być bardziej zdecydowane, ponieważ pewne kwestie mogą mieć konsekwencje dla każdej osoby korzystającej z usługi
- Komunikaty nie mogą być zbyt negatywne, ponieważ mogą zniechęcić firmy

Cele / potrzeby

- Przekazywanie opinii publicznej i personelowi aktualnych informacji
- Pozytywne wpływanie na zachowanie opinii publicznej, czego wynikiem jest mniej kwestii do rozwiązania
- Utrzymanie i przyciąganie nowych firm dzięki opinii dotyczącej bezpieczeństwa i oferowanym usługom

Specjalistyczni

Podobni do dostawców ogólnych - jedyna różnica polega na tym, że produkty i usługi skierowane są albo na rynek niszowy, albo zakres usług jest węższy. Zazwyczaj grupa ta oferuje tylko dostęp do Internetu.

Główne zagadnienia

- Główne zagadnienia dotyczące specjalistycznych ISP są podobne do tych, które wymieniono w części poświęconej ogólnym ISP

Cele / potrzeby

- Główne interesy i potrzeby są podobne do tych, które wymieniono w części poświęconej ogólnym ISP

Władze lokalne

Ta grupa docelowa jest ważna, ponieważ musi być postrzegana jako silna i bezpieczna pod względem bezpieczeństwa informacyjnego. W związku z charakterem oferowanych usług często przetwarzane są informacje prywatne i poufne, których naruszenie ma daleko sięgające skutki. Poszczególne państwa członkowskie mają różne systemy polityczne, jednak wszystkie mają te same cele w zakresie świadczenia bezpiecznych i pewnych usług dla społeczeństwa, zarówno w ramach konwencjonalnych umów, takich jak usługi bezpośrednie i nowoczesnych usług online wykorzystujących technologie, takie jak transakcje online.

Grupę użytkowników, którzy tworzą władze lokalne można podzielić na podkategorie wykorzystywane dla grupy docelowej MŚP:



Dyrektor, kadra zarządzająca IT, kadra zarządzająca i pracownicy

Szczegółowe informacje dotyczące każdej kategorii znajdują się w odpowiedniej części *Profile grup* dla grupy docelowej MŚP.

Główne zagadnienia

- Zob. główne zagadnienia wymienione w poprzedniej części dla grupy docelowej MŚP.
- Ponadto użytkownicy z władz lokalnych muszą przestrzegać procedur i protokołów zgodności obowiązujących służby publiczne

Cele / potrzeby

- Zob. interesy i potrzeby wymienione w poprzedniej części dla grupy docelowej MŚP.
- Ponadto użytkownicy z władz lokalnych muszą zapewniać bezpieczne i skuteczne usługi w miejscu pracy, a także w komunikacji ze społeczeństwem

Katalog dobrych praktyk

Poniższa matryca stanowi katalog rodzajów odpowiedzi i wyszczególnienie informacji dostarczonych przez państwa członkowskie w odpowiedzi na kwestionariusz:

- Kolumna „państwa członkowskie” zawiera nazwę kraju, do którego wysłano kwestionariusz
- Państwa członkowskie (wiersze) zostały pogrupowane za pomocą różnych kolorów Pogrupowano je pod kątem podobieństw odnoszących się do kultury, wiedzy, doświadczenia, interesów / potrzeb grup docelowych oraz języka. Grupowanie wykonano wyłącznie w celach orientacyjnych
- Kolumny „Pytania” zawierają skrócone nazwy różnych części kwestionariusza. „X” w danym wierszu oznacza, że państwo członkowskie przekazało informację lub odpowiedź dla danej części
- Kolumny „Informacje o grupie docelowej” zawierają pięć grup docelowych, których profil znajduje się w Pakiecie informacyjnym. „X” w danym wierszu oznacza, że państwo członkowskie przekazało informację dla określonej grupy
- Kolumna „Dostępne materiały” informuje, że ENISA zapoznała się z materiałem, który został opracowany przez państwa członkowskie. „X” w wierszu pokazuje, że opracowany materiał może być wykorzystany jako podstawa do opracowania materiału do kampanii w innym państwie członkowskim lub w całości ponownie wykorzystany. Należy zauważyć, że większość materiałów zostało opracowanych w oficjalnych językach państw członkowskich
- Kolumna „Strony internetowe” zawiera adresy stron internetowych przekazane przez państwa członkowskie w odpowiedzi na kwestionariusz

Państwa członkowskie	Pytania					Informacje o grupie docelowej					Dodatkowe informacje	Dostępne materiały	Strony internetowe		
	Władze jako projektant	Władze jako użytkownik	Władze lokalne jako użytkownik	Władze jako partner (firmy)	Władze jako partner (społeczeństwo)	Statystyki/kluczowe wskaźniki wydajności	Użytkownik prywatny	MŚP	Media	ISP	Władze lokalne	Bieżąca sytuacja		Kampanie	Zdobyte doświadczenie
1	Austria														
				X			X	X				X		X	http://www.it-safe.at , http://portal.wko.at/wk/format_detail.wk?AnglID=1&StlID=209879&BrID=0&DstID=5344 , http://www.itsafe.at/siha/fragebogen.html , http://www.ocg.at/publikationen/books/volumes/sr181.html , http://www.cio.gv.at/securenetworks/sihb/
2	Belgia														
							X						X	X	http://www.click2win.be , http://www.web4me.be
3	Cypr														
	X												X		
4	Czechy														
	X	X	X	X				X							http://www.micr.cz/nppg.html
5	Dania														
	X			X	X		X	X				X	X	X	www.it-borger.dk/netsikkernu , www.netsikkernu.dk
6	Estonia														
	X	X	X	X	X	X									http://www.egov-goodpractice.org
7	Finlandia														
				X	X		X	X					X	X	www.tietoturvaopas.fi , http://www.pelastakaalapset.fi/hiiripii/ , http://www.pelastakaalapset.fi/nettivihje/english
8	Francja														
	X				X		X		X					X	http://www.famille.gouv.fr/protection-famille
9	Niemcy														
	X	X	X	X	X	X	X	X			X			X	www.bsi.bund.de , www.bsi-fuer-buerger.de , www.bsi.de/literat/buanzg.htm , www.bsi.de/literat/brosch.htm , www.bsi.de/literat/index.htm , http://www.bsi.bund.de/english/index.htm

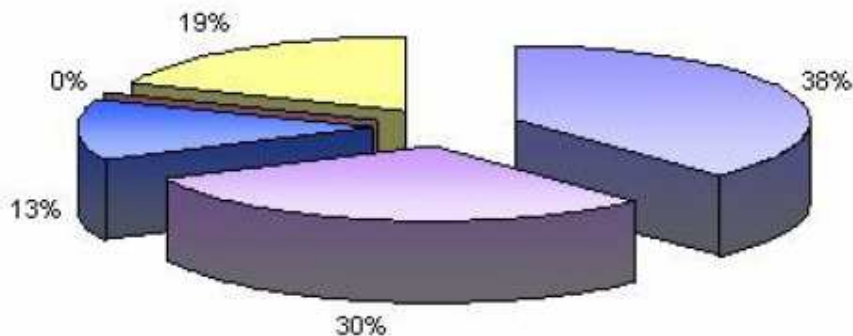
													www.bsi.de/english/gshb/guidelines/index.htm , www.bsi.de/gshb/deutsch/musterriichtlinien/index.htm , www.bsi.de/gshb/deutsch/hilfmi/beispielprofile.htm , www.teletrust.de , www.mcert.de , www.initiated21.de
10	Grecja						X			X	X	X	http://www.saferInternet.gr
11	Węgry	X	X	X	X	X	X	X		X	X		www.ihm.gov.hu , www.biztonsagosInternet.hu , www.halozatbiztonsag.hu , www.english.itktb.hu/Engine.aspx , www.meh.hu/szervezet/hivatalok/ekk/kietb/kietb20041116.html , www.nhh.hu , www.spam.baratsagosInternet.hu , www.magyarorszag.hu , www.telehaz.hu , www.itmentor.hu , www.esec.hu , www.iszt.hu/iszt/English , www.ivsz.hu , www.Internethotline.hu , www.matisz.hu , www.mte.hu , www.inforum.org.hu
12	Islandia						X			X		X	www.saft.is
13	Irlandia				X		X	X		X	X		
14	Włochy	X	X	X		X	X	X	X	X		X	www.cnipa.gov.it/site/itit/La_Documentazione/Pubblicazioni/i_Quaderni/ , www.cnipa.gov.it/site/itit/Attivit%c3%a0/Sicurezza_informativa/ , http://www.cnipa.gov.it , http://www.italia.gov.it
15	Łotwa	X	X	X	X	X	X						
16	Lichtenstein												
17	Litwa	X	X		X	X		X	X			X	www.esaugumas.lt , www.vrm.lt , www.securityconference.rtt.lt , http://www.esaugumas.lt/VRM/VRM/index.html
18	Luksemburg	X	X	X	X	X	X	X	X	X		X	www.cases.lu , www.mysecureit.lu , www.petitweb.lu
19	Malta	X	X	X	X	X	X	X	X			X	http://www.miti.gov.mt/site/page.aspx?pageid=4 , www.miti.gov.mt
20	Holandia	X	X	X	X	X		X	X	X		X	www.digibewust.nl , www.ecp.nl , www.surfsafe.nl , http://www.onderzoeksdatabank.minez.nl/onderzoeken/onderzoekkaart.aspx?onderzoekID=2934






													http://www.onderzoeksdatabase.minez.nl/rapporten/Rapport.aspx?rapportId=485 , www.waarschuwingsdienst.nl
21	Norwegia	X		X	X		X	X	X			X	www.norsis.no , www.nettvett.no
22	Polska	X	X	X			X	X	X				www.zpp.pl , http://hotline.org.pl/ , www.saferInternet.pl , www.dzieckowsieci.pl , http://www.cert.pl
23	Portugalia	X					X		X	X			www.unic.pt , www.cert.pt , www.ina.pt , www.crie.min-edu.pt , www.fccn.pt
24	Słowacja	X	X	X	X	X	X						
25	Słowenia	X	X	X	X	X	X	X			X		http://www.zrss.si/ , http://www.safe.si , http://www.ris.org/index.php?fl=0&p1=276&p2=285&p3=&id=
26	Hiszpania												
27	Szwecja	X	X	X	X	X	X	X	X		X	X	http://www.pts.se/Default.asp?Sectionid=&Itemid=&Languageid=EN , http://www.sitic.se/eng/index.html , http://www.konsumentverket.se/mallar/en/startsidan.asp?lngCategoryId=646 , http://www.konsumentverket.se/mallar/en/lista_artiklar.asp?lngCategoryId=922 , http://www.verva.se/web/t/Page_492.aspx , http://www.krisberedskapsmyndigheten.se/6193.epibrw , http://kikaren.skl.se/artikel.asp?C=756&A=180 , http://www.pts.se/Nyheter/pressmeddelande.asp?Itemid=4718 , www.pts.se/internetsakerhet , www.testadatorn.se , http://www.surfalugnt.se
28	Wielka Brytania	X	X	X	X	X	X	X	X		X	X	www.cctmark.gov.uk , www.itsafe.gov.uk , www.getsafeonline.org , www.cabinetoffice.gov.uk/csia/ia_governance/content.asp , http://www.niscc.gov.uk/niscc/warpInfo-en.html , www.dti.gov.uk/sectors/infosec , www.kable.co.uk , www.securityhealthcheck.dti.gov.uk , www.cbi.org.uk , www.bobs-business.co.uk , www.instisp.org , www.securitysurvey

gov.uk,
http://www.wda.co.uk/index.cfm/technology_and_innovation/mtp/partner_programme/ecrime/en8118,
<http://www.internetsafetyzone.co.uk>

Poniższy wykres przedstawia podział odpowiedzi państw członkowskich na kategorie:

Programy poszerzania wiedzy według grup docelowych:



-  20 inicjatyw poszerzania wiedzy skierowanych do użytkowników prywatnych (38 %)
-  16 inicjatyw poszerzania wiedzy skierowanych do MŚP (30 %)
-  10 inicjatyw poszerzania wiedzy skierowanych do władz lokalnych (19 %)
-  7 inicjatyw poszerzania wiedzy skierowanych do ISP (13 %)
-  brak inicjatyw poszerzania wiedzy skierowanych do (0 %)

Dobre praktyki w poszczególnych krajach

Informacje znajdujące się w następującej części odnoszą się do odpowiedzi na kwestionariusz ENISA, które otrzymano od państw członkowskich i/lub do informacji i materiałów dodatkowych dostarczonych przez inne instytucje/organizacje. Warto zauważyć, że:

- Pod względem układu kwestionariusz jest podobny do kwestionariuszy stosowanych przez OECD przy tworzeniu raportu „The Promotion of a Culture of Security for Information Systems and Networks in OECD Countries” z 2005 r.
- Jeżeli brakuje jakiejś części, to znaczy, że państwo członkowskie nie dostarczyło informacji
- Części „Bieżąca sytuacja”, „Kampanie” czy „Doświadczenia” dla każdego kraju zawierają szczegóły, o ile państwa członkowskie przekazały dodatkowe lub zmienione informacje do odpowiedzi na kwestionariusz

1. Austria

Na podstawie odpowiedzi na kwestionariusz oraz uzupełnionych informacji z przeprowadzonych rozmów, badań i dodatkowych materiałów dla Austrii wyszczególniono następujące części.

[Bieżąca sytuacja](#)

[Rząd jako partner przedsiębiorstw i przemysłu](#)

[Kampanie](#)

Bieżąca sytuacja

- Podobnie jak w pozostałych państwach członkowskich znaczenie małych i średnich przedsiębiorstw dla gospodarki austriackiej jest ogromne. 99.8% wszystkich przedsiębiorstw to małe i średnie przedsiębiorstwa (do 500 pracowników) zatrudniające średnio około 10 pracowników na firmę.
- Łączna liczba przedsiębiorstw, szczególnie mikroprzedsiębiorstw wzrosła w latach 1988-1993. Z uwagi na to, że zatrudnienie rosło w podobnym tempie, średnia wielkość przedsiębiorstw pozostała niezmienną. Tworzenie przedsiębiorstw było jednak znacznie mniej dynamiczne w Austrii niż w innych krajach europejskich, takich jak Niemcy, Belgia, Dania czy Holandia.
- Cały sektor prywatny w Austrii, szczególnie rzemiosło, usługi i turystyka jest zdominowany przez MŚP, chociaż duże przedsiębiorstwa mają znaczny udział w łącznym zatrudnieniu w produkcji przemysłowej i transporcie.
- W 1993 r. około 195 000 prywatnych przedsiębiorstw zatrudniało w Austrii około 2 mln ludzi. Około 500 przedsiębiorstw to duże przedsiębiorstwa, podczas

gdy ponad 194 500 to MŚP, których udział w łącznym zatrudnieniu wynosił z ponad 75 %.

Rząd jako partner przedsiębiorstw i przemysłu **Małe i średnie przedsiębiorstwa (MŚP)**

Inicjatywa IT-SAFE

Inicjatywa poszerzania wiedzy IT-SAFE była skierowana do małych firm, które dotąd nie rozważały i nie wprowadziły bezpieczeństwa danych do swoich planów i wewnętrznych polityk. Celem tej inicjatywy jest poszerzanie wiedzy o bezpieczeństwie informacji poprzez udzielanie przedsiębiorstwom praktycznych porad na temat tego, jak osiągnąć ten cel z uwzględnieniem profilu (np. potrzeby przedsiębiorstwa) tej grupy docelowej.

Zasadniczo istnieją dwa główne problemy:

- Ochrona komputerów wykorzystywanych przez MŚP przed zagrożeniami z zewnątrz
- Unikanie utraty danych wskutek niewystarczających zasobów rezerwowych i procedur zachowania danych

Każde MŚP jest unikatowe i dlatego ma swoje własne określone potrzeby w kwestii bezpieczeństwa IT. Ponadto należy brać pod uwagę, że dostępne systemy zabezpieczania informacji, takie jak CobIT, ISO 17799/27001 czy Common Criteria są prawie w każdym przypadku niedostosowane do mniejszych firm z uwagi na ich ukierunkowanie na potrzeby dużych przedsiębiorstw.

Dlatego inicjatywa IT-SAFE udostępnia kwestionariusz online, który ocenia zarówno infrastrukturę IT danej firmy oraz jej konieczny poziom ochrony w danym przedsiębiorstwie w celu dostosowania i dostarczenia indywidualnych wersji podręcznika IT-SAFE na potrzeby poszerzania wiedzy o bezpieczeństwie informacji. Informacje znajdujące się w podręczniku zawierają porady krok po kroku dla administratora IT, które mają na celu pomoc w zabezpieczeniu infrastruktury IT firmy. Indywidualna wersja podręcznika IT-SAFE jest wykonywana w formacie HTML lub Adobe Acrobat.

Austriacka izba handlowa we współpracy z federalnym ministerstwem gospodarki i pracy (BMWA) i instytutem promocji gospodarki (WiFi) zaproponowała specjalne udogodnienia dla uczestniczących firm. Było wśród nich 75 % wsparcie dla doradztwa na temat bezpieczeństwa IT (do 6 godzin usług doradczych). Ponadto zaoferowano pakiet zawierający programy zwiększające bezpieczeństwo, takie jak programy antywirusowe i antyszpiegowskie. Inicjatywy były sponsorowane przez takie firmy jak Ikarus, Nimbus Datentechnik, Symantec i Microsoft. Oprogramowanie udostępniono bezpłatnie.

Cele / potrzeby

Inicjatywa w zakresie bezpieczeństwa IT-SAFE jest skierowana do MŚP zatrudniających do 25 pracowników i polega na doradzaniu personelowi odpowiedzialnemu za IT z uwzględnieniem jego wiedzy, interesów i potrzeb. Inicjatywa IT-SAFE jest zwykle skierowana do przedsiębiorstw, które wiedzą niewiele o bezpieczeństwie informacji. Wykorzystane materiały i kanały:

- Podręcznik w wersji papierowej
 - Brak wymagania uprzedniej ekspertyzy
 - Zrozumiały, ale wszechstronny
 - Bez opłat, dostępny online
- Podręcznik online i strona internetowa
 - Indywidualny podręcznik
 - Dostępne dwie wersje: jedna dla dyrektorów generalnych i jedna dla administratorów
 - Strona internetowa z kwestionariuszem
- Kontrola bezpieczeństwa w przedsiębiorstwie
 - Darmowy program antywirusowy i zabezpieczający dane
 - Doradztwo indywidualne
 - Wsparcie dla 60 godzin doradztwa

Z uwagi na to, że IT-SAFE została zainicjowana przez austriacką izbę handlową inicjatywa była bardzo przejrzysta i odniosła sukces.

W przyszłości planuje się dotarcie do szerszych kręgów odbiorców. Dlatego podręcznik zostanie dostosowany w celu uwzględnienia interesów, potrzeb i wiedzy tej grupy docelowej. Informacje dotyczące tej inicjatywy są dostępne online od roku. Więcej informacji znajduje się pod poniższymi linkami:

- <http://www.it-safe.at>
- http://portal.wko.at/wk/format_detail.wk?AnglID=1&StID=209879&BrID=0&DstID=5344
- <http://www.it-safe.at/siha/fragebogen.html> – kwestionariusz i podręcznik online

Austriacki podręcznik dotyczący bezpieczeństwa IT

Austriacki podręcznik dotyczący bezpieczeństwa IT jest przewodnikiem, który pomaga zapewnić wszechstronną podstawową ochronę IT w przedsiębiorstwach i organizacjach. Inaczej niż w przypadku niemieckiego podręcznika dotyczącego podstawowej ochrony IT nie jest on tak wszechstronny (około 400 stron wobec 3000 stron podręcznika dotyczącego podstawowej ochrony IT). Jego treść koncentruje się bardziej na zarządzaniu ryzykiem, któremu poświęcono jedną z dwóch części. Druga część dotyczy środków bezpieczeństwa IT.

Program poszerzania wiedzy (część podręcznika)

Skuteczne wdrażanie polityki i zasad bezpieczeństwa w organizacji jest możliwe tylko poprzez zrozumienie i stałe motywowanie członków personelu. Aby to osiągnąć konieczny jest wszechstronny, obejmujący całą organizację program poszerzania wiedzy. Program ten powinien składać się z następujących części:

- Informowanie wszystkich członków personelu o polityce bezpieczeństwa IT organizacji
- Cele polityki bezpieczeństwa IT instytucji oraz ich objaśnienie
- Znaczenie bezpieczeństwa IT instytucji
- Organizacja i obowiązki w obszarze bezpieczeństwa IT
- Strategia analizy ryzyka
- Bezpieczna klasyfikacja danych
- Wybrane środki bezpieczeństwa (szczególnie te, które są ważne dla całej organizacji)

Więcej informacji znajduje się pod adresem:

http://www.cio.gv.at/securenetworks/sihb/OE-IT-SIHB_V2_2_Teil1.pdf.

Cele / potrzeby

Podręcznik jest przede wszystkim skierowany do następujących osób o niskim lub średnim poziomie wiedzy:

- Personel IT odpowiedzialny za bezpieczeństwo IT w instytucjach publicznych i firmach
- Zainteresowane osoby prywatne

Podręcznik jest stale ulepszany i poprawiany.

- <http://www.ocg.at/publikationen/books/volumes/sr181.html>
- <http://www.cio.gv.at/securenetworks/sihb/>

Kampanie

SaferInternet - Saferinternet.at jest skierowany do rodziców (artykuł)⁹

Streszczenie

Dostępne są nowe broszury i materiały o bezpiecznym korzystaniu z Internetu i telefonów komórkowych. Materiały dotyczą roli rodziców i opiekunów.

Szczegóły

Saferinternet.at jest obecnie skierowany do rodziców jako głównej grupy docelowej i ma na celu poprawę bezpieczeństwa korzystania z Internetu i telefonów komórkowych przez nieletnich w Austrii.

Według ostatniego raportu Eurobarometru coraz więcej rodziców w Austrii określiło zasady dotyczące korzystania z nowoczesnej technologii i narzędzi komunikacji (63 %). Znacznie poprawiła się także wiedza o tym, jak informować o nielegalnych treściach w Internecie. Mimo tych pozytywnych wyników wielu rodziców nadal obawia się zagrożeń online i chce dowiedzieć się jak radzić sobie z tymi kwestiami w swoich rodzinach.

Dlatego Saferinternet.at opublikował niedawno, we współpracy z Familienverband Österreich, największą w Austrii organizacją ds. rodziny, broszurę „Kein Stress mit Web and SMS – Fakten und Tipps für Eltern und Erziehungsberechtigte zum Umgang mit Internet und Handy”. Broszura zawiera informacje i porady na temat bezpieczeństwa Internetu i telefonów komórkowych dla rodziców i wychowawców oraz kładzie szczególny nacisk na edukację medialną. Zostanie dostarczona do 70 000 rodzin w całym kraju.

W odpowiedzi na aktualne zjawiska w Austrii, takie jak przemoc i dostęp do szkodliwych treści wideo za pomocą telefonów komórkowych Saferinternet.at opracował także broszury na ten temat.

Wszystkie materiały (dostępne w języku niemieckim) można ściągnąć ze strony internetowej Saferinternet.at pod adresem <http://www.Saferinternet.at>.

Ponadto punkt Awareness organizuje wiele imprez dla rodziców i opiekunów: od wieczorów informacyjnych do wspólnych warsztatów dla rodziców i ich dzieci.

⁹ <http://www.saferinternet.org/ww/en/pub/insafe/news/articles/0606/at.htm>, 12 czerwca 2006 r.

2. Belgia

Na podstawie odpowiedzi na kwestionariusz oraz informacji uzupełniających z przeprowadzonych rozmów, badań i dodatkowych materiałów dla Belgii wyszczególniono następujące części.

Kampanie

Kampanie

Kampania „Bezpieczne korzystanie z Internetu”

W Belgii kampania „Bezpieczne korzystanie z Internetu” została zorganizowana w celu promowania wiedzy wśród dzieci w wieku 11-12 lat. W celu skutecznego przekazywania komunikatu kampanii z wykorzystaniem najbardziej odpowiednich kanałów przekazywania informacji organizatorzy kampanii zdecydowali o stworzeniu komiksu opartego na popularnym serialu „Suske en Wiske” (w języku niderlandzkim i niemieckim. W języku francuskim tytuł brzmi „Bob i Bobette”).

W dniu 6 lutego 2006 r. Peter Van Velthoven (minister informacji państwa), przedstawił komiks w trzech oficjalnych językach: "De Sinistere Site" (w języku niderlandzkim), "Le Site Sinistre" (w języku francuskim) i "Der Listige Link" (w języku niemieckim).



Łączna liczba wydrukowanych albumów wyniosła 120 000 (wersji niderlandzkiej), 80 000 (wersji francuskiej) i 1500 (wersji niemieckiej).

Komiks, który nie jest dostępny w księgarniach został rozprowadzony wśród dzieci szóstej (i ostatniej) klasy wszystkich szkół podstawowych w tygodniu rozpoczynającym się 27 marca 2006 r.

Uznano, że kanał wykorzystany do poszerzenia wiedzy dzieci jako część kampanii dotyczącej bezpieczeństwa informacji był bardzo skuteczny, ponieważ dotarł do grupy docelowej bezpośrednio.

Co więcej w ramach kampanii wszyscy obywatele belgijscy w wieku 12 lat otrzymują elektroniczne dowody tożsamości z darmowym czytnikiem kart. Umożliwi im to bezpieczne rozmowy przez Internet. Dzieci będą korzystać z określonych stron internetowych. Celem jest zmniejszenie ryzyka kontaktu dziecka z ludźmi o złych zamiarach.

Pułapka w celu lepszego informowania

Agencja komunikacji „Edge Communication” rozpoczęła kampanię poszerzania wiedzy o bezpieczeństwie informacji. Ta nowa kampania jest prowadzona w ramach projektu European Safer Internet i jest skierowana do młodych ludzi w wieku 14-18 lat.

Za pośrednictwem strony internetowej <http://www.click2win.be> fikcyjny operator komórkowy (CelBel) oferuje darmowy abonament dla osób poniżej 21 roku życia, w tym SMS, Chat, MSN i e-mail. Aby się zarejestrować internauta musi wprowadzić swoje dane osobowe. Zaraz po rejestracji na ekranie pojawia się komunikat wyjaśniający internaucie, że nowy operator nie istnieje. Internauta jest następnie proszony o odwiedzenie strony internetowej „Web4me” pod adresem <http://www.web4me.be>. Celem strony internetowej, która pojawiła się w maju ubiegłego roku jest promowanie odpowiedzialnego korzystania z Internetu przez młodzież.

Na stronie można także znaleźć stowarzyszenia i osoby kontaktowe, do których młodzi ludzie mogą dotrzeć jeżeli spotkają się z pięcioma rodzajami zagrożeń:

- Sekta – centrum opinii i informacji o szkodliwych organizacjach sektowych, Centre d'information et d'avis sur les organisations sectaires nuisibles (CIAOSN)
- Marketing – centrum badań i informacji organizacji konsumentów, Centre de recherche et d'information des organisations de consommateurs (CRIOC)
- Technika - stowarzyszenie dostawców usług internetowych, Internet Service Providers Association (ISPA)
- Dyskryminacja - centrum równości szans i walki z rasizmem, Centre pour l'égalité des chances et la lutte contre le racisme
- Pornografia - Child Focus association

Operator „CelBel” będzie nadal obecny w Internecie na bannerach i na listach mailingowych. Od początku września fikcyjny operator będzie przedstawiany w systemach peer-to-peer (np. Kaaza, który umożliwia wymianę plików między prywatnymi osobami).

3. Cypr

Na podstawie odpowiedzi na kwestionariusz oraz informacji uzupełniających z przeprowadzonych rozmów, badań i dodatkowych materiałów dla Cypru wyszczególniono następujące części:

[Rząd jako twórca prawnych, regulacyjnych i instytucjonalnych uregulowań służących poszerzaniu wiedzy](#)

[Kampanie](#)

Rząd jako twórca prawnych, regulacyjnych i instytucjonalnych uregulowań służących poszerzaniu wiedzy

Krajowa strategia poszerzania wiedzy

Dokument programowy w sprawie bezpieczeństwa sieci i informacji jest obecnie oceniany przez ministra komunikacji i pracy. Uważa się, że minister komunikacji i pracy sfinalizuje dokument we wrześniu, 2006 r., dlatego ocenia się, że wdrażanie dokumentu programowego zacznie się przed końcem roku.

Środki służące poszerzaniu wiedzy będą wdrażane jako część dokumentu programowego w sprawie bezpieczeństwa sieci i informacji. Początkowo plan działania będzie dotyczył poszerzania wiedzy użytkowników końcowych, właściwych organów publicznych do spraw bezpieczeństwa sieci i informacji, innych podmiotów publicznych i prywatnych oraz przedsiębiorstw. Plan działania ma być zakończony w pierwszym kwartale 2007 r. stąd początek jego wdrażania jest planowany na kwiecień 2007 r.

Prawne, regulacyjne i instytucjonalne porozumienia służące poszerzaniu wiedzy

OCECPR jest z mocy prawa (L.112(I)/2004) organem odpowiedzialnym za koordynowanie spraw związanych z bezpieczeństwem sieci i informacji na Cyprze. OCECPR jest przedstawicielem Cypru w zarządzie ENISA i działa jako centralny punkt kontaktowy i koordynacyjny między Cyprem a europejską agencją.

Do niedawna na Cyprze nie były prowadzone działania w zakresie koordynacji w tym obszarze. Niektóre działania służyły do ochrony państwa i cywilnych sieci i usług, natomiast prywatne firmy i organizacje, takie jak ISP i banki przedstawiły kilka inicjatyw. Znaczna część firm na Cyprze, szczególnie MŚP nie okazuje większego zainteresowania kwestiami bezpieczeństwa, przede wszystkim ze względu na wysokie koszty z tym związane, ich ograniczone dochody wynikające z niewielkich rozmiarów rynku oraz brak oczywistych korzyści (bezpośredni dochód) z takich inwestycji. Ramy współpracy między podmiotami publicznymi oraz między podmiotami publicznymi a prywatnymi będą określone we wskazanym wyżej dokumencie programowym, a także zostanie określona hierarchia działań w celu wzmocnienia polityki bezpieczeństwa sieci

i informacji. Poszerzanie wiedzy jest jednym z głównych problemów tego dokumentu programowego.

Kampanie

OCECPR realizuje obecnie zadania w zakresie koordynacji poszerzania wiedzy i planuje prowadzić inicjatywę tworzenia grup roboczych, które będą skupiać przedstawicieli instytucji publicznych, placówek bankowych, instytucji akademickich, projektantów i dostawców systemów bezpieczeństwa sieci i informacji, dostawców sieci i organizacji ochrony konsumentów.

Celem wysiłku będzie kształcenie i informowanie użytkowników z uwzględnieniem charakterystyki każdej grupy docelowej oraz wdrażanie konkretnych działań w zakresie rozwoju odpowiedniej kultury bezpieczeństwa w kwestiach związanych z bezpieczeństwem nowoczesnych sieci i wymianą informacji.

OCECPR bierze pod uwagę doświadczenia innych krajów europejskich, które miały duże doświadczenie w tym sektorze uwzględniając różnorodność parametrów w poszczególnych krajach, strukturę społeczną, system edukacji, strukturę przedsiębiorstw, kulturę korzystania z nowych urządzeń elektronicznych i systemów bezpieczeństwa, strukturę gospodarki i inne elementy.

Pozytywne przykłady zostaną wzięte pod uwagę, o ile mogą być przystosowane. Wraz z kilkoma inicjatywami, które będą prowadzone we współpracy z innymi właściwymi instytucjami publicznymi i prywatnymi będzie to stanowić źródło działania na rzecz jak najlepszego rozpowszechniania odpowiednich informacji zgodnie z potrzebami każdego użytkownika. Jeżeli chodzi o biznesowych użytkowników sieci i usług komunikacji elektronicznej, wysiłek będzie skoncentrowany na odpowiednim stosowaniu międzynarodowych standardów dotyczących bezpieczeństwa sieci i informacji oraz na tworzeniu odpowiedniej polityki zarządzania ryzykiem w kwestiach bezpieczeństwa.

4. Czechy

Na podstawie odpowiedzi na kwestionariusz oraz informacji uzupełniających z przeprowadzonych rozmów, badań i dodatkowych materiałów dla Czech wyszczególniono następujące części:

[Rząd jako twórca prawnych, regulacyjnych i instytucjonalnych rozwiązań służących poszerzaniu wiedzy](#)

[Władze państwowe jako użytkownik systemów informacyjnych](#)

[Władze lokalne jako użytkownik systemów informacyjnych](#)

Rząd jako partner przedsiębiorstw i przemysłu

Rząd jako twórca prawnych, regulacyjnych i instytucjonalnych rozwiązań służących poszerzaniu wiedzy

Krajowa strategia poszerzania wiedzy

W celu dokonania przeglądu czeskiej krajowej strategii poszerzania wiedzy skontaktowano się z kilkoma organizacjami. Wydaje się, że nie mają one doraźnej strategii poszerzania wiedzy. Takie inicjatywy stanowią część działań ministerstwa właściwego do spraw związanych z systemami informacyjnymi.

Bieżące działania koncentrują się głównie na takich zadaniach wspierania korzystania z podpisu elektronicznego oraz promowanie korzystania z certyfikatów w komunikacji z systemami informacyjnymi administracji publicznej (PAIS).

Prawne, regulacyjne i instytucjonalne postanowienia służące poszerzaniu wiedzy

Głównym aktem prawnym jest ustawa 227/2000 (w sprawie podpisu elektronicznego). Celem jest większe wsparcie dla korzystania z podpisu elektronicznego, ponieważ jest to postrzegane jako ważny element bezpieczeństwa. Inny akt prawny, ustawa 365/2000 (w sprawie PAIS) zawiera nową poprawkę, która będzie regulować bezpieczeństwo i poszerzanie wiedzy w PAIS.

Ministerstwo współpracowało z Microsoftem w kwestii promowania bezpieczeństwa jako kluczowego komponentu publicznego i prywatnego zarządzania. Przeanalizowano także praktyki ENISA i innych organów UE.

Prowadzone są krajowe kursy w zakresie umiejętności informacyjnych (w tym bezpieczeństwa). Są skierowane do obywateli. Szczegółowe informacje: <http://www.micr.cz/nppg.html>

Władze państwowe jako użytkownik systemów informacyjnych

Najnowsze inicjatywy i programy poszerzania wiedzy

Jeden z projektów technicznych prowadzonych obecnie dotyczy tworzenia dwóch systemów metainformacyjnych PAIS. Jednym z celów wdrażania jest skłonienie użytkowników do zaakceptowania działań; kiedy przenoszą dane z systemów, dane te muszą być opatrzone podpisem elektronicznym.

Władze lokalne jako użytkownik systemów informacyjnych

Najnowsze inicjatywy i programy poszerzania wiedzy

Poniższe linki mogą być wykorzystane do uzyskania informacji o krajowym programie umiejętności informacyjnych. Strony w języku czeskim:

- <http://www.micr.cz/scripts/detail.php?id=3361>
- <http://www.micr.cz/scripts/detail.php?id=1930>
- <http://www.micr.cz/scripts/detail.php?id=2137>
- <http://www.micr.cz/scripts/detail.php?id=2813>

Rząd jako partner przedsiębiorstw i przemysłu

Małe i średnie przedsiębiorstwa (MŚP)

Ministerstwo prowadzi wspólnie z firmą Microsoft prace nad inicjatywami mającymi na celu promowanie bezpieczeństwa informacji. Obecnie w przedsięwzięciu tym nie bierze udziału żadna inna firma z sektora prywatnego. Ministerstwo wykorzystuje współpracę z firmą Microsoft i doświadczenia agencji ENISA i innych organów UE dla potrzeb związanych z działaniami mającymi na celu poszerzanie wiedzy.

5. Dania

Na podstawie odpowiedzi na kwestionariusz oraz informacji uzupełniających z przeprowadzonych rozmów, badań i dodatkowych materiałów dla Danii wyszczególniono następujące części:

Bieżąca sytuacja

Rząd jako twórca prawnych, regulacyjnych i instytucjonalnych postanowień służących poszerzaniu wiedzy

Rząd jako partner przedsiębiorstw i przemysłu

Rząd jako partner społeczeństwa

Kampanie

Bieżąca sytuacja

- Istnieje potrzeba przekazywania informacji na temat bezpieczeństwa IT, ponieważ coraz więcej Duńczyków codziennie korzysta z Internetu; 79% ma dostęp do Internetu w domu, przy czym 57% korzysta z Internetu codziennie. Główne powody korzystania z Internetu to komunikowanie się, poszukiwanie informacji i korzystanie z usług on-line; Ministerstwo Nauki, Technologii i Innowacji postrzega to w kategoriach pozytywnego rozwoju i chce zachęcić Duńczyków do korzystania z Internetu; jednocześnie zastanawia się także nad tym, w jaki sposób Duńczycy korzystają z Internetu;
- Najbardziej aktualne problemy związane z bezpieczeństwem IT w Danii to spam, utrata informacji czy czas, jaki jest potrzebny na unieszkodliwienie wirusów; w 2005 r. 35 % ludności Danii utraciło informacje w wyniku ataku wirusów, 55 % ludności Danii utraciło dane w związku ze spamem.

Rząd jako twórca prawnych, regulacyjnych i instytucjonalnych uregulowań służących poszerzaniu wiedzy

Krajowa strategia poszerzania wiedzy

Kampania „Net-safe now!” (wydarzenie coroczne)

Ministerstwo Nauki, Technologii i Innowacji po raz drugi zorganizowało kampanię informacyjną skierowaną do społeczeństwa na temat bezpieczeństwa IT zatytułowaną „Net-safe now!”. Ministerstwo współpracowało z kilkoma różnymi instytucjami zarówno prywatnymi, jak i publicznymi (między innymi z firmami Microsoft, Nordea, PBS, itd.) w celu zorganizowania i poprowadzenia kampanii.

Podstawa kampanii

Celem Ministerstwa Nauki, Technologii i Innowacji i kampanii „Net-safe now!” jest poszerzanie wiedzy na temat bezpieczeństwa IT i bezpiecznego poruszania się po Internecie. W ramach kampanii na terytorium całej Danii prowadzonych jest wiele działań.

Kampania obejmuje serię działań skierowanych do docelowych odbiorców, np. informowanie dzieci i osób starszych o sposobie zachowania podczas korzystania z Internetu. Działania w ramach kampanii, która rozpoczęła się 2 maja, były prowadzone przez cały maj. Celem kampanii jest przekazanie grupie docelowej jasnych wskazówek w celu poszerzenia ogólnej wiedzy i świadomości na temat bezpieczeństwa IT.

Ogólnie rzecz biorąc głównym celem kampanii jest rozpowszechnienie wiedzy na temat bezpieczeństwa IT i uświadomienie społeczeństwu istnienia zagrożeń, jakie wynikają z korzystania z Internetu. Celem długoterminowym jest przyczynienie się do rozwoju kultury bezpieczeństwa IT w Danii poprzez zachęcanie użytkowników IT do przejawiania odpowiedzialnych zachowań i w konsekwencji podejmowania bezpieczniejszych działań.

Oprócz różnych inicjatyw organizowanych w ramach kampanii w całym kraju, kampania jest także promowana w mediach, takich jak prasa ogólnokrajowa i lokalna, telewizja, radio i Internet. W ramach kampanii prowadzonych jest wiele działań on-line, które są dostępne na stronie internetowej www.it-borger.dk/netsikkernu. Na stronie tej znajdują się istotne informacje skierowane do użytkowników na temat kampanii, takie jak na przykład harmonogram, lista organizatorów i uczestników, jak również ważne odniesienia w postaci linków. Ponadto, na stronie zawarte są przydatne dla użytkowników informacje na tematy dotyczące IT.

W celu poszerzenia wiedzy, czyli działania stanowiącego część inicjatywy na rzecz bezpieczeństwa informacji, wykorzystano różne kanały przekazywania informacji.

Grupy docelowe

Wybór grup docelowych został przeprowadzony według poziomu wiedzy społeczeństwa na temat bezpieczeństwa IT. Z raportu wynika możliwość podziału społeczeństwa na dwie grupy: jedna mała grupa, na którą składają się osoby o dużej wiedzy na temat bezpieczeństwa IT i jedna duża grupa, na którą składają się osoby o niewielkiej wiedzy na temat bezpieczeństwa IT:

- kobiety;
- osoby starsze (+60);
- osoby, które nie korzystają z IT codziennie.

Grupy docelowe to dzieci (10-16 lat), osoby starsze (+60 lat), kobiety i pracownicy.

Współpracujący partnerzy

Zorganizowanie kampanii było możliwe dzięki znacznej liczbie uczestników, którzy wnieśli swój wkład w kampanię w różny sposób. Uczestnicy kampanii mają prawo do używania logo kampanii (wspieramy kampanię net-safe now!), stworzonego na potrzeby promocji rozpoznawalnego wizerunku kampanii. Zamieszczenie logo kampanii na swojej stronie internetowej przez użytkowników oznacza jednocześnie zobowiązanie się do przestrzegania prostych zasad zawartych w kodeksie postępowania.

Współpracujący ze sobą partnerzy podzielili się na różne grupy o różnych zadaniach. Na ogół współpracujące ze sobą firmy są reprezentowane we wszystkich trzech grupach przez jedną osobę:

- Grupa robocza: Członkowie są na ogół pracownikami sektora IT i posiadają konkretną wiedzę na temat tego, o czym należy informować. Zadaniem tej grupy jest zorganizowanie działań, materiałów lub wydarzeń, jakie są realizowane podczas kampanii. Wszystkie działania muszą mieścić się w ramach kampanii net-safe now! Osoby należące do tej grupy wypełniają formularz zamieszczając swoje uwagi na temat strategii medialnej, wykorzystania zasobów i logistyki. Podpisując taki formularz członkowie zobowiązują się jednocześnie do przeprowadzenia działania.
- Grupa medialna: Członkowie tej grupy są najczęściej pracownikami działu PR lub komunikacji. Głównym zadaniem tej grupy jest dopilnowanie, aby kampania została przedstawiona w mediach. Grupa medialna odpowiada za kontakty z prasą, zamieszczanie komunikatów prasowych, artykułów, itd. Grupa ta miała swoje pierwsze spotkanie miesiąc wcześniej niż pozostałe dwie grupy. Celem tego spotkania było bardziej szczegółowe określenie grup docelowych i sposobu dotarcia do nich.
- Grupa nadzorująca: Członkowie tej grupy reprezentują najczęściej kadrę kierowniczą firm. Głównym celem tej grupy jest zatwierdzenie ogólnego przesłania, strategii komunikacji i strategii medialnej, jak również inicjatyw PR. Poniżej znajduje się wykaz uczestników

Strona internetowa kampanii to www.netsikkernu.dk

Ocena

W ramach kampanii zorganizowano 333 wydarzenia, przy czym 142 polegały na wizytach w duńskich szkołach, a 126 na kursach szkoleniowych skierowanych do osób starszych prowadzonych w ośrodkach przetwarzania danych.

Biuletyn kampanii „netsikker nu @visen” został wydany w 120 000 egzemplarzy. W biuletynie zamieszczono kilka artykułów skierowanych do różnych grup docelowych. Zrealizowano także spot filmowy (zatytułowany "Czy Klaus jest w domu?") przekazujący informacje na temat bezpieczeństwa IT w najbardziej przystępny sposób. Spot filmowy był duńską wersją niemieckiego spotu zatytułowanego „Wo ist Klaus?”. Biuletyn był

rozprowadzany za pośrednictwem współpracujących ze sobą partnerów i bibliotek, punktów handlowych TDC i oddziałów Nordea.

Spot filmowy był także rozpowszechniany za pośrednictwem współpracujących ze sobą partnerów i prezentowany na ogromnej ilości stron internetowych. Film został wyświetlony 100 568 razy.

Zarówno biuletyn, jak i spot filmowy były dostępne na stronie internetowej kampanii.

Wyprodukowano także serię materiałów:

- spot telewizyjny na temat przemocy w Internecie, w którym wystąpiła osoba znana między innymi z programów dla dzieci (Andrea Vagn Jensen); spot był wyświetlany trzy razy dziennie na dwóch różnych kanałach w okresie od 10 do 23 kwietnia;
- opaski na rękę z napisem www.netsikkernu.dk;
- film zrealizowany z uczestnictwem dzieci jako wynik projektu „Dzień Bezpiecznego Internetu”, który miał miejsce w lutym.

Pełna lista partnerów

Bornholms Erhvervsskole, Cyberhuset, DANSK IT, Dansk Metal, EA Vest, EUC Midt, EUC Nord, EUC Syd, Habbo Hotel, IT- og Telestyrelsen, ITB, ITEK/DI, Medierådet for børn og unge, Microsoft Danmark, Morgendagens heltinder, Niels Brock, Nordea, Odense tekniske skole, Parkegaard & Kristensen, PBS, Protego/PWC, Roskilde handelsskole, Syddansk universitet, TDC, TEC Ballerup, Uni-C, Vejle bibliotek, Vejle tekniske skole, Videnskabsministeriet, Vi Kvinder, Ældremobiliseringen.

Rząd jako partner przedsiębiorstw i przemysłu

Najnowsze programy i inicjatywy poszerzania wiedzy

W celu uzyskania informacji na temat kampanii Net-safe now! por. część [Rząd jako twórca](#).

Rząd jako partner społeczeństwa

Najnowsze programy i inicjatywy poszerzania wiedzy

W celu uzyskania informacji na temat kampanii Net-safe now! por. część [Rząd jako twórca](#)

Kampanie

SaferInternet - Danish network knowledge [Wiedza na temat sieci w Danii]¹⁰

Streszczenie

Procedury związane z bezpieczeństwem w Internecie, wiedza na temat korzystania przez dzieci z telefonów komórkowych i Internetu to niektóre tematy zawarte w harmonogramie prac krajowej sieci duńskiego punktu Awareness skupiającej zainteresowane podmioty. Na dzień dzisiejszy do sieci należy 22 członków.

Szczegóły

Od samego początku istnienia Sieci Insafe, której celem jest poszerzanie wiedzy na temat bezpieczeństwa, duński punkt Awareness (Media Council) funkcjonował jako krajowy ośrodek wiedzy na temat korzystania z Internetu i nowych technologii przez dzieci i młode osoby. Prowadził on dialog z duńskim sektorem przemysłu, z władzami publicznymi, uczelniami i organizacjami za pośrednictwem krajowej grupy skupiającej zainteresowane podmioty.

Regularnie organizowane spotkania i aktualizowanie informacji miało na celu stworzenie sieci służącej wymianie pomysłów, wiedzy, dobrych praktyk i procedur. Dzięki na przykład ogólnokrajowym broszurom zainteresowane podmioty są na bieżąco informowane na temat korzystania przez dzieci i młodzież z mediów. Biuletyn opiera się na informacjach uzyskanych od krajowych podmiotów zainteresowanych zagadnieniem i zawiera bezpośrednie odniesienie do stowarzyszenia Insafe.

Końcowym rezultatem były liczne inicjatywy i projekty poszerzające wiedzę opracowane przez współpracujące ze sobą różne zainteresowane podmioty. Stowarzyszenie „The Youth Ring” skupiające około 1 200 ośrodków prowadzących zajęcia pozaszkolne dla dzieci i klubów dla dzieci i młodzieży w wieku 10-18 lat jest członkiem sieci od 2004 r. Flemming Moestrup, doradca stowarzyszenia, podkreśla korzyści jakie „The Youth Ring” wniosło z przynależności do grupy: „Otrzymywanie informacji i materiałów dydaktycznych, jak również uzyskiwanie informacji na temat partnerów działających na naszym obszarze miało dla nas bardzo duże znaczenie i było bardzo przydatne dla naszych członków” mówi Flemming Moestrup.

Przedstawia on konkretne wyniki uzyskane przez sieć, podając jako przykład „the Youth Ring”: „Wskazaliśmy zasoby, za których pośrednictwem możliwe było przekazanie wyników badań przeprowadzonych przez Media Council i zalecenia dotyczące korzystania z gier komputerowych przez dzieci i młodzież oraz na temat zachowania się przy korzystaniu z Internetu. Aktualnie jest to najpotrzebniejsza usługa w sekretariacie.

¹⁰ <http://www.saferinternet.org/www/en/pub/insafe/news/articles/0706/dk.htm> , 3 sierpnia 2006 r..

Ścisłe współpracujemy także z wieloma partnerami grupy – jest to możliwość, którą zaproponowała grupa zainteresowanych podmiotów.”

6. Estonia

Na podstawie odpowiedzi na kwestionariusz i dodatkowych informacji z przeprowadzonych wywiadów, badań i dodatkowych materiałów wyszczególniono dla Estonii następujące części:

[Rząd jako twórca prawnych, regulacyjnych i instytucjonalnych postanowień służących poszerzaniu wiedzy](#)

[Władze państwowe jako użytkownik systemów informacyjnych](#)

[Władze lokalne jako użytkownik systemów informacyjnych](#)

[Rząd jako partner przedsiębiorstw i przemysłu](#)

[Rząd jako partner społeczeństwa](#)

[Statystyki i kluczowe wskaźniki wydajności \(KPI\)](#)

Rząd jako twórca prawnych, regulacyjnych i instytucjonalnych postanowień służących poszerzaniu wiedzy

Krajowa strategia poszerzania wiedzy

Estońskie Ministerstwo Gospodarki i Łączności opracowało ogólnokrajową politykę związaną z bezpieczeństwem informacji, która określa inicjatywy związane z e-bezpieczeństwem i zajmuje się koordynacją między estońskimi organizacjami rządowymi. Prace w kierunku harmonizacji estońskiej polityki bezpieczeństwa informacji są prowadzone w różnych ministerstwach. Polityka wymaga zastosowania opracowywanej strategii bezpieczeństwa informacji.

Głównym celem estońskiej polityki bezpieczeństwa informacji jest stworzenie bezpiecznego i świadomego kwestii związanych z bezpieczeństwem estońskiego społeczeństwa informacyjnego. Do szczególnych celów należy usunięcie niemożliwych do zaakceptowania zagrożeń, obrona praw człowieka, poszerzanie wiedzy na temat bezpieczeństwa informacji i szkolenia, jak również zapewnienie konkurencyjności gospodarki.

Polityka obejmuje pięć dziedzin. Estońskie Ministerstwo Gospodarki i Łączności (MEAC) koordynuje współpracę i koordynację bezpieczeństwa. Dziedzina ta obejmuje inicjatywy, takie jak koordynowanie estońskiej analizy ryzyka środowiskowego ITC, utworzenie i prowadzenie estońskiego zespołu ds. reagowania na przypadki naruszenia bezpieczeństwa teleinformatycznego CERT (Computer Emergency Response Team),

uczestnictwo w działaniach ENISA (Europejska Agencja Bezpieczeństwa Sieci i Informacji) i koordynowanie inicjatyw międzynarodowych.

Dziedziną zarządzania kryzysowego i cyberprzestępczości zajmuje się Ministerstwo Spraw Wewnętrznych wraz z Ministerstwem Obrony. Dziedzina ta obejmuje opracowanie krajowego planu zarządzania kryzysowego, koordynowanie prac krajowych i lokalnych komitetów kryzysowych, jak również koordynowanie inicjatyw związanych z międzynarodową cyberprzestępczością.

Bezpieczna e-administracja musi opierać się na odpowiednim ustawodawstwie i procedurach, takich jak wymogi bezpieczeństwa dotyczące baz danych, usług i zamówień państwowych. Regulacje w tej dziedzinie są koordynowane przez MEAC i Ministerstwo Spraw Wewnętrznych.

Zarówno ludzie, jak i zasoby muszą być chronieni podczas korzystania z aplikacji e-administracji. Zadania związane z koordynacją e-bezpieczeństwa w ramach aplikacji, takie jak rozpowszechnianie rozwiązań w zakresie kart identyfikacyjnych i korzystanie z sieci TESTA (Trans European Services for Telematics between Administrations - system teleinformatyczny służący wymianie danych między władzami państw europejskich) są prowadzone w ramach programu działającego w tej domenie. Domena ta jest przypisana Ministerstwu Spraw Wewnętrznych i Ministerstwu Obrony.

W celu wdrożenia polityki bezpieczeństwa informacji, MEAC co roku koordynuje opracowywanie i przyjmowanie rocznego planu działania na rzecz estońskiej polityki informacji i bezpieczeństwa.

Bardziej szczegółowe informacje znajdują się w poniżej zamieszczonych publikacjach:

- komunikaty prasowe wydawane przez estońskie Ministerstwo Gospodarki i Łączności;
- Zasady estońskiej polityki informacji 2004-2006;
- IT w administracji publicznej w Estonii 2005.

Prawne, regulacyjne i instytucjonalne postanowienia służące poszerzaniu wiedzy

Zgodnie z polityką bezpieczeństwa informacji, Ministerstwo Edukacji i Nauki, Ministerstwo Obrony, Ministerstwo Gospodarki i Łączności oraz Kancelaria Stanu są odpowiedzialne za edukację i szkolenia. Przewidziane inicjatywy to działania PR, szkolenia, informacyjne strony internetowe, współpraca ze szkołami (wyższymi) i badanie poziomu zadowolenia społecznego.

Ustawa o ochronie danych została przyjęta przez parlament 12 czerwca 1996 r. Celem ustawy jest ochrona podstawowych praw i wolności osób fizycznych w odniesieniu do przetwarzania danych osobowych i zgodnie z prawem osób fizycznych

do bezpłatnego otrzymywania wszelkich informacji, które są rozpowszechniane publicznie.

Ochrona danych osobowych jest gwarantowana ze względu na fakt, że administratorzy danych i upoważnione podmioty przetwarzające mogą przetwarzać dane osobowe tylko dla celów i na warunkach, które zostały określone w ustawie o ochronie danych. Osoby fizyczne mają prawo do wyrażenia zgody na przetwarzanie danych ich dotyczących, do otrzymania informacji na temat przetwarzania i do odmowy przyznania zgody na przetwarzanie danych osobowych, które ich dotyczą.

Ustawa o ochronie danych osobowych dzieli dane osobowe na dwie grupy: dane szczególnie chronione i dane niepodlegające szczególnej ochronie. Dane szczególnie chronione to takie dane, które dotyczą poglądów politycznych, przekonań religijnych lub filozoficznych, pochodzenia rasowego lub etnicznego, stanu zdrowia osoby fizycznej, życia seksualnego oraz wyroków skazujących, nałożonych sankcji i udziału w postępowaniu karnym.

Przetwarzanie danych osobowych niepodlegających szczególnej ochronie jest możliwe bez zgody osoby, której te dane dotyczą, jeżeli prowadzone jest zgodnie z postanowieniami Ustawy o ochronie danych. Dane szczególnie chronione natomiast mogą być przetwarzane tylko za zgodą osoby, której dane dotyczą, chyba, że ustawa stanowi inaczej.

Przetworzone dane osobowe są chronione za pomocą środków organizacyjnych lub technicznych, co musi być udokumentowane. Administratorzy danych mają obowiązek rejestrowania operacji przetwarzania danych szczególnie chronionych w organie ochrony danych, czyli Departamencie Ochrony Danych w Ministerstwie Spraw Wewnętrznych. Komitet prawny Parlamentu sprawuje nadzór nad Organem ochrony danych osobowych.

Pozostałe ustawodawstwo IT zawiera między innymi następujące ustawy:

- Ustawa o elektronicznych podpisach;
- Ustawa o bazach danych;
- Ustawa o archiwach;
- Ustawa o tajemnicach państwowych;
- Ustawa o oficjalnych statystykach;
- Ustawa o zamówieniach publicznych;
- Ustawa o łączności elektronicznej;
- Ustawa o informacji publicznej;
- Ustawa o ochronie konsumentów;
- Uchwalenie ustawy w sprawie elektronicznych podpisów w Estonii;
- Zasady estońskiej polityki informacji;

Estonia przewodniczyła programowi współpracy państw bałtyckich w zakresie budowy społeczeństwa informacyjnego i rozwoju technologii informatycznych „Northern eDimension eSecurity Action Line”, na którą składają się następujące dziedziny: badanie i wymiana dobrych praktyk w sieci i bezpieczeństwo infrastruktury informacyjnej; współpraca dotycząca podpisu elektronicznego; bezpieczna wymiana danych między krajowymi rejestrami ludności.

Przygotowano wiele seminariów, prezentacji, artykułów i propozycji projektów dotyczących e-bezpieczeństwa: przykłady projektów z zakresu e-administracji „A Population-Wide ID card (Estonia)” (karta identyfikacyjna dla całego społeczeństwa) i „Special citizens web portal with Standard DB-services”(specjalny portal dla obywateli na temat standardowych usług DB) są dostępne w basie danych serwisu systemu dobrych praktyk e-administracji, *eGovernment Good Practice Framework* (<http://www.egov-goodpractice.org>).

Władze państwowe jako użytkownik systemów informacyjnych

Najnowsze programy i inicjatywy poszerzania wiedzy

Zarówno ludzie, jak i zasoby muszą być chronieni podczas korzystania z aplikacji e-administracji. Zadania związane z koordynacją e-bezpieczeństwa w ramach aplikacji, takie jak rozpowszechnianie rozwiązań w zakresie kart identyfikacyjnych i korzystanie z sieci TESTA (Trans European Services for Telematics between Administrations - system teleinformatyczny służący wymianie danych między władzami państw europejskich) są prowadzone w ramach programu działającego w ramach tej domeny. Domena ta jest przypisana do Ministerstwa Spraw Wewnętrznych i Ministerstwa Obrony.

Władze lokalne jako użytkownik systemów informacyjnych

Najnowsze programy i inicjatywy poszerzania wiedzy

Nie było odrębnego programu poszerzania wiedzy na temat bezpieczeństwa skierowanego do użytkowników systemów władzy lokalnej.

Rząd jako partner przedsiębiorstw i przemysłu

Małe i średnie przedsiębiorstwa (MŚP)

Duży wpływ na poszerzenie wiedzy na temat bezpieczeństwa informacji mają standardy i publikacje dotyczące bezpieczeństwa informacji. Publikacje te są dostępne w języku estońskim. Oto niektóre przykłady:

- ISO/IEC 17799:2003 Technika informatyczna - Praktyczne zasady zarządzania bezpieczeństwem informacji;
- EVS-ISO/IEC TR 13335:1999 Technika informatyczna – Wytyczne dotyczące zarządzania bezpieczeństwem IT (1-5);

- COBIT zarządzanie, nadzór i audyt systemów informatycznych i związanych z nimi technologii; Trzecia edycja. Stowarzyszenie ds. audytu i kontroli systemów informatycznych, Rolling Meadows, USA;
- ISO TR 13569 Bankowość i związane usługi finansowe. Wskazówki dotyczące zabezpieczania informacji;
- ISO/IEC 90003, projektowanie oprogramowania — wytyczne w sprawie stosowania ISO 9001:2000 do oprogramowania komputerowego;
- EVS-ISO/IEC 12207:1998 Technika informatyczna - cykle życia w tworzeniu oprogramowania;
- ISO/IEC TR 15271:1998 Wytyczne w sprawie ISO/IEC 12207 (cykle życia w tworzeniu oprogramowania).

Ponadto planowano utworzenie specjalnej strony internetowej na temat bezpieczeństwa IT, która będzie skupiała się na zagadnieniach dotyczących poszerzania wiedzy na temat bezpieczeństwa, w tym także tych, które dotyczą MŚP.

Dostawcy usług internetowych (ISP)

Nie było odrębnego programu poszerzania wiedzy na temat bezpieczeństwa skierowanego do klientów różnych ISP w Estonii. Planuje się przeprowadzenie kampanii i działań mających na celu poszerzenie wiedzy wśród użytkowników Internetu.

Media

Należy zwrócić uwagę, że poniżej wskazany przykład wykorzystuje media jako kanał dotarcia do innych grup docelowych, i nie przedstawia ich jako odrębnej grupy docelowej.

Nie było odrębnej kampanii na temat poszerzania wiedzy na temat bezpieczeństwa w mediach, której celem byłoby promowanie kultury bezpieczeństwa. Gazety i czasopisma często publikują różne artykuły promujące kulturę bezpieczeństwa. Większość z nich dotyczy specjalnych e-usług lub produktów; na przykład: jak korzystać z kart identyfikacyjnych, jak bezpiecznie korzystać z usług świadczonych w ramach e-handlu, jak chronić prywatnych użytkowników komputerów prywatnych, jak chronić użytkowników sieci WiFi, itd.

Partnerstwo publiczno-prywatne

Skuteczne partnerstwo publiczno-prywatne (w dziedzinie poszerzania wiedzy i edukacji/szkolenia)

Projekt „Look at world” był prowadzony kilka lat temu. Jednym z celów projektu było poszerzenie wiedzy na temat komputerów i rozwinięcie umiejętności użytkowników końcowych, promując korzystanie z e-usług wśród użytkowników końcowych.

Przyszłe partnerstwa publiczno-prywatne

Poddano analizie możliwość ustanowienia partnerstwo publiczno-prywatnych w przyszłości. Dotychczas nie przeprowadzono jeszcze żadnego działania.

Rząd jako partner społeczeństwa

Najnowsze programy i inicjatywy poszerzania wiedzy

Estonia była uczestnikiem blogathonu zorganizowanego w ramach Dnia Bezpiecznego Internetu 7 lutego 2006 r.

Istnieją plany dotyczące utworzenia specjalnej strony internetowej na temat bezpieczeństwa IT, która będzie skupiała się na zagadnieniach dotyczących poszerzania wiedzy na temat bezpieczeństwa wśród użytkowników prywatnych.

Partnerstwo publiczno-prywatne

Skuteczne partnerstwo publiczno-prywatne (w dziedzinie poszerzania wiedzy i edukacji/szkolenia)

Projekt „Look at world” był prowadzony kilka lat temu. Jednym z celów projektu było poszerzenie wiedzy na temat komputerów i rozwinięcie umiejętności użytkowników końcowych, promując korzystanie z e-usług wśród użytkowników końcowych.

Statystyki i kluczowe wskaźniki wydajności (KPI)

Statystyki/KPI do oceny skuteczności inicjatywy poszerzania wiedzy

Żadne kluczowe wskaźniki wydajności służące do pomiarów skuteczności inicjatyw dotyczących poszerzania wiedzy nie zostały opracowane ani wdrożone.

Znaczenie statystyk/KPI

Znaczenie statystyk zostało uznane, ponieważ dają one możliwość porównania wiedzy na temat bezpieczeństwa, która dzięki różnym kampaniom zwiększyła się. Jednak polecenie konkretnej strategicznej metody służącej pomiarom skuteczności kampanii jest trudnym zadaniem. W rzeczywistości zależy to od samej kampanii, od tego w jaki sposób została zorganizowana i do kogo była skierowana.

7. Finlandia

Na podstawie odpowiedzi na kwestionariusz oraz informacji uzupełniających z przeprowadzonych rozmów, badań i dodatkowych materiałów dla Finlandii wyszczególniono następujące części:

[Rząd jako partner przedsiębiorstw i przemysłu](#)

[Rząd jako partner społeczeństwa](#)

[Kampanie](#)

Rząd jako partner przedsiębiorstw i przemysłu

Małe i średnie przedsiębiorstwa (MŚP)

Projekt Krajowego Dnia Bezpieczeństwa Informacji 2006 dostarcza informacji na temat bezpiecznego korzystania z Internetu MŚP w rozumieniu definicji Pakietu informacji ENISA 2005. Głównym celem projektu jest obrazowe przedstawienie tego, czym dla MŚP jest bezpieczeństwo informacji. Uwzględniono następujące obszary: definicję bezpieczeństwa informacji, analizę ryzyka, plan dotyczący bezpieczeństwa informacji dla MŚP, bezpieczne korzystanie z ICT na co dzień.

Projekt, którego realizację rozpoczęto w lutym 2006 r., jest rodzajem usługi on-line skierowanej do MŚP (www.tietoturvaopas.fi). Usługi on-line mają charakter wskazówek i są skierowane głównie do tych MŚP, które jeszcze nie korzystają z wszechstronnego operacyjnego systemu bezpieczeństwa informacji. Na stronie internetowej znajduje się wiele praktycznych narzędzi przeznaczonych zarówno dla pracodawców, jak i pracowników MŚP. Krajowy Dzień Bezpieczeństwa Informacji 2006 jest jednym z pierwszych projektów rządowego Komitetu ds. bezpieczeństwa informacji. Projekt został przygotowany przez administrację publiczną, podmioty ze świata biznesu i różne zainteresowane stowarzyszenia i organizacje.

Partnerstwo publiczno-prywatne

Skuteczne partnerstwo publiczno-prywatne (w dziedzinie poszerzania wiedzy i edukacji/szkolenia)

Projekt Krajowego Dnia Bezpieczeństwa Informacji 2006 jest szeroko zakrojonym projektem komunikacyjnym mającym na celu poszerzenie wiedzy na temat bezpieczeństwa informacji. Dla potrzeb projektu współpracuje ze sobą około 30 organizacji. W projekcie uczestniczyły przedstawicielstwa administracji publicznej, podmiotów ze świata biznesu i różnych zainteresowanych stowarzyszeń i organizacji. Krajowy Dzień Bezpieczeństwa Informacji 2005 jest jednym z pierwszych projektów rządowego Komitetu ds. bezpieczeństwa informacji. Grupami docelowymi tego projektu,

którego celem jest poszerzanie wiedzy, są dzieci w wieku szkolnym, MŚP i prywatni użytkownicy Internetu.

W partnerstwo publiczno-prywatne zaangażowane były następujące organizacje: Aina Group, Główna Izba Gospodarcza Finlandii, Federacja fińskich przedsiębiorców, D-Fence, Elisa, Finnet Union, Fińska Grupa Użytkowników Macintosha FiMUG, F-Secure, Hewlett-Packard, Stowarzyszenie Władz Regionalnych i Lokalnych, Agencja konsumentów, Ministerstwo Finansów, Ministerstwo Edukacji, Ministerstwo Handlu i Przemysłu, Ministerstwo Transportu i Łączności, Liga na rzecz dzieci im. Mannerheima, Microsoft, Krajowa Agencja Dostaw w Sytuacjach Nadzwyczajnych, Krajowa Rada ds. Edukacji, Panda Software Finland, Ośrodek Ewidencji Ludności, Save the Children, TeliaSonera Finland, TIEKE, Fińska Federacja ds. Komunikacji i Teleinformatyki FiCom, Biuro Rzecznika Ochrony Danych Osobowych, Fińskie Stowarzyszenie ds. Bezpieczeństwa Informacji, Program dot. Społeczeństwa informacyjnego, Fiński Regulator Rynku Telekomunikacyjnego, VTT Ośrodek badań Technicznych w Finlandii.

Projekt jest finansowany przez wymienione powyżej ministerstwa i podmioty ze świata biznesu. Różne zainteresowane organizacje wnoszą swój wkład do projektu w postaci wiedzy. Wszystkie organizacje mają swoich przedstawicieli w grupach roboczych, które przygotowują informacje i opracowują materiały dla potrzeb usług świadczonych on-line, jak również planują i przeprowadzają kampanie w mediach.

W ciągu ostatnich trzech lat partnerstwo publiczno-prywatne wykazało się dobrą pracą. Dzięki takiemu rodzajowi współpracy wielu organizacji projekt charakteryzuje wszechstronne podejście do tematu i możliwość dotarcia do szerokiego grona odbiorców należących do grup docelowych.

Rząd jako partner społeczeństwa

Najnowsze programy i inicjatywy poszerzania wiedzy

Projekt Krajowego Dnia Bezpieczeństwa Informacji 2006 jest szeroko zakrojonym projektem komunikacyjnym mającym na celu poszerzenie wiedzy na temat bezpieczeństwa informacji. Dla potrzeb projektu współpracuje ze sobą około 30 organizacji. W projekcie uczestniczyły przedstawicielstwa administracji publicznej, podmiotów ze świata biznesu i różnych zainteresowanych stowarzyszeń i organizacji. Krajowy Dzień Bezpieczeństwa Informacji 2005 jest jednym z pierwszych projektów rządowego Komitetu ds. bezpieczeństwa informacji. Grupami docelowymi tego projektu, którego celem jest poszerzanie wiedzy, są dzieci w wieku szkolnym, MŚP i prywatni użytkownicy Internetu.

Użytkownicy prywatni byli grupą docelową projektu przez ostatnie trzy lata. W ciągu tego czasu przeprowadzonych zostało kilka działań. W roku 2004 do ponad jednego miliona mieszkań w Finlandii dostarczono poradnik na temat bezpiecznego korzystania

z Internetu w domu (Joka Kodin Tietoturvaopas) i uruchomiono stronę internetową (www.tietoturvaopas.fi). Od tego czasu strona ta jest regularnie uaktualniana.

Na stronie znajdują się głównie informacje na temat tego, jak chronić komputer przed złośliwymi programami i spamem, jak bezpiecznie korzystać z usług on-line, jak chronić prywatność w Internecie, jak bezpiecznie korzystać z różnych połączeń on-line, przedstawione są opisy zagrożeń występujących w Internecie i sposobów ochrony przed nimi.

Temat bezpiecznego korzystania z Internetu był przedmiotem ogólnokrajowej debaty podczas Dnia Bezpieczeństwa Informacji zorganizowanego w ramach Krajowego Projektu Dnia bezpieczeństwa Informacji. Do użytkowników prywatnych docierano za pośrednictwem wiadomości, komunikatów prasowych, reklam w telewizji, gazet, magazynów i Internetu.

Kampanie

SaferInternet – Good practice in Finnish (Dobra praktyka po fińsku (artykuł))¹¹

Streszczenie

W Finlandii do dobrych praktyk dotyczących bezpieczeństwa Internetu zalicza się podręcznik Hiiripiiri, Dzień Bezpiecznego Internetu, komiksy dla dzieci i współpracę z dostawcami treści.

Szczegóły

Hiiripiiri, publikacja na temat bezpieczeństwa w mediach: w 2004 r. 4 000 dzieci w fińskich szkołach otrzymało publikację zatytułowaną Hiiripiiri na temat bezpieczeństwa w Internecie i mediach.

Celem Hiiripiiri jest zbudowanie szeroko zakrojonej sieci angażującej osoby uczące się, nauczycieli, ekspertów i zainteresowane podmioty. Dzieci zbierają tak zwane „Myszkopunkty” w celu uzyskania tytułu i dyplomu „Doktora Myszki”. Praca dzieci związana z Hiiripiiri, informacje na temat zadań i nowy materiał opracowany przez ośrodki opieki dziennej będą dostępne na stronie internetowej Hiiripiiri: <http://www.pelastakaalapset.fi/hiiripiiri/>

Fiński Dzień Bezpiecznego Internetu skierowany jest do szkół:

Fiński Dzień Bezpiecznego Internetu jest częścią politycznego programu fińskiego rządu angażującego prawie wszystkie ministerstwa, związki współpracy przemysłowej,

¹¹ <http://www.saferinternet.org/www/en/pub/insafe/news/articles/0706/fi.htm> , 31 lipca 2006 r.

organizacje pozarządowe i, w tym roku, także fińskie organizacje handlu i bankowości. Koszty tej inicjatywy zostaną podzielone między największych ISP i producentów oprogramowania, jak również rząd. To corocznie organizowane wydarzenie zawsze będzie skierowane do szkół i dzieci.

Komiksy i opowiadania dla dzieci i młodzieży:

Strona internetowa www.tietoturvakoulu.fi, wspierająca inicjatywę bezpiecznego Internetu, została rozbudowana i uaktualniona na podstawie informacji zwrotnych otrzymanych od użytkowników. Zamieszczono dwa nowe opowiadania w formie komiksów, celem zwrócenia uwagi na trzy podstawowe elementy dotyczące bezpiecznego korzystania z Internetu: przestrzeganie zasad, ochrona własnej osoby i zabezpieczenia komputera:

- Nowi przyjaciele Ani jest skierowane do najmłodszych dzieci w wieku szkolnym i porusza problematykę dotyczącą publicznego charakteru Internetu, znaczenia prywatności, publikowania zdjęć i praw autorskich.
- Niefortunne wypadki i zdarzenia jest opowiadaniem skierowanym do starszych dzieci i zwraca uwagę na prawdziwą wartość informacji zamieszczonych w Internecie, zagadnienia dotyczące praw autorskich, odpowiedzialności oraz publikowania tekstów i zdjęć.

Opowiadania mogą być czytane indywidualnie, grupami lub razem z nauczycielami. Zawierają informacje na temat bezpieczeństwa i konkursów on-line sprawdzających poziom wiedzy na temat bezpieczeństwa informacji. Jak dotąd ponad 15 000 uczniów wzięło udział w konkursie i 80 % nauczycieli szkolnych odwiedziło stronę internetową.

Współpraca z dostawcami treści – idź tam, gdzie są dzieci! (go where the children are!):

Kwestionariusz „Głos dzieci” (Children’s voice) jest publikowany od czterech lat w maju. Dzięki współpracy z dostawcami treści, fińskie ośrodki uzyskały bezpłatną przestrzeń w Internecie na ich stronach internetowych, jak również wsparcie służące osiągnięciu celów i prowadzeniu prac. Kwestionariusz jest dostępny na stronie internetowej:

<http://www.pelastakaalapset.fi/nettivihje/english/>

8. Francja

Na podstawie odpowiedzi na kwestionariusz oraz informacji uzupełniających z przeprowadzonych rozmów, badań i dodatkowych materiałów dla Francji wyszczególniono następujące części:

[Rząd jako twórca prawnych, regulacyjnych i instytucjonalnych uregulowań służących poszerzaniu wiedzy](#)

[Rząd jako partner społeczeństwa](#)

Rząd jako twórca prawnych, regulacyjnych i instytucjonalnych postanowień służących poszerzaniu wiedzy

Krajowa strategia poszerzania wiedzy

W celu uzyskania informacji na temat kampanii mających na celu poszerzenie wiedzy skierowanych do młodzieży i rodziców por. część [Rząd jako partner \(społeczeństwa\)](#).

Rząd jako partner społeczeństwa

Najnowsze programy i inicjatywy poszerzania wiedzy

Kampania francuskiego Ministerstwa ds. Rodziny (F@mille en ligne: “Sur internet, la securite ca commence aussi par vous”)

Grupa robocza na Konferencji w sprawie rodziny

Na wniosek ministra ds. rodziny utworzono grupę roboczą, której zadaniem było przygotowanie Konferencji w sprawie rodziny 2005. Grupa ta w ciągu trzech miesięcy raz w tygodniu organizowała spotkania wszystkich zainteresowanych podmiotów na temat ochrony dzieci w Internecie: ministerstw (ds. Rodziny, Spraw Wewnętrznych, Sprawiedliwości, Przemysłu, Edukacji, Młodzieży i Sportu), stowarzyszeń na rzecz rodziny (association du mouvement familial), stowarzyszeń na rzecz dzieci (association de protection de l'enfance), związków i osób zajmujących się Internetem (dostawcy dostępu do Internetu, edytorzy treści, programiści, operatorzy sieci telefonii komórkowej, itd.). W pracach grupy uczestniczyli również eksperci, w tym lekarze, psychiatrzy dziecięcy, nauczyciele akademicy, dziennikarze prasy specjalistycznej i przedstawiciele francuskich władz ds. radiofonii i telewizji (Conseil supérieur de l'audiovisuel), francuski organ ochrony danych osobowych (La Commission nationale de l'informatique et libertés) i forum praw w Internecie (Forum des droits sur l'Internet).

Grupie roboczej przewodniczył Joël THORAVALL, przewodniczący Krajowej komisji praw człowieka (Commission Nationale Consultative des Droits de l'Homme).

Cele tej grupy były następujące:

- Określenie sposobu korzystania z Internetu przez dzieci i ich zachowania, jak również wiedzy rodziców na temat korzystania przez dzieci z Internetu;
- Określenie potrzeb rodziny i oczekiwań związanych z tym zagadnieniem;
- Określenie narzędzi i koniecznych warunków niezbędnych do bezpiecznego korzystania z Internetu przez dzieci.

Grupa przekazała przygotowany przez siebie raport zatytułowany „Protection de l'enfant et usages de l'Internet” (Ochrona dziecka i korzystanie z Internetu) ministrowi ds. rodziny, Philippe BAS.

Po otrzymaniu takiego wstępnego dokumentu i zawartych w nim propozycji, Premier podczas Konferencji w sprawie rodziny, jaka odbyła się 22 września 2005 r. zapowiedział trzy działania mające na celu ochronę dzieci podczas korzystania z Internetu:

- skierowana do rodziców propozycja skutecznego i bezpłatnego oprogramowania do kontroli dostępu z możliwością aktualizacji;
- opracowanie oznaczeń, które umożliwiłyby rodzicom kontrolowanie treści w celu ochrony dzieci;
- kampania informacyjna skierowana do społeczeństwa, opierająca się na krótkich filmach przedstawiających rodzinę podczas korzystania z Internetu.

Kampania informacyjna na temat korzystania z Internetu skierowana do rodziców

Minister ds. rodziny zorganizował kampanię informacyjną skierowaną do społeczeństwa. Celem kampanii było przekazanie rodzicom informacji na temat potencjalnych zagrożeń, na jakie narażeni są małoletni korzystając z Internetu, jak również odpowiedzialnego korzystania z jego zasobów. Ministerstwo, w ramach programu „f@mille en ligne” przedstawiło serię dziesięciu filmów. Filmy przedstawiają doświadczenia rodziny związane z Internetem i tym, w jaki sposób jest ona informowana na temat różnych istniejących rozwiązań dotyczących bezpieczeństwa. Każdy z 45 sekundowych filmów był wyświetlany dwa razy dziennie na dwóch najpopularniejszych kanałach dla dzieci i młodzieży we Francji (TF1 i M6) w dniach od 15 maja do 2 czerwca 2006 r.

Ta krajowa kampania informacyjna na temat bezpieczeństwa informacji miała na celu promocję konstruktywnego i pozytywnego dialogu w rodzinach na temat Internetu, po to aby:

- poinformować rodziców o potencjalnych zagrożeniach wynikających z korzystania z Internetu przez ich dzieci;
- pokazać rodzinom, jak odpowiedzialnie korzystać z Internetu.

Przesłaniem kampanii było poinformowanie o tym, że „władze publiczne i ISP chcą zaproponować darmowe oprogramowanie do kontrowania dostępu do Internetu przez rodziców i ochrony rodziny”.

Kluczowym przesłaniem kampanii było hasło: „bezpieczeństwo w Internecie zależy od Ciebie”.

Badania wstępne

Zwrócono się do instytutu badania opinii publicznej *l'Institut Français d'Opinion Publique* z prośbą o przeprowadzenie sondażu, który pozwoliłby porównać wiedzę i świadomość rodziców na temat tego, co ich dzieci robią w Internecie z tym, co nastolatki same mówią o swoich działaniach w sieci.

Sondaż został podzielony na dwie części: „rodzice i korzystanie z Internetu przez ich dzieci” i „korzystanie z Internetu według nastolatków”. Badanie to pokazało w szczególności, że:

- podczas gdy 25 % nastolatków przyznaje, że robi zakupy przez Internet, 91 % pytanym rodziców twierdzi, że ich dzieci nigdy nie kupują przez sieć;
- 42 % nastolatków posiadających blog „nigdy” lub „rzadko” mówi o tym rodzicom;
- 38 % nastolatków „nigdy” lub „rzadko” mówi rodzicom o swojej działalności w Internecie; 69 % z nich uważa, że to „nie interesuje ich rodziców”;
- spośród 55 % nastolatków, którzy wiedzą, że domowy komputer jest wyposażony w oprogramowanie do kontroli rodzicielskiej, 20 % mówi, że takie oprogramowanie jest „skuteczne, ale łatwo go uniknąć”, a 6 % uważa je za „nieskuteczne”;
- 36 % nastolatków twierdzi, że mieli już więcej niż raz do czynienia z „szokującymi, agresywnymi lub pornograficznymi obrazami lub treściami w Internecie”;
- tylko 48 % z nich mówi o tym rodzicom;
- równoległe badanie grupy rodziców pokazało, że w lutym 2006 r. tylko 15 % domowych połączeń do Internetu było wyposażone w oprogramowanie do kontroli rodzicielskiej;
- pod koniec 2004 r. badanie instytutu CREDOC wykazało, że podczas gdy 75 % dzieci w wieku 11-17 lat przyznało, że „zna” techniczne środowisko Internetu, tylko 45 % rodziców podało podobną odpowiedź.

Grupy docelowe kampanii

Grupy docelowe kampanii „f@mille en ligne” to: ogół społeczeństwa, rodzice małych dzieci i nastolatków surfujących po sieci, nastolatki w wieku 11 – 17 lat.

Zasada działania

Na zasadzie subiektywnej kamery (widz znajduje się „wewnątrz” ekranu komputerowego) można zobaczyć członków rodziny korzystających z Internetu. Dzięki doświadczeniom, w których ci ostatni biorą udział, można przyjrzeć się różnym kwestiom, takim jak:

- ochrona danych osobowych i bankowych;
- blokowanie niechcianych stron internetowych i poczty;
- obserwowanie uzależnienia od gier itd.;

Kampania zachęca rodziców do kontrolowania dzieci.

Wykorzystywane kanały

- Transmisje telewizyjne i radiowe (TF1, M6); 45 sekundowe filmy nadawane tuż przed wiadomościami. Informacje na temat wszystkich filmików znajdują się na końcu tej części.
- Strony internetowe zaangażowanych ministerstw: Urząd Premiera, Ministerstwo Rodziny, Przemysłu, Edukacji Narodowej, Spraw Wewnętrznych, Sprawiedliwości, Młodzieży i Sportów; bannery z logo kampanii z linkami do strony Ministerstwa Rodziny.
- Strony internetowe prywatnych partnerów (ISP – sygnatariusze porozumienia z 16 listopada): bannery z logo kampanii z linkami do własnych stron informacyjnych na temat kampanii;

Rozpowszechnianie

W kwietniu ubiegłego roku ISP rozpoczęli kampanię mającą na celu poinformowanie o inicjatywie wszystkich swoich subskrybentów.

Wpływ

Aby ocenić wpływ tych filmików instytut badania opinii publicznej BVA przeprowadził badanie na reprezentatywnej próbie francuskiej populacji. BVA przepytiał 1007 osób w wieku, co najmniej 15 lat w czasie bezpośredniej rozmowy w ich miejscu zamieszkania.

Przebadani uważali, że kampania jest:

- słuszną (89 % uznało, że ważniejsze, "aby chronić nieletnich, którzy korzystają z Internetu");
- znaną (50% uznało, że kampania jest przeprowadzana z inicjatywy władz);
- docenioną (83 % rodziców powiedziało, że "doceniło" kampanię);

Kampania została również przeprowadzona na portalach ISP.

Ramy czasowe

Kampania została ogłoszona we wrześniu. Niektóre działania rozpoczęto zaraz potem (np. zaopatrzenie, projekt, zdjęcia), aby wprowadzić kampanię przed latem i by dopasować się do powiązanych projektów (tj. wydania oprogramowania do kontroli

rodzicielskiej w kwietniu i wprowadzenia etykiety rodzinnej we wrześniu-październiku). Tworzenie kampanii zajęło osiem miesięcy.

Budżet

Budżet kampanii to 1000000 € (zarezerwowane dla ministerstwa na realizację i nadawanie filmów) plus koszt banerów internetowych dla ministerstw i ISP.

Streszczenie 10 filmików (http://www.famille.gouv.fr/protoc_enfance/).

Odcinek 1: Le contrôle parental sur Internet (kontrola rodzicielska w Internecie) -

http://www.premier-ministre.gouv.fr/IMG/mpg/ep_1.mpg

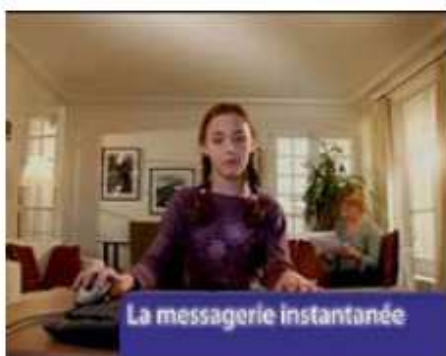


Tato właśnie zainstalował oprogramowanie do kontroli rodzicielskiej. Zgodnie z metodą zasugerowaną przez ISP i przed określeniem profili każdego z członków rodziny dyskutuje o tym z żoną i Chloé, dwunastoletnią córką. Zgadzają się co do celu, jakim jest możliwość posiadania ochrony dostosowanej do wieku ich dzieci.

Rady kampanii/funkcje oprogramowania:

definicja profili: „dzieci”, „nastolatki”, „dorośli”.

Odcinek 2: La messagerie instantanée (komunikator internetowy) - http://www.premier-ministre.gouv.fr/IMG/mpg/ep_2.mpg



Chloé korzysta z komunikatora. Nieznajomy chce, żeby dodała go do swojej listy kontaktów i przesyła jej wiadomość. Mama ostrzega ją: „W Internecie jak na ulicy – nie rozmawia się z nieznajomymi”.

Rady kampanii/funkcje oprogramowania:

kontrola działania, wybór dostarczanych informacji.

Odcinek 3: Les sites indésirables (niepożądane strony) - http://www.premier-ministre.gouv.fr/IMG/mpg/ep_3.mpg



Michel (tato) i jego syn Yann (17) szukają czegoś w Internecie. Yann otrzymuje wiadomość z linkiem do pedofilskiej strony. Michel proponuje synowi, aby powiadomił władze na stronie www.internet-mineurs.gouv.fr.

Rady kampanii/funkcje oprogramowania:
strony z czarnej i białej listy.

Odcinek 4: Le Blog (blog) - http://www.premier-ministre.gouv.fr/IMG/mpg/ep_4.mpg



W czasie aktualizowania swojego bloga Malika otrzymuje komentarz z linkiem do pornograficznej strony o tendencjach pedofilskich. Szuka rady u Yanna, swojego chłopaka, przed usunięciem linku. Decydują się powiadomić władze na stronie www.internet-mineurs.gouv.fr.

Rady kampanii/funkcje oprogramowania:
strony z czarnej i białej listy.

Odcinek 5: La sécurité des paiements (bezpieczeństwo płatności) - http://www.premier-ministre.gouv.fr/IMG/mpg/ep_5.mpg



Mama chce zamówić bilet przez Internet. Syn pomaga jej i pokazuje jej ikonę przedstawiającą kłódkę, która zapewnia bezpieczeństwo przy płatności.

Rady kampanii/funkcje oprogramowania:
możliwość wyboru dostarczanych informacji,
zastrzeżenie pewnych danych osobowych,
odnajdywanie numeru karty kredytowej.

Odcinek 6: L'achat en ligne (kupowanie przez Internet) - http://www.premier-ministre.gouv.fr/IMG/mpg/ep_6.mpg



Chloé, młodsza siostra, chce kupić produkt przez Internet. Prosi mamę o kartę kredytową. Rozmawiają o tym.

Rady kampanii/funkcje oprogramowania:

kontrola działania, blokowanie danych osobowych, odnajdywanie numeru karty kredytowej

Odcinek 7: Les données personnelles (dane osobowe) - http://www.premier-ministre.gouv.fr/IMG/mpg/ep_7.mpg



Starszy brat Yann właśnie stworzył bloga, gdy otrzymał reklamy na swoją komórkę. Tato tłumaczy mu, że nie musi podawać danych osobowych, żeby się zarejestrować i doradza mu przedstawienie wymyślonych danych.

Rady kampanii/funkcje oprogramowania:

Możliwość wyboru dostarczanych informacji, zastrzeżenie pewnych danych osobowych.

Odcinek 8: Le courrier indésirable (niepożądana poczta) - http://www.premier-ministre.gouv.fr/IMG/mpg/ep_8.mpg



Yann utworzył właśnie adres mailowy dla babci. Ona martwi się z powodu spamu. Jej wnuczek uruchamia funkcję antyspamową.

Rady kampanii/funkcje oprogramowania:

funkcja antyspamowa.

Odcinek 9: Chantage sur le net (szantaż przez Internet) - http://www.premier-ministre.gouv.fr/IMG/mpg/ep_9.mpg



Chloé czatuje z kolegą ze szkoły, którego prawie nie zna; ten prosi ją o przesłanie zdjęć w stroju kąpielowym; zmartwiona, mówi o wszystkim mamie... Ta tłumaczy jej zagrożenia, jakie niesie takie zachowanie.

Rady kampanii/funkcje oprogramowania:

blokowanie danych osobowych, nieprzesyłanie osobistych zdjęć nieznanym

Odcinek 10: La Dépendance au jeu (uzależnienie od gier) - http://www.premier-ministre.gouv.fr/IMG/mpg/ep_10.mpg



Yann gra w swoją ulubioną grę, a jego dziewczyna Malika nie może go od niej oderwać. Malika uważa, że spędza on za dużo czasu przed ekranem. Yann przegrywa w grze.

Wprowadzenie nowego hasła: kontrola działania ogranicza czas poświęcany na granie.

Projekt banneru wykorzystywany przez ISP i ministerstwa na portalach znajduje się w części Pliki Elektroniczne pod nazwą [banniere cegetel3.gif](#).

Okno zachęcające do instalacji oprogramowania do kontroli rodzicielskiej w czasie konfigurowania nowego połączenia do Internetu znajduje się w części Pliki Elektroniczne pod nazwą [neufkit2.jpg](#).

Partnerstwo publiczno-prywatne

Porozumienie między rządem a ISP

16 listopada 2005 r. w wyniku Konferencji na temat rodziny podpisano porozumienie między Ministerstwem, ISP (łącznie z AOL, Wanadoo, Alice / Telecom Italia, Noos-Numéricable, Club Internet / T-Online itd.) a stowarzyszeniami na rzecz dobra rodziny i dziecka. Informacje na temat porozumienia między francuskim rządem a ISP znajdują się w części Pliki Elektroniczne pod nazwą [accord afa famille avec logo.pdf](#).

Zobowiązania ISP

ISP zobowiązali się do zaproponowania swoim subskrybentom darmowego oprogramowania do kontroli rodzicielskiej zawierającego trzy profile dopasowane do wieku dziecka: „dziecko”, „nastolatek” i „dorosły”. Każdy profil otwierał lub ograniczał surfowanie po Internecie zgodnie z obiektywnymi kryteriami ochrony dziecka (na przykład żadnych szokujących treści dla profilu „dziecko”). System ten działa od kwietnia 2006 r.

„E-enfance” („E-dzieciństwo”), stowarzyszenie zajmujące się ochroną dziecka w Internecie przeprowadza sondaże i badania bezpośrednio z portalu ISP, sprawdzając czy ISP postępują zgodnie z porozumieniem.

Umowa między rządem a operatorami telefonii komórkowej

10 stycznia 2006 r. operatorzy telefonii komórkowej France Telecom, SFR i Bouygues Telecom podpisali umowę utworzoną przy współpracy z ministerstwem. Informacje o umowie między francuskim rządem a operatorami telefonii komórkowej w części Pliki Elektroniczne pod nazwą [charte d'engagements des op contenu multimédia-signée.pdf](#).

Zobowiązania operatorów telefonii komórkowej

Operatorzy telefonii komórkowej zgodzili się dostarczyć narzędzi do kontroli rodzicielskiej systematycznie i za darmo dla każdego nowego abonenta telefonii komórkowej od listopada 2005 r. Ponadto między kwietniem a październikiem 2006 r. obecni abonenci telefonii komórkowej otrzymają trzy wiadomości prezentujące nową bezpieczną usługę.

9. Niemcy

W przypadku Niemiec - na podstawie odpowiedzi na kwestionariusz i innych uzupełniających informacji z przeprowadzonych wywiadów, badań oraz na bazie dodatkowych materiałów – wyszczególniono następujące części:

[Rząd jako twórca prawnych, regulacyjnych i instytucjonalnych postanowień służących poszerzaniu wiedzy](#)

[Władze państwowe jako użytkownik systemów informacyjnych](#)

[Władze lokalne jako użytkownik systemów informacyjnych](#)

[Rząd jako partner przedsiębiorstw i przemysłu](#)

[Rząd jako partner społeczeństwa](#)

[Statystyki i kluczowe wskaźniki wydajności \(KPI\)](#)

Rząd jako twórca prawnych, regulacyjnych i instytucjonalnych postanowień służących poszerzaniu wiedzy

Krajowa strategia poszerzania wiedzy

Bezpieczeństwo IT jest integralną częścią niemieckiej strategii bezpieczeństwa krajowego.

Działania rządu federalnego skupiają się na różnych aspektach związanych z bezpieczeństwem informacji, wśród których poszerzanie wiedzy jest zasadniczym zagadnieniem.

W Federalnym Ministerstwie Spraw Wewnętrznych (*Bundesministerium des Innern*) rząd federalny wprowadził struktury konieczne ze względu na złożone wymagania technologii informacyjnej i technologii łączności na początkowym etapie.

Kolejny środek przyjęto na początku 2002 r., tworząc Zespół IT (Biuro urzędnika ds. Informacji), który zajmuje się kwestiami bezpieczeństwa IT.

Zakres odpowiedzialności rządu federalnego za bezpieczeństwo IT

Federalne Ministerstwo Spraw Wewnętrznych (BMI), a przede wszystkim jego Zespół IT (Biuro urzędnika ds. Informacji) są odpowiedzialne za bezpieczeństwo IT w rządzie federalnym.

Niemiecki Urząd Federalny ds. Bezpieczeństwa Informacji (BSI) podlega Federalnemu Ministerstwu Spraw Wewnętrznych.

Niemiecki Urząd Federalny ds. Bezpieczeństwa Informacji (BSI)

BSI centralnym oddziałem ds. Bezpieczeństwa IT rządu federalnego.

Dzięki ofercie obsługi informacji i usługom doradczym dla organów federalnych, producentów i użytkowników IT, urzędników ochrony danych, doradców w sprawach bezpieczeństwa, ekspertów, audytorów, instytutów badawczych i organizacji dostarczających standardów Urząd Federalny ds. Bezpieczeństwa Informacji w ogromnym stopniu przyczynia się do większego bezpieczeństwa IT.

Podczas gdy portal www.bsi.bund.de oferuje profesjonalnym użytkownikom wszelkiego rodzaju techniczne i specjalistyczne informacje, prywatni użytkownicy mogą znaleźć bardziej ogólne informacje na stronie www.bsifuer-buerger.de.

Praca Urzędu Federalnego ds. Bezpieczeństwa Informacji obecnie skupia się na pewnych zagadnieniach, takich jak na przykład: krytyczne infrastruktury informacyjne, Zespół reagujący na naruszenia bezpieczeństwa w Internecie (Computer Emergency Response Team) CERT-Bund, systemy wczesnego ostrzegania, zwiększanie wiedzy obywateli na temat kwestii związanych z bezpieczeństwem IT, bezpieczeństwo internetowe, zarządzanie bezpieczeństwem IT (IT-Grundschutz), złośliwe oprogramowanie, technologia trusted computing, tworzenie metod i produktów kryptograficznych, świadectwa, a następnie rozwój wspólnych kryteriów, bezpieczna e-administracja, podpis elektroniczny i biometria.

Nowy Krajowy Plan Ochrony Infrastruktury Informacyjnej

Aby zapewnić pełną ochronę infrastruktur informacyjnych w Niemczech, rząd federalny ustanowił trzy strategiczne cele w nowym Krajowym Planie Ochrony Infrastruktury Informacyjnej:

- zapobieganie: odpowiednia ochrona infrastruktur informacyjnych;
- gotowość: skuteczne reakcje na incydenty naruszenia bezpieczeństwa IT;
- zrównoważenie: zwiększanie niemieckiej konkurencyjności w bezpieczeństwie IT/tworzenie międzynarodowych standardów;

Cele te są dodatkiem do strategii IT rządu federalnego. Powstaną plany wykonawcze dla administracji federalnej i dla krytycznych infrastruktur, by zapewnić osiągnięcie tych celów. Po nich mogą pojawić się dodatkowe plany, jeśli będzie to konieczne.

Rosnące znaczenie infrastruktur informacyjnych wymaga wspólnego działania państwa, gospodarki i społeczeństwa. W ramach obecnego Krajowego Planu rząd federalny dba, aby zadania te zostały wypełnione.

Bezpieczeństwo IT w administracji federalnej

Administracja federalna sama obsługuje części krajowej infrastruktury informacyjnej. Obecny Krajowy Plan służy zagwarantowaniu średnio- i długookresowego bezpieczeństwa IT na wysokim poziomie. Dlatego rząd federalny określi szczegółowe wytyczne dotyczące ochrony infrastruktur informacyjnych administracji federalnej w planie wykonawczym dla administracji federalnej (Umsetzungsplan Bund).

Plan powinien określać wspólnie przygotowane techniczne, organizacyjne i proceduralne standardy dla administracji federalnej, które w elastyczny sposób i na własną odpowiedzialność powinny stosować ministerstwa.

Jako krajowy organ odpowiedzialny za bezpieczeństwo IT oraz jako główny dostawca usług w zakresie bezpieczeństwa IT rządu federalnego BSI jest odpowiedzialny za koordynowanie wykonywania tego Krajowego Planu. Aby umożliwić BSI spełnienie tego zadania powiększono i do pewnego stopnia nadal będzie się powiększać jego zespół, a priorytety zostaną ponownie określone; ogólnie BSI zostanie przypisana bardziej aktywna rola jako instytucji doradczej ds. bezpieczeństwa IT.

Współpraca między rządem federalnym a sektorem prywatnym

W Niemczech większość infrastruktur informacyjnych jest utrzymywana przez prywatne przedsiębiorstwa. Dlatego rząd federalny wzywa swoich partnerów z sektora prywatnego do wzięcia czynnego udziału w wykonywaniu Krajowego Planu.

W tym celu rząd federalny, razem z podmiotami krytycznych infrastruktur przygotowuje Plan Wykonawczy ramowy na rzecz konkurencyjności i innowacji (CIP, Umsetzungsplan KRITIS). Określi on środki znacznie podnoszące poziom bezpieczeństwa IT. BSI jak i inne właściwe organy publiczne będą oferowały swoją specjalistyczną wiedzę wspierając podmioty krytycznej infrastruktury we wprowadzaniu środków określonych w Planie Wykonawczym CIP.

Obywatele i społeczeństwo jako całość

Wszechstronna ochrona infrastruktur informacyjnych w Niemczech nie jest tylko zadaniem specjalistów od IT. Wymaga zaangażowania każdego – producentów produktów IT, dostawców usług, pracowników, osób odpowiedzialnych za kwestie związane z IT w państwowych organach i podmiotach prywatnych, a także tych, którzy korzystają z tych struktur.

Jako konsumenci obywatele coraz częściej korzystają z infrastruktur informacyjnych. Robiąc to dobrze poinformowani konsumenci wiedzą wiele na temat kwestii bezpieczeństwa i dlatego stawiają na godne zaufania produkty i procedury. Stąd zgodność z wysokimi standardami bezpieczeństwa jest również pozytywnym czynnikiem

ekonomicznym dla producentów, dystrybutorów i dostawców usług IT; jest to podstawa funkcjonowania rynku i schematów pojawiania się innowacji.

Celem rządu federalnego jest zachęcenie społeczeństwa do bardziej intensywnego wykorzystania istniejących informacji i informacji dostarczanych przez Krajowy Plan. Postępując zgodnie z zaleceniami rządowymi obywatele aktywnie przyczyniają się do bezpieczeństwa IT w Niemczech. Jednocześnie producenci i dystrybutorzy produktów i usług IT są zachęceni do jak najintensywniejszego uwzględniania bezpieczeństwa własnych produktów już w czasie ich tworzenia i odpowiedniego informowania swoich klientów o zagrożeniach związanych z IT i możliwych środkach ochronnych.

Poszerzanie wiedzy jako podstawowa kwestia bezpieczeństwa IT

Ryzyko naruszenia bezpieczeństwa można zmniejszyć poprzez rozpowszechnianie wiedzy o zagrożeniach i możliwościach ochrony, poprzez jasne rozdzielenie odpowiedzialności za sprawy bezpieczeństwa, wdrażanie środków bezpieczeństwa i stosowanie godnych zaufania produktów i procesów.

Poszerzyć wiedzę na temat ryzyka związanego ze stosowaniem IT

Rząd federalny pokłada nadal nadzieje w poszerzaniu wiedzy, informowaniu ogółu społeczeństwa i sektora handlowego o ryzyku stosowania IT. Z tego powodu rozpoczęto inicjatywy, które są skierowane do społeczeństwa na wszystkich poziomach, od zarządzania przedsiębiorstwem i publicznej administracji na wysokim szczeblu po zwykłych pracowników i osoby prywatne, takie jak użytkownicy komputerów osobistych.

Stosowanie bezpiecznych produktów i pewnych systemów IT

Rząd federalny wspiera stosowanie niezawodnych produktów i systemów IT, i zaufanych („trusted”) aplikacji bezpieczeństwa IT w Niemczech, przede wszystkim w obrębie administracji federalnej. Urząd Federalny ds. Bezpieczeństwa Informacji rozszerzy i zwiększy możliwość badania i oceny produktów i systemów IT pod względem bezpieczeństwa i wyda odpowiednie certyfikaty. BSI publikuje najlepsze praktyki, wyszczególnia produkty, które otrzymały niemiecki certyfikat bezpieczeństwa IT i publikuje techniczne wytyczne do stosowania tych produktów.

Sektor handlowy jest szczególnie świadomy ryzyka związanego z kradzieżą informacji (np. w wyniku szpiegostwa gospodarczego) oraz możliwości zapobiegania takim kradzieżom poprzez stosowanie niezawodnych, niemieckich produktów do kodowania i korzyści z niego.

Tworzenie podstawowych warunków i wytycznych

Rząd federalny podjął się wysiłku stworzenia odpowiednich podstawowych warunków i wytycznych, biorąc przy tym pod uwagę międzynarodowe normy i standardy, by zapewnić pełną ochronę we wszystkich obszarach związanych z bezpieczeństwem.

Każde ministerstwo federalne upewni się, czy standardy i wytyczne są wdrażane zgodnie z Umsetzungsplan Bund przez ministerstwo i wszystkie organy mu podlegające, na przykład poprzez utworzenie niezbędnych struktur (np. rzecznika bezpieczeństwa IT; sprawozdania, określenie roli i zakresu odpowiedzialności zarządu itd.).

Dla tych gałęzi gospodarki, gdzie stosuje się specjalne wymogi odnośnie do bezpieczeństwa IT zostaną stworzone odpowiednie wskazówki. Pozostała część społeczeństwa otrzyma zalecenia i wytyczne o bezpieczeństwie IT.

Identyfikowanie, rejestracja i ocena incydentów

Centrum reakcji na kryzysy IT w BSI, które jest obecnie tworzone, odegra rolę ośrodka krajowej kontroli i analiz, który będzie w stanie dostarczyć wiarygodnej oceny bieżącej sytuacji bezpieczeństwa IT w Niemczech w dowolnej chwili. Będzie też współpracował z innymi istniejącymi już, krajowymi i międzynarodowymi ośrodkami kryzysowymi w sprawie konkretnych incydentów. Aby umożliwić BSI pełnienie tej funkcji zostanie utworzona sieć czujników do wykrywania incydentów naruszania bezpieczeństwa IT.

Dodatkowe źródła dostarczające informacji na temat incydentów IT będą dostępne dla BSI dzięki poszerzeniu międzynarodowej sieci obserwacji i ostrzegania, której członkiem-założycielem był rząd federalny. Wszystkie te środki zapewnią, że odpowiedzialne organy sektora publicznego i do pewnego stopnia prywatnego będą posiadać informacje niezbędne do podejmowania szybkiej decyzji, jakie działania należy podjąć i jakie można podjąć.

Informowanie, powiadamianie i ostrzeganie

Właściwe organy federalne dostarczą informacji na temat bieżących zagrożeń i ryzyka, dopasowanych do pewnych grup docelowych. Wszyscy odpowiedzialni za systemy IT i infrastruktury informatyczne - od zwykłego, prywatnego użytkownika po administratora w firmach, organy publiczne i inne organizacje - będą mieli dostęp do odpowiednich informacji.

Powstanie system powiadamiania i ostrzegania, jako części krajowej koncepcji zarządzania kryzysem IT rządu federalnego, służący informowaniu wszystkich, których incydent może potencjalnie dotyczyć, w szybki i powszechny sposób o nadciągających atakach lub poważnych zakłóceniach infrastruktury informacyjnych. To pozwoli reagować w porę i zapobiegać uszkodzeniom na szeroką skalę.

Kwalifikacje w zakresie bezpieczeństwa IT w edukacji szkolnej i szkoleniach zawodowych

Rząd federalny korzysta z własnej fachowej wiedzy z zakresu bezpieczeństwa IT, by nadać rangę priorytetu bezpieczeństwu IT w edukacji szkolnej i szkoleniach zawodowych na szerszą skalę i by upewnić się, że bezpieczeństwo IT jest zapewnione dzięki skupieniu się na tworzeniu nowych zawodów, szkoleń i przedmiotów nauczania. Ponadto zwiększy się zakres usług informacyjnych dla obywateli, szkół, uniwersytetów, sektora handlowego i administracji publicznej i zostaną one ulepszone poprzez szerzenie wiedzy na temat bezpieczeństwa IT w obrębie społeczeństwa jako całości.

BSI ściśle współpracuje z instytucjami w Niemczech, które dostarczają materiałów do szkół i przedszkoli. Często zdarzało się, że bezpieczeństwo IT nie było częścią tych materiałów, które skupiały się bardziej na pedagogicznych aspektach tego zagadnienia. BSI doradza tym instytucjom, aby wprowadziły również techniczne aspekty bezpieczeństwa IT i pomaga im w realizacji tego pomysłu.

Prawne, regulacyjne i instytucjonalne postanowienia służące poszerzaniu wiedzy

Więcej informacji na początku części [Administracja jako twórca](#).

Władze państwowe jako użytkownik systemów informacyjnych

Najnowsze programy i inicjatywy poszerzania wiedzy

Więcej informacji w części [Administracja jako twórca](#) i [Administracja jako partner \(przedsiębiorstw\)](#).

Władze lokalne jako użytkownik systemów informacyjnych

Najnowsze programy i inicjatywy poszerzania wiedzy

Więcej informacji w części [Administracja jako twórca](#) (...) i [Administracja jako partner \(przedsiębiorstw\)](#).

Rząd jako partner przedsiębiorstw i przemysłu

Najnowsze programy i inicjatywy poszerzania wiedzy

Informacji i wytycznych dostarcza BSI.

Urząd federalny ds. Bezpieczeństwa Informacji zapewnia informacje i wytyczne zarówno dla profesjonalnych użytkowników, jak i obywateli na portalu www.bsi.bund.de.

W ramach serii publikacji Urzędu Federalnego ds. Bezpieczeństwa Informacji warto przyrzeć się następującym pozycjom:

- Podręcznik IT- Grundschrift / Narzędzie IT-Grundschrift / Wytyczne IT-Grundschrift / Przykładowe wytyczne;
- Podręcznik do e-administracji;

- Bezpieczne użytkowanie sprzętu telekomunikacyjnego;

Więcej informacji - pod adresem: www.bsi.de/literat/buanzg.htm.

Wykorzystane broszury to m. in.:

- "Drahtlose lokale Kommunikationssysteme und ihre Sicherheitsaspekte" („Radiowe, lokalne systemy przekazywania informacji i związane z nimi zagrożenia bezpieczeństwa”);
- "GSM-Mobilfunk - Gefährdungen und Sicherheitsmaßnahmen" („Łączność GSM – zagrożenia i środki bezpieczeństwa”);
- „Bluetooth – zagrożenia i środki bezpieczeństwa”
- "IT-Sicherheit Kompakt" (Krótki podręcznik na temat bezpieczeństwa IT);

Więcej informacji - pod adresem: www.bsi.de/literat/brosch.htm.

Wyniki badań i publikacje:

- Wyniki badań wtargnięć, wyniki kontroli bezpieczeństwa IT, wykrywanie naruszeń;
- Biometria, RFID, e-administracja, bezpieczeństwo aplikacji internetowych;

Więcej informacji pod adresem: www.bsi.de/literat/studien/index.htm i www.bsi.de/literat/index.htm.

Niektóre późniejsze inicjatywy, które zasługują na szczególną uwagę

IT-Grundschutz

Podręcznik IT-Grundschutz Urzędu Federalnego ds. Bezpieczeństwa Informacji opisuje standardowe środki bezpieczeństwa dla typowych aplikacji i systemów IT o normalnych potrzebach ochrony. Podręcznik ten zawiera:

- opis przyjętej sytuacji zagrożenia;
- szczegółowe opisy środków, które należy wdrożyć;
- opis procesu osiągania i utrzymania odpowiedniego poziomu bezpieczeństwa IT;
- prostą procedurę określania osiągniętego poziomu bezpieczeństwa IT poprzez porównanie go z wynikiem docelowym;

Wdrażanie zaleceń streszczonych w IT-Grundschutz jest również w szerszym znaczeniu warunkiem koniecznym dla systemów o dużej i największej potrzebie ochrony. Narzędzie IT- Grundschutz (narzędzie GS) wspierało rozwój koncepcji bezpieczeństwa. Od 2003 r. Urząd Federalny ds. Bezpieczeństwa Informacji proponował system wydawania certyfikatów zgodnie z procedurą IT-Grundschutz, która umożliwia weryfikację aktualnie osiągniętego poziomu bezpieczeństwa IT. Ponad 100 audytorów

zostało w międzyczasie upoważnionych przez Urząd Federalny ds. Bezpieczeństwa Informacji do kontroli na miejscu technicznego i organizacyjnego wdrażania IT-Grundschutz. Więcej informacji pod adresem: <http://www.bsi.bund.de/english/index.htm> (strona w języku angielskim).

Do podręcznika IT-Grundschutz opublikowano dodatek "Wytyczne w zakresie bezpieczeństwa IT" - wytyczne te zawierają zwięzły i ogólny opis najważniejszych środków bezpieczeństwa IT.

Wytyczne skupiają się na środkach organizacyjnych i praktycznych przykładach, by podkreślić potencjalne zagrożenia. Więcej informacji pod adresem: www.bsi.de/english/gshb/guidelines/index.htm (strona w języku angielskim).

W związku z silnym zapotrzebowaniem na poprawne pojmowanie bezpieczeństwa IT w 2004 r. opublikowano "przykładowe wytyczne i pojęcia". Planuje się publikację „przykładów profili dla małych instytucji i średnich przedsiębiorstw”.

www.bsi.de/gshb/deutsch/musterrichtlinien/index.htm (strona w języku niemieckim)

www.bsi.de/gshb/deutsch/hilfmi/beispielprofile.htm (strona w języku niemieckim)

Podręcznik do e-administracji jako standard bezpieczeństwa IT e-administracji Urzędu Federalnego ds. Bezpieczeństwa Informacji

Grupy docelowe obejmują nie tylko koordynatorów i decydentów e-administracji szczebla federalnego, stanowego i lokalnego, ale także twórców rozwiązań dla e-administracji i zainteresowanych obywateli. Podręcznik obejmuje takie zagadnienia jak „bezpieczna obecność w Internecie”, „e-administracja bez ograniczeń”, „kodowanie i podpis”, „e-administracja w zgodzie z ochroną danych”.

Wytyczne w zakresie bezpieczeństwa IT

Wytyczne w zakresie bezpieczeństwa IT zawierają przegląd najważniejszych środków bezpieczeństwa IT i są pomocne przy dążeniu do IT-Grundschutz. Wytyczne zostały pomyślane przede wszystkim jako pomoc dla nowicjuszy, a także dla menadżerów i osób odpowiedzialnych za bezpieczeństwo w małych i średnich przedsiębiorstwach przy zajmowaniu się bezpieczeństwem IT.

Informacje na temat bezpieczeństwa i kodowanie

Broszura „Bezpieczeństwo IT stworzone w Niemczech – najlepsza praktyka w bezpiecznych procesach handlowych” została opublikowana w 2004 r. we współpracy z TeleTrust Deutschland e.V. i była skierowana do ekspertów od bezpieczeństwa IT i kodowania.

Publikację tę udostępniono po raz pierwszy w czasie konferencji ISSE 2004 (*Information Security Solutions Europe*), która odbyła się w Berlinie we wrześniu 2004 r. wraz z konferencją ICCC (International Common Criteria Conference) zorganizowaną przez Urząd Federalny ds. Bezpieczeństwa Informacji.

Aktualne wydanie broszury jest planowane na czas konferencji ISSE 2006 w Rzymie. Więcej informacji - pod adresem: www.teletrust.de.

Informacje dla sektora handlowego

Federalne Ministerstwo Gospodarki i Pracy (*Bundesministerium für Wirtschaft und Arbeit*, obecnie Federalne Ministerstwo Gospodarki i Technologii, przyp. tłum.) i Federalne Ministerstwo Spraw Wewnętrznych zainicjowały w 2003 r. utworzenie zespołu CERT dla małych i średnich przedsiębiorstw (Mcert) jako spółki publiczno-prawnej - przedsięwzięcie angażujące między innymi kilku poważnych partnerów z niemieckiego przemysłu IT.

Mcert świadczy usługę ostrzegania i powiadamiania o incydentach, która skupia się szczególnie na słabościach oprogramowań regularnie stosowanych w małych i średnich przedsiębiorstwach lub na innych zagrożeniach, które stanowią dla nich zagrożenie. Więcej informacji - pod adresem: www.mcert.de.

TeleTrusT Deutschland e.V.

Różne projekty mające na przykład na celu promowanie wiarygodności technologii informacji i łączności, zostały wykonane we współpracy z TeleTrusT Deutschland e.V. (TTT). TeleTrusT Deutschland e.V. zostało utworzone w 1989 r. jako stowarzyszenie, którego zadaniem było promowanie wiarygodności aplikacji i usług opartych na podpisach elektronicznych, uwierzytelnianiu i kodowaniu w otwartym środowisku systemowym. Odpowiednia ochrona sprzętu, usług i aplikacji technologii informacji i łączności, wraz z zastosowaniem międzynarodowych standardów i współpracy (*interoperability*) to podstawowe zasady, drogą do nich są innowacyjne metody kryptograficzne i biometryczne. Więcej informacji - pod adresem: www.teletrust.de.

Inicjatywa D21 spółki publiczno-prawnej

Inicjatywa D21 jest największą, niemiecką spółką publiczno-prywatną z ponad 400 przedstawicielami przemysłu, stowarzyszeń, partii politycznych, instytucji politycznych i innych organizacji, które zobowiązały się do ulepszania ram dla szybkich i skutecznych przemian w społeczeństwie informacyjnym, by zwiększyć międzynarodową konkurencyjność Niemiec i przygotować kraj na przyszłe lata. Więcej informacji – pod adresem: www.initiaved21.de.

BSI jest obecne na dwóch głównych targach IT w Niemczech, „CeBIT” i „Systems”. Usługi i produkty BSI są oferowane dla różnych grup docelowych, także dla ludzi z sektora handlowego.

Rząd jako partner społeczeństwa

Najnowsze programy i inicjatywy poszerzania wiedzy

Szczególnie udane inicjatywy to kampanie na rzecz poszerzania wiedzy (co zostało szczegółowo opisane w częściach *Administracja jako twórca (...)* i *Administracja jako partner (przedsiębiorstw)*) zainicjowane przez Urząd Federalny ds. Bezpieczeństwa Informacji ("BSI für Bürger" – „Urząd Federalny ds. Bezpieczeństwa Informacji dla Obywateli”). Podręczniki i wytyczne z zakresu bezpieczeństwa także znacznie przyczyniły się do podnoszenia ogólnego poziomu bezpieczeństwa IT w Niemczech.

BSI dostarcza szereg materiałów informujących prywatnych użytkowników o konieczności zmierzenia się z tematem bezpieczeństwa IT w „życiu prywatnym”. Dostarcza on również narzędzia dla użytkowników. 2 przykłady najlepszej praktyki w poszerzaniu wiedzy:

- www.bsi-fuer-buerger.de: Strona informuje prywatnego użytkownika o wszystkich kwestiach związanych z bezpieczeństwem IT. Zawarte informacje są napisane łatwym do zrozumienia językiem, dzięki czemu nieprofesjonalista jest w stanie zrozumieć wskazówki i listy kontrolne oraz zastosować je. Można także ściągnąć ze strony darmowe narzędzia, takie jak ochrona antywirusowa, osobista zapora sieciowa (firewall) itd. Treść strony jest również rozprowadzana na CD-Romie, np. w czasie targów handlowych lub innych wydarzeń. Prowadzona jest także współpraca z dużymi firmami, by wykorzystać materiały BSI do poszerzania wiedzy pracowników.
- www.bsi-fuer-buerger.de: Portal dla prywatnych użytkowników komputerów osobistych został utworzony w 2003 r. Dostarczane tam informacje są dodatkowo przekazywane różnymi kanałami milionom użytkowników.

Bürger-CERT (www.buerger-cert.de) – pierwszy zespół CERT dla obywateli w Niemczech: prywatni użytkownicy mogą zapisać się do trzech różnych usług ostrzegawczych (w wyniku indywidualnego wniosku o ochronę).

1. Biuletyn "SICHER ° INFORMIERT". Od końca 2004 r. ten biuletyn dostarcza aktualnych informacji z BSI na temat wirusów i ogólnych aspektów bezpieczeństwa IT dla wszystkich obywateli.
2. Techniczne Ostrzeżenia ("Technische Warnungen") dla obywateli posiadających wiedzę techniczną.
3. Specjalna edycja biuletynu SICHER ° INFORMIERT". W przypadku olbrzymiego, niecierpiącego zwłoki ryzyka dla użytkowników.

Ponadto obywatele są ostrzegani, gdy pojawiają się krytyczne zagrożenia bezpieczeństwa, a także otrzymują oni wskazówki, jak postępować przy takim ryzyku (np. gdzie znaleźć *patch* itd.).

Informacje na temat innych, niemieckich inicjatyw znajdują się w części [Administracja jako partner \(przedsiębiorstw\)](#).

Statystyki i kluczowe wskaźniki wydajności (KPI)

Statystyki/KPI do oceny skuteczności inicjatywy poszerzania wiedzy

Różne metody przystosowane do konkretnego celu zostały stworzone, by sprawdzać i weryfikować systemy bezpieczeństwa IT i oceniać wydajność inicjatyw rządu federalnego z zakresu bezpieczeństwa IT i poszerzania wiedzy.

Badania wtargnięć

Badania wtargnięć są przeprowadzane w celu ustalenia, w jakim stopniu bezpieczeństwo systemów IT jest podatne na zagrożenia ze strony hakerów, krakerów itd. i/lub czy aktualnie powzięte środki bezpieczeństwa zapewniają bezpieczeństwo danemu systemowi IT.

Urząd Federalny ds. Bezpieczeństwa Informacji uruchomił w tym celu własne centrum badań wtargnięć.

Działania centrum badań wtargnięć IT Urzędu Federalnego ds. Bezpieczeństwa Informacji skupiają się obecnie na sprawdzaniu bezpieczeństwa aplikacji internetowych w ramach inicjatywy BundOnline 2005 i na kontroli Sieci Informacyjnej Berlin-Bonn (IVBB).

Ankiety Urzędu Federalnego ds. Bezpieczeństwa Informacji

Ankiety przyszłych osiągnięć i trendów w technologii informacyjnej i bezpieczeństwie informacji są przygotowywane w ramach analiz trendów.

Służą one jako podstawa do ogólnej definicji przyszłych, politycznych decyzji związanych z bezpieczeństwem IT i do identyfikacji przyszłych, służących za punkt wyjścia działań niemieckiego Urzędu Federalnego ds. Bezpieczeństwa Informacji.

Raz w roku przeprowadza się monitoring pod kątem wiedzy na temat produktów Urzędu Federalnego ds. Bezpieczeństwa Informacji. Reprezentatywne ankiety są przeprowadzane wśród osób odpowiedzialnych za bezpieczeństwo IT, ochronę danych i dziennikarzy.

W 2004 r. "monitoring wiedzy" został również przeprowadzony w tym kontekście wśród grupy docelowej prywatnych użytkowników komputerów osobistych. Wyniki są

uwzględniane w planie projektu Urzędu Federalnego ds. Bezpieczeństwa Informacji. Ankiety wśród ekspertów i obywateli są również planowane na przyszłość.

10. Grecja

Na podstawie odpowiedzi na kwestionariusz oraz uzupełniających informacji z przeprowadzonych rozmów, badań i dodatkowych materiałów dla Grecji wyszczególniono następujące części:

Bieżąca sytuacja

Kampanie

Bieżąca sytuacja

Zgodnie z raportem [SafeNetHome](#):

- Ponad 50 % użytkowników Internetu ma program antywirusowy lub zaporę sieciową (firewall). Problemy rzeczywiście spotykane w Internecie to przede wszystkim spam i wirusy komputerowe, z mniej niż 1 % przypadków dotyczących kart kredytowych lub nadużyć danych osobowych.
- Sytuacja nie jest taka sama w przypadku bezpieczeństwa w Internecie: 92 % greckich rodzin odczuwa potrzebę szerszej edukacji na temat tego, jak chronić dzieci przed nielegalną lub szkodliwą treścią w Internecie, umieszczając Grecję na pierwszym miejscu w rankingu 25 państw członkowskich Unii Europejskiej.
- Zgodnie z najnowszą ankietą Eurobarometru, korzystanie z Internetu przez dzieci jest nadal niewielkie w Grecji (15 %): 7 % dzieci surfuje z domu, podczas gdy 8 % robi to w szkole, co umieszcza Grecję na samym końcu listy wśród 25 państw członkowskich Unii.
- Większość greckich rodziców oczekuje od mediów, że pouczą ich o odpowiednim korzystaniu z Internetu (43 %), pozostawiając wszystkie inne źródła informacji daleko w tyle (ISP jest na drugim miejscu z 19 %). Wśród pożądanych sposobów zdobywania informacji telewizja znajduje się na pierwszym miejscu (66 % - najwyższy udział spośród 25 państw członkowskich UE), za nią znajduje się prasa (37 %) i radio (31 %).

Kampanie

SafeNetHome

Punkt Awareness w Grecji "SafeNetHome"

SafeNetHome, <http://www.saferinternet.gr/> jest w Grecji głównym źródłem społecznej wiedzy o szkodliwych treściach rozprowadzanych w Internecie i w innych nowych mediach. SafeNetHome jest członkiem Insafe (<http://www.saferinternet.org>), sieci 23 ośrodków poszerzenia wiedzy w 21 krajach, która koordynuje działania na rzecz wiedzy na temat bezpieczeństwa w Internecie w Europie.

Celem SafeNetHome jest projekt i realizacja demaskatorskiej kampanii dla różnych grup docelowych na rzecz szerzenia wiedzy w Grecji o potencjalnych zagrożeniach, jakie

czyhają w nielegalnej i szkodliwej treści w Internecie, ale także w technologii komórkowej i innych pojawiających się technologiach. Kampania została przeprowadzona pod hasłem „Bezpieczny Internet - razem”, zachęcając w ten sposób wszystkich członków społeczeństwa do wzięcia udziału w robieniu z Internetu i każdej nowej technologii bezpiecznego miejsca dla wszystkich konsumentów, ale przede wszystkim dla dzieci i młodzieży. Kampania skupiała się na rodzicach, wychowawcach i dzieciach, ale była także zaadresowana do organów publicznych, rządu i mediów.

Kampania na temat bezpieczniejszego Internetu w Grecji

Biorąc pod uwagę fakt, że proces wprowadzania Internetu do życia codziennego w Grecji jest jeszcze w powijakach, kraj korzysta z możliwości tworzenia go na podstawie zdobywanej wiedzy i doświadczenia, promowania współpracy z kluczowymi graczami i stronami zainteresowanymi i tworzenia publicznego zaufania do korzyści wynikających z nowych technologii. Celem jest podkreślenie znaczenia optymalnego i bezpiecznego korzystania z Internetu, pokonanie różnicy pokoleń, połączenie istniejących inicjatyw, wymiana informacji, narzędzi i metod z innymi europejskimi punktami Awareness.

Zgodnie z najnowszą ankietą Eurobarometru greckie społeczeństwo woli telewizję, radio i prasę jako źródło informacji o bezpieczniejszym korzystaniu z Internetu. Z tego powodu kampania miała miejsce głównie w telewizji, radiu i prasie, tylko w niewielkim stopniu w Internecie – na bogatym w informacje portalu w języku greckim dla młodzieży i dorosłych – i w formie różnych, elektronicznych i drukowanych materiałów szkoleniowych.

Równolegle do tych działań zorganizowano serie otwartych imprez dla wychowawców, rodziców, dzieci i młodzieży, z których najważniejsza to coroczne obchody „Dnia bezpieczniejszego Internetu” we współpracy z InSafe i wszystkimi innymi, krajowymi punktami Awareness. Więcej informacji na temat kampanii SafeNetHome znajduje się w części Pliki Elektroniczne pod nazwą [safenethome_annualreport2005.pdf](#).

Konsorcjum “SafeNetHome”

Prace nad projektem SafeNetHome są przeprowadzane przez konsorcjum dwóch greckich podmiotów, ściśle współpracujących na rzecz wiedzy o bezpiecznym Internecie od 2000 r.: Helleńska Organizacja Konsumentka E.KAT.O. i Extreme Media Solutions Ltd.

Więcej informacji – na stronie:

<http://www.saferinternet.gr/Default.aspx?PageContentID=88&tabid=105>

11. Węgry

Na podstawie odpowiedzi na kwestionariusz oraz informacji uzupełniających z przeprowadzonych wywiadów, badań oraz na bazie dodatkowych materiałów wyszczególniono dla Węgier następujące części:

[Bieżąca sytuacja](#)

[Rząd jako twórca prawnych, regulacyjnych i instytucjonalnych postanowień służących poszerzaniu wiedzy](#)

[Administracja krajowa jako użytkownik systemów informacyjnych](#)

[Władze lokalne jako użytkownik systemów informacyjnych](#)

[Rząd jako partner przedsiębiorstw i przemysłu](#)

[Rząd jako partner społeczeństwa](#)

[Statystyki i kluczowe wskaźniki wydajności \(KPI\)](#)

Obecna sytuacja

W kwietniu-maju 2006 r. na Węgrzech odbyły się wybory parlamentarne, które wpłynęły na obecne inicjatywy rządowe. Wszystkie strategie, ramy, programy i plany zawarte w tym raporcie są odzwierciedleniem działań poprzedniego rządu. Struktura organizacyjna nowego rządu tworzy się obecnie, tym samym nowe strategie i programy zostaną najprawdopodobniej przedstawione we wrześniu-październiku 2006 r.

Wcześniejsze i obecne regulacje i inicjatywy, jak i koncepcje na najbliższą przyszłość zostały zawarte tam, gdzie istniała taka możliwość.

Rząd jako twórca prawnych, regulacyjnych i instytucjonalnych postanowień służących poszerzaniu wiedzy

Krajowa strategia poszerzania wiedzy

Rozporządzenie rządu 41/2001, zmienione w 2003 r. określiło Ministerstwo Informatyki i Łączności (IHM – www.ihm.gov.hu) jako Europejskie Centrum ds. Informacji. W latach 2003 – 2004 utworzono zespół CERT-Węgry i przeniesiono na niego całą odpowiedzialność. Aby działać zgodnie z ogólną rolą poszerzania wiedzy zespół CERT-Węgry stworzył dwie internetowe strony informacyjne, jedną dla ogółu społeczeństwa z myślą o bezpieczeństwie w Internecie - www.biztonsagosinternet.hu – i drugą dla bezpieczeństwa w sieci, głównie dla administratorów sieci - www.halozatbiztonsag.hu. Ponadto zespół CERT-Węgry obsługuje własną stronę, upowszechniając wszystkie najważniejsze i potwierdzone słabości i zagrożenia.

Istnieją dwa międzyministerialne komitety zajmujące się kwestiami związanymi z technologią informacji i łączności, jeden to ITKTB (Międzyministerialny Komitet ds. Społeczeństwa Informacyjnego www.english.itktb.hu/Engine.aspx), który współpracuje przy tworzeniu węgierskiej strategii i planu działania w sprawie Społeczeństwa Informacyjnego. Drugi to KIETB (Międzyministerialny Komitet ds. e-administracji - www.meh.hu/szervezet/hivatalok/ekk/kietb/kietb20041116.html), utworzony w obrębie urzędu premiera zajmuje się wszystkim kwestiami dotyczącymi bezpiecznej e-administracji.

Nowa strategia IT, łącznie z poszerzaniem wiedzy, zostanie skoordynowana z Urzędem Premiera.

Prawne, regulacyjne i instytucjonalne rozwiązania służące poszerzaniu wiedzy

IHM cofnęło wszystkie główne programy, które zajmowały się poszerzaniem wiedzy, łącznie z węgierskim i europejskim planem działania i współpracą z przedsiębiorstwami i organizacjami społecznymi. Organy prawne, takie jak Krajowy Organ ds. Łączności (NHH – www.nhh.hu) podjął środki mające na celu pomiar spamu, poszerzanie wiedzy na jego temat i filtrowanie go (www.spam.baratsagosinternet.hu). Ostatnie Dzień Bezpiecznego Internetu był poświęcony zwalczaniu spamu.

Władze państwowe jako użytkownik systemów informacyjnych

Najnowsze programy i inicjatywy poszerzania wiedzy

Istnieje jeden ogólny system władz państwowych - węgierski portal elektroniczny www.magyarorszag.hu. Portal ten ma działać na rzecz obywateli Węgier, ale jego skuteczne wykorzystanie wymaga odpowiednich kompetencji urzędników. Przeprowadzono powszechną kampanię medialną propagującą korzystanie z portalu, a także przeszkolono operatorów.

Wyżej wspomniany KIETB zajmuje się również poszerzaniem wiedzy społeczeństwa w zakresie ustawicznie rozwijającego się systemu e-administracji. Jego zalecenia w kwestii funkcji i nabywania elementów portalu również podporządkowane są aspektom bezpieczeństwa użytkowników końcowych.

Kolejną inicjatywą, mającą na celu promowanie bezpieczeństwa sieci, jest doradztwo zespołu CERT-Hungary dla jego użytkowników. Ponieważ jest to rządowy zespół CERT, do jego głównych klientów należą niektóre części krytycznej infrastruktury informacyjnej na Węgrzech, np.:

- Węgierski Urząd Lotnictwa Cywilnego
- Ministerstwo Informatyki i Komunikacji
- Krajowy Urząd Komunikacji

- NETI Ltd.
- NT Public Beneficiary Ltd.
- Sieć publiczna
- Theodore Puskas Foundation

Kanał przekazywania informacji poszerzających wiedzę obejmuje cotygodniowe biuletyny i publiczne informacje na stronie zespołu CERT-Hungary.

Władze lokalne jako użytkownik systemów informacyjnych

Najnowsze programy i inicjatywy poszerzania wiedzy

Trudno jest oszacować programy poszerzania wiedzy realizowane przez władze lokalne, ponieważ system gmin jest bardzo podzielony i władze lokalne mogą mieć własne systemy informacyjne. Jednakże istnieją też programy, których celem jest edukacja w dziedzinie bezpieczeństwa na szczeblu lokalnym. Sieć Telehouse (www.telehaz.hu) zajmuje się propagowaniem umiejętności obsługi Internetu i komputera, a program mentorski w dziedzinie IT (www.itmentor.hu) poszerza wiedzę użytkowników na szczeblu lokalnym.

Rząd jako partner przedsiębiorstw i przemysłu

Małe i średnie przedsiębiorstwa (MŚP)

W 2005 r. Ministerstwo Informatyki i Komunikacji rozpoczęło inicjatywę o nazwie eSec.hu (www.esec.hu), łączącą znaczące MŚP zajmujące się bezpieczeństwem IT i będące własnością węgierską. Każdy z członków grupy reprezentuje inną dziedzinę bezpieczeństwa IT, pokrywając w sumie wszystkie zagadnienia:

- Kürt Ltd. – odzyskiwanie i ochrona danych
- BalaBit Ltd. – zapory sieciowe, filtrowanie zawartości
- VirusBuster Ltd. – ochrona przed wirusami i spamem
- Megatrend Ltd. – systemy informacji handlowych
- E-Group Ltd. – PKI (Public Key Infrastructure - Infrastruktura Klucza Publicznego), ochrona dokumentów
- CERT-Hungary – reagowanie na incydenty, poradnictwo, szkolenie

W 2006 r. grupa firm stworzyła konsorcjum, które ma wspólne cele, mianowicie:

- wspólne przetargi UE i Węgier
- reprezentowanie wspólnych interesów w dziedzinie bezpieczeństwa IT
- wpływ na decydentów i doradzanie im
- podtrzymywanie opłacalności na terenie UE

Konsorcjum eSec.hu jest przedsięwzięciem nastawionym na zysk, jednakże jest ono blisko związane z programami poszerzania wiedzy społeczeństwa, ponieważ jednym z członków jest zespół CERT-Hungary. Wiele projektów przetargów wiąże się

z „poszerzaniem wiedzy”, np. Bezpieczniejszy Internet Plus lub eContent; pożądana jest w nich współpraca między partnerami.

Dostawcy usług internetowych (ISP)

ISP są w dużym stopniu odpowiedzialni za poszerzanie wiedzy użytkowników. Posiadają własne stowarzyszenie (www.iszt.hu/iszt/English), reprezentujące ich interesy wobec decydentów. Pierwszym krokiem w powszechnym poszerzaniu wiedzy przy pomocy rządu są statuty w sprawie samoregulacji. Za koordynowanie przekazywania informacji między rządem a ISP odpowiada zespół Hun-CERT, zajmujący się sektorem przemysłu i ISP na Węgrzech.

Do tej pory nie było żadnych wspólnych programów poszerzania wiedzy, skierowanych do społeczeństwa. CERT-Hungary i Hun-CERT pozostają w dobrych stosunkach; elementem ich współpracy była operacja, której celem było sprawdzenie skłonności ISP do współpracy w dziedzinie bezpieczeństwa IT. Wyniki mają zostać jesienią przekazane przez różne kanały, skierowane zarówno do specjalistycznych mediów, jak i do ogółu społeczeństwa.

Media

Należy zwrócić uwagę, że w poniżej wymienionych przykładach media wykorzystywane są jako kanał dotarcia do innych grup docelowych, a nie przedstawione jako odrębna grupa docelowa.

Drukowane media o tematyce ogólnej nie zajmują się jeszcze kwestiami bezpieczeństwa na dużą skalę, więc tematem podstawowych inicjatyw poszerzania wiedzy zajmowały się do tej pory media specjalistyczne. Ponieważ media internetowe zyskują coraz większą popularność, ważne jest utworzenie stron informacyjnych na temat bezpieczeństwa IT i propagowanie ich. Zadaniem tym częściowo zajął się zespół CERT-Hungary poprzez uruchomienie dwóch witryn internetowych poświęconych bezpieczeństwu IT. Jedna z nich, www.biztonsagosinternet.hu, przeznaczona jest dla ogółu społeczeństwa i dotyczy bezpieczeństwa w Internecie, zaś druga, www.halozatbiztonsag.hu, przeznaczona jest głównie dla administratorów sieci i zajmuje się bezpieczeństwem sieci.

Istnieją też prywatne publikacje przeznaczone specjalnie dla rynku technologii informacyjnych i komunikacyjnych, np. *IT business* (www.it-business.hu) lub *Connect magazin* (www.connectmagazin.hu). Znaczenie pozostałych magazynów, np. *Chip* (www.chiponline.hu) lub *Linuxvilág* (www.linuxvilag.hu) itp., ograniczone jest w zasadzie do celów komercyjnych.

Nie tak blisko związane z sektorem mediów, a warte wspomnienia, są konferencje mające w ostatnich latach miejsce na Węgrzech. Na Węgrzech odbyło się kilka bardzo istotnych wydarzeń, takich jak konferencja FIRST w 2004 r. i konferencja ISSE w 2005 r.

Oba wydarzenia zostały szeroko zrelacjonowane w mediach; w latach 2006-2007 także mają się tu odbyć ważne wydarzenia specjalistyczne.

Partnerstwo publiczno-prywatne

Skuteczne partnerstwo publiczno-prywatne (w dziedzinie poszerzania wiedzy i edukacji/szkolenia)

Najlepszym przykładem poszerzania wiedzy w partnerstwach publiczno-prywatnych (PPP) jest wspomniane już konsorcjum eSec.hu. Członkowie tej grupy obejmują szerokie spektrum bezpieczeństwa IT, a ich celem jest stworzenie bezpiecznego środowiska IT, zarówno w sektorze publicznym, jak i w prywatnym. Nowatorskie rozwiązania stosowane są przez rząd, administrację publiczną, środowisko akademickie, przedsiębiorstwa handlowe, a także przez ogół społeczeństwa.

Jednym z przykładów działań partnerstwa publiczno-prywatnego jest konferencja w sprawie wdrożenia standardu ISO 27000, na której wszyscy członkowie eSec.hu mogli przyczynić się do promowania tego standardu.

Głównym celem konsorcjum eSec.hu jest prowadzenie kampanii na rzecz stworzenia prawa normalizującego stosowanie partnerstwa publiczno-prywatnego w dziedzinie bezpieczeństwa IT.

Rząd jako partner społeczeństwa

Najnowsze inicjatywy i programy poszerzania wiedzy

Rząd i społeczeństwo podejmują współpracę w dziedzinie poszerzania wiedzy w celu ochrony użytkowników prywatnych i ogółu społeczeństwa.

Jedną z organizacji realizujących wspólne cele wszystkich stron jest IT KTB (Międzyministerialny Komitet ds. Społeczeństwa Informatycznego), utworzony 25 lutego 2003 r. na mocy rozporządzenia rządu nr 1214/2002 (www.english.itktb.hu/Engine.aspx). Głównym zadaniem komitetu jest doradzanie w kwestiach dotyczących krajowej strategii IT. Za główne zagadnienia odpowiedzialne są podkomitety w każdej z dziedzin. W dyskusjach biorą udział również środowiska społeczne.

Do KIETB, Międzyministerialnego Komitetu ds. e-administracji utworzonego na mocy rozporządzenia rządu nr 1054/2004, należy także kilku członków pozarządowych, działających jako stali delegaci doradcy. Umożliwia to szerszą dyskusję na temat aspektów bezpiecznych i przyjaznych dla użytkowników portali e-administracji.

Kolejnym głównym forum, na którym rząd aktywnie uczestniczy w dyskusji o kwestiach bezpieczeństwa IT, jest Stowarzyszenie Węgierskich Przedsiębiorstw Informatycznych (IVSZ, www.ivsz.hu). IVSZ jest zaangażowane w kilka projektów zainicjowanych

przez UE i związanych częściowo z bezpieczeństwem IT i poszerzaniem wiedzy, np. IT mentor lub Secure-Force.

Ministerstwo Informatyki i Komunikacji także brało czynny udział w popieraniu kilku inicjatyw poszerzania wiedzy w środowiskach społecznych. Unijny program Bezpieczniejszy Internet rozpoczął na Węgrzech kilka projektów, które są częściowo zarządzane lub wspierane przez wyżej wymienione ministerstwo. Do projektów tych należy węgierski punkt kontaktowy ds. zwalczania nielegalnych treści w Internecie (Internethotline, www.internethotline.hu), funkcjonujący we współpracy z MATISZ (Węgierskie Stowarzyszenie Przemysłu Technologii Informacyjnych, www.matisz.hu) i z wydziałem policji ds. cyberprzestępczości (Krajowe Biuro Śledcze). Punkt kontaktowy jest już akredytowanym członkiem organizacji INHOPE. Kolejną ważną akcją jest oznaczanie stron internetowych, co poszerza wiedzę dzieci i rodziców. MTE (Węgierskie Stowarzyszenie Dostawców Treści – www.mte.hu) czuwa nad witryną internetową Węgierskiego Bezpieczniejszego Internetu (www.baratsagosinternet.hu), współpracując z MATISZ, INFORUM (www.inforum.org.hu), Ministerstwem Informatyki i Komunikacji i zespołem CERT-Hungary.

Zaplanowane na najbliższą przyszłość działania we współpracy ze środowiskami społecznymi obejmują między innymi wspólny plan działania z zespołem CERT-Hungary i MATISZ (Węgierskie Stowarzyszenie Przemysłu Technologii Informacyjnych, www.matisz.hu). Celem tego planu jest przeprowadzenie szkoleń w sieci Telehouse w zakresie informowania o zagadnieniach dotyczących bezpieczeństwa IT. Podstawą mają być materiały opublikowane na stronie www.biztonsagosinternet.hu; projekt wzorowany jest na niemieckim BMI, www.bsi-fuer-buerger.de. Materiały te są stworzone w sposób umożliwiający ich łatwe zrozumienie przez użytkowników prywatnych, dzieci i rodziców. Dalszym celem jest możliwość dotarcia do szkół i wywarcia na młodych użytkowników wpływu w zakresie kwestii związanych z bezpieczeństwem. Pomysł ten podporządkowany jest zamierzeniu włączenia znajomości IT, w tym bezpieczeństwa IT, do państwowego programu nauczania.

Kolejnym kierunkiem w poszerzaniu wiedzy i edukacji w dziedzinie technologii ICT jest współpraca między węgierskim oddziałem ISACA, a zespołem CERT-Hungary, polegająca na gromadzeniu różnych poziomów programu nauczania w celu prowadzenia szkoleń na różnych poziomach znajomości technologii ICT. Zespół CERT-Hungary będzie w stanie prowadzić wykłady dla profesjonalistów z certyfikatami CISA i CISM, zatwierdzonymi przez ISACA. Ponadto ogromna ilość wspólnych materiałów informacyjnych będzie stanowiła podstawę dla dowolnej formy edukacji. Na Węgrzech prowadzona jest także kampania na rzecz włączenia bezpieczeństwa IT do państwowego programu nauczania.

Statystyki i kluczowe wskaźniki wydajności (KPI)

Statystyki/KPI do oceny skuteczności inicjatywy poszerzania wiedzy

W chwili obecnej nie ma dostępnych wskaźników KPI oceniających inicjatywy poszerzania wiedzy.

Konieczne jest ustalenie wspólnego sposobu oceny wydajności, jednakże przy porównywaniu różnych państw członkowskich trzeba uwzględnić cechy charakterystyczne danego kraju.

12. Islandia

Na podstawie odpowiedzi na kwestionariusz oraz uzupełniających informacji z przeprowadzonych rozmów, badań i dodatkowych materiałów dla Islandii wyszczególniono następujące części:

[Kampanie](#)

Kampanie

SAFT (Samfélag, fjölskylda og tækni) jest projektem poszerzającym wiedzę, realizowanym przez Heimili og skóli (Dom i Szkoła) - narodowe stowarzyszenie zrzeszające rodziców w Islandii (listopad 2005 r. – czerwiec 2006 r.).



Wstęp

Heimili og skóli, narodowe stowarzyszenie rodziców, jest islandzkim punktem Awareness (ang. *awareness node*) w dziedzinie bezpieczeństwa w Internecie. Projekt nosi nazwę SAFT – *Samfélag, fjölskylda og tækni* (Społeczeństwo, rodzina i technologia). Projekt ten stanowi element sieci europejskich punktów Awareness INSAFE, funkcjonującym w ramach umowy na podstawie unijnego programu Bezpieczniejszy Internet. Akronim nazwy projektu (Safer Internet Action Plan Iceland) brzmi SIAP; projekt ma być realizowany od 1 października 2004 r. do 30 września 2006 r.

W okresie od listopada 2005 r. do czerwca 2006 r. podjęto działania w zakresie poszerzania wiedzy w kilku dziedzinach, takich jak bezpieczeństwo telefonów komórkowych, gry komputerowe, a także bezpieczne i etyczne korzystanie z Internetu. Tworzenie sieci jest ważnym elementem działań poszerzających wiedzę; z kilkoma różnymi stronami zainteresowanymi nawiązano owocną współpracę.

Najważniejsze etapy w tym okresie to:

- Listopad 2005 r.: Broszura dla rodziców na temat bezpieczeństwa telefonów komórkowych (we współpracy z Og Vodafone w Islandii)
- Listopad-grudzień 2005 r.: Gry komputerowe i system klasyfikacji PEGI: Broszura dla rodziców i kampania medialna (współpraca i wsparcie – SMAIS (Islandzkie Stowarzyszenie Właścicieli Praw Filmowych), Ministerstwo Edukacji, Microsoft i Gallup)

- Luty 2006 r.: Dzień Bezpiecznego Internetu obchodzony 7 lutego. Konferencja i blogathon na stronie internetowej SAFT (www.saft.is) na temat etyki i Internetu
- Czerwiec 2006 r.: Karta-przewodnik dla rodziców, zawierająca 10 rad na temat bezpieczeństwa telefonów komórkowych i 10 rad na temat bezpieczeństwa w Internecie (we współpracy z Siminn (Iceland Telecom))
- Marzec-czerwiec 2006 r.: Projekt kampanii medialnej na temat etyki internetowej, do przeprowadzenia w okresie od sierpnia do września; projekt dwóch modułów edukacyjnych dla szkół, dotyczących etyki internetowej i krytycznego podejścia do źródeł, do rozprowadzenia we wrześniu. Ponadto korekta broszury dla rodziców na temat bezpieczeństwa telefonów komórkowych, do rozprowadzenia w okresie od sierpnia do września

Oprócz wymienionych działań należy wspomnieć także o aktywnej stronie internetowej, www.saft.is; ponadto ważnym elementem prac są spotkania z rodzicami i osobami zainteresowanymi.

1. Broszura dla rodziców na temat bezpieczeństwa telefonów komórkowych

„Foreldrar börn og farsímar” (Rodzice, dzieci i telefony komórkowe) - taki tytuł nosi broszura dla rodziców na temat bezpieczeństwa telefonów komórkowych, wydana w listopadzie 2005 r. we współpracy z Og Vodafone. Pierwszy egzemplarz broszury otrzymał islandzki Minister Edukacji 1 listopada podczas konferencji prasowej. Była ona rozdawana podczas spotkań z rodzicami, organizowanych przez SAFT, a także w sklepach i centrach obsługi firmy Og Vodafone.

Po badaniach przeprowadzonych w maju 2006 r. broszura została poprawiona i będzie ponownie wydana i rozpowszechniona w okresie do sierpnia do września 2006 r.



2. Kampania na temat gier komputerowych (listopad-grudzień 2005 r.)

W listopadzie i grudniu przeprowadzono kampanię poszerzającą wiedzę o grach komputerowych i systemie klasyfikacji PEGI. Kampania ta została zaplanowana i przeprowadzona przez SAFT, przy wsparciu ze strony Ministerstwa Edukacji, SMÁÍS (Islandzkiego Stowarzyszenia Właścicieli Praw Filmowych), PEGI, Microsoft w Islandii i Gallup:

- Badania wśród dzieci w wieku 9-16 lat w zakresie korzystania z gier komputerowych przeprowadziło dla SAFT we wrześniu Rannsóknir og greining (Islandzkie Centrum Badań i Analiz Społecznych).



Badania przeprowadzono we współpracy ze szkołami; dzieci odpowiadały w klasach na 20 pytań kwestionariusza. Grupę badanych wybrano losowo, odsetek odpowiedzi wynosił 90%

- Badania wśród dorosłych na temat znajomości systemu klasyfikacji PEGI przeprowadzono we wrześniu 2005 r. i powtórzono w grudniu, tj. przed kampanią i po niej. Wykazują one 35% wzrost wiedzy na temat systemu klasyfikacji PEGI wśród osób, które stwierdziły, że kupiły gry komputerowe
- Broszura dla rodziców na temat gier komputerowych i systemu klasyfikacji PEGI (patrz zdjęcie). Zaprojektowano ją, wydrukowano i rozdano rodzicom wszystkich dzieci w kraju uczęszczających do szkół podstawowych (w sumie 45 tys.). Tekst oparty był na badaniach wśród dzieci i informacjach na temat systemu klasyfikacji PEGI. Broszurę rozprowadzono we współpracy ze wszystkimi szkołami podstawowymi w Islandii, które przekazały broszury do domów za pośrednictwem uczniów
- Zaprojektowano animowaną reklamę zatytułowaną „Dla kogo jest ta gra komputerowa?” i pokazywano ją w kinach i głównych stacjach telewizyjnych w trakcie trwania kampanii. W kinach wyświetlano ją od 7 grudnia do 10 stycznia. Nadal jest od czasu do czasu emitowana w stacjach telewizyjnych
- Zaprojektowano reklamę w formie slajdów (plansz), którą pokazywano w kinach i telewizji w okresie od 7 grudnia do 10 stycznia. Nadal jest ona od czasu do czasu emitowana w głównych stacjach telewizyjnych
- Zaprojektowano reklamę autobusową, która była prezentowana na 20 autobusach w Reykjavíku, stolicy Islandii, w okresie od 26 listopada, przez cały grudzień i znaczną część stycznia.
- Zaprojektowano cztery rodzaje banerów internetowych, które były następnie widoczne na popularnych islandzkich stronach internetowych
- Artykuły prasowe: W głównych gazetach w Islandii opublikowano artykuły napisane przez dziennikarzy na temat gier komputerowych i klasyfikacji

Skuteczność kampanii na temat gier komputerowych została oceniona poprzez przeprowadzenie badań dotyczących znajomości systemu klasyfikacji PEGI przed kampanią i po niej. Badania wśród osób w wieku od 16 do 75 lat przeprowadziła firma Gallup, najpierw we wrześniu i ponownie w grudniu. Wykazały one 35% wzrost wiedzy na temat systemu klasyfikacji PEGI wśród osób, które stwierdziły, że kupiły gry komputerowe.

3. Dzień Bezpiecznego Internetu 2006 – konferencja SAFT na temat etyki i Internetu; blogathon.

W Dniu Bezpiecznego Internetu, 7 stycznia 2006 r., SAFT zorganizował trwającą pół dnia konferencję. W tym samym czasie na stronie projektu, www.saft.is, rozpoczął się blogathon na temat etycznego korzystania z Internetu.

Konferencja była publicznie reklamowana, przesłano także zaproszenia osobom działającym w ramach systemu edukacji, agencji rządowych i dostawców usług

internetowych. Przed konferencją wydrukowano i rozdano pięćset zaproszeń. Dużo zaproszeń rozprawdano także za pośrednictwem poczty elektronicznej. W gazetach zamieszczono reklamy, a także umieszczono banery na kilku stronach internetowych, między innymi na popularnych serwisach z blogami, takich jak www.folk.is, z którego powszechnie korzystają młodzi Islandczycy.

W konferencji uczestniczyło stu gości, była ona ponadto transmitowana na żywo na stronie www.saft.is. W tym dniu zanotowano ponad 30.000 wejść na tę stronę. Przy technicznej stronie nagrywania i transmisji pomógł nauczyciel multimediów i uczniowie szkoły ogólnokształcącej we Flensburgu. Strumieniową transmisją danych na stronie internetowej zajęła się firma Og Vodafone.

Islandzka Minister Edukacji, Thorgerdur Katrin Gunnarsdottir, otworzyła konferencję i rozpoczęła blogathon na temat etyki w Internecie, trwający przez tydzień na stronie www.saft.is. Blogathon został przed rozpoczęciem przedstawiony we wszystkich szkołach, jak również w mediach, spodziewano się więc dużego udziału na różnych szczeblach. Pomimo tego, że na serwisie z blogami toczyły się pewne owocne dyskusje, liczba uczestników była niższa, niż oczekiwano.

Konferencja i omawiane na niej zagadnienia były wzmiankowane nie tylko w reklamach – islandzkie media poświęciły im 7 lutego i w ciągu następnych dni wiele uwagi. Wszystkie główne media informacyjne w kraju informowały o konferencji; w prasie, telewizji i radiu przeprowadzano wywiady zarówno z pracownikami SAFT, jak i z prelegentami.

Konferencja i zainteresowanie nią mediów zapoczątkowały w całym społeczeństwie dyskusję na temat etycznego i bezpiecznego korzystania z Internetu. Liczba telefonów od osób proszących o poradę i pomoc, jak również liczba wizyt na stronie internetowej SAFT gwałtownie zwiększyły się w trakcie trwania konferencji.

Głównym prelegentem była Isabella Santa z ENISA, a czterech innych specjalistów wygłosiło przemówienia. Konferencja zakończyła się dyskusją panelową, prowadzoną przez Þorbjorn Broddason, profesora socjologii i dziennikarstwa z Uniwersytetu Islandzkiego. Uczestnicy reprezentowali dostawców usług internetowych, media, rząd i rodziców.

Ogólny wniosek z konferencji zwrócił uwagę na konieczność podejmowania ciągłych działań poszerzających wiedzę, aby dotrzeć do różnych poziomów społeczeństwa. Wszyscy prelegenci podkreślali, że rodzice mają kluczową rolę w uczeniu dzieci korzystania z Internetu w sposób bezpieczny i pozytywny, ponieważ „swobodne” korzystanie z Internetu ma w większości miejsce w domu.

4. Karta-przewodnik dla rodziców dotycząca korzystania z telefonów komórkowych i Internetu

Poradnik dla użytkowników: Jak poszerzyć wiedzę o bezpieczeństwie informacji

Kartę-przewodnik dla rodziców, dotyczącą korzystania z telefonów komórkowych i Internetu, wprowadzono 15 czerwca 2006 r. podczas konferencji prasowej. Następnego dnia karta ta została rozesłana pocztą do rodziców wszystkich dzieci w wieku 6-14 lat w Islandii.

Dwustronna karta na jednej stronie posiada 10 rad na temat korzystania z telefonów komórkowych, a na drugiej 10 rad dotyczących korzystania z Internetu.

Karta-przewodnik jest wspólnym projektem SAFT i Siminn (Iceland Telecom)



4. Działania poszerzające wiedzę zaplanowane na sierpień i wrzesień 2006 r.

a) AUGA – kampania medialna na temat etyki internetowej

Projektowana jest wielka kampania medialna na temat etyki internetowej, skierowana do dzieci i młodzieży. Zostanie ona rozpoczęta pod koniec sierpnia. Do otrzymania grantu z funduszu AUGA w formie kampanii medialnej wybrano SAFT.

AUGA (AD-AID) jest funduszem utworzonym przez Stowarzyszenie Islandzkich Agencji Reklamowych we współpracy z największymi przedsiębiorstwami medialnymi w Islandii, IMARK (Stowarzyszeniem Islandzkich Specjalistów ds. Marketingu) i SAU (Stowarzyszeniem Specjalistów ds. Reklamy). Celem Ad-Aid jest pomoc organizacjom non-profit w promowaniu ich działań.

b) Moduły edukacyjne na temat etyki internetowej i krytycznego podejścia do źródeł

Projektowane są dwa moduły edukacyjne – jeden dotyczy etyki internetowej, a drugi krytycznego podejścia do źródeł. We wrześniu zostaną one przekazane wszystkim szkołom podstawowym w Islandii, będą także dostępne na stronie internetowej projektu: www.saft.is.

Moduł edukacyjny na temat etyki internetowej będzie się składał z dwóch części, dla dzieci w wieku 9-12 lat i 13-16 lat.

Moduł na temat krytycznego podejścia do źródeł będzie zaprojektowany dla dzieci w wieku 13-16 lat.

13. Irlandia

Na podstawie odpowiedzi na kwestionariusz oraz uzupełniających informacji z przeprowadzonych rozmów, badań i dodatkowych materiałów dla Irlandii wyszczególniono następujące części:

[Kampanie](#)

Kampanie

Szczegółowe informacje na temat inicjatyw poszerzania wiedzy, organizowanych przez prywatną organizację VigiTrust, znajdują się w części *Dobre praktyki w grupach docelowych – Władze lokalne*.

Nie dostarczono informacji na temat programów poszerzania wiedzy realizowanych przez rząd irlandzki, ministerstwa lub organizacje publiczne.

14. Włochy

Na podstawie odpowiedzi na kwestionariusz oraz uzupełniających informacji z przeprowadzonych rozmów, badań i dodatkowych materiałów dla Włoch wyszczególniono następujące części:

[Rząd jako twórca prawnych, regulacyjnych i instytucjonalnych postanowień służących poszerzaniu wiedzy](#)

[Władze państwowe jako użytkownik systemów informacyjnych](#)

[Władze lokalne jako użytkownik systemów informacyjnych](#)

[Rząd jako partner społeczeństwa](#)

[Kampanie](#)

Rząd jako twórca prawnych, regulacyjnych i instytucjonalnych uregulowań służących poszerzaniu wiedzy

Krajowa strategia poszerzania wiedzy

Główna inicjatywa

Pod koniec marca 2006 r. opublikowano Krajowy Plan Bezpieczeństwa ICT w Administracji Publicznej, jak również Krajowy model organizacyjny bezpieczeństwa ITC w Administracji Publicznej. Obie publikacje dostępne są pod adresem

[www.cnipa.gov.it/site/it-it/La Documentazione/Pubblicazioni/i_Quaderni/](http://www.cnipa.gov.it/site/it-it/La_Documentazione/Pubblicazioni/i_Quaderni/), w „I Quaderni” nr 23, marzec 2006 r.

Oba dokumenty zostały szczegółowo opracowane przez Krajowy Komitet Techniczny (www.cnipa.gov.it/site/it-it/Attivit%c3%a0/Sicurezza_informatica/), którego zadaniem jest ustalenie krajowej strategii wdrażania odpowiedniego bezpieczeństwa ICT w Administracji Publicznej.

Inicjatywy poszerzania wiedzy odgrywają w tej strategii główną rolę. W szczególności głównym celem kampanii poszerzania wiedzy i kształtowania świadomości było rozpowszechnienie w Administracji Publicznej najlepszych praktyk w dziedzinie bezpieczeństwa ICT.

Określono trzy główne grupy docelowe:

- Ścisłe kierownictwo. Dla ścisłego kierownictwa zorganizowano jednodniowe seminarium, obejmujące wszystkie ogólne aspekty bezpieczeństwa ICT (prawne, techniczne, budżetowe), za które odpowiedzialne jest kierownictwo. W takim seminarium udział wzięło już 60% ścisłego kierownictwa administracji publicznej
- Odpowiedzialni za bezpieczeństwo ICT. Dla tej grupy użytkowników zaplanowano tygodniowe seminarium, obejmujące szczegółowe techniczne i organizacyjne aspekty bezpieczeństwa ICT. Jednym z celów takich seminariów jest przygotowanie osób odpowiedzialnych za bezpieczeństwo ICT do pełnienia funkcji „nauczyciela” w zakresie bezpieczeństwa ICT dla swoich pracowników. Seminaria rozpoczną się w drugiej połowie 2006 r. Liczba osób, do których ma dotrzeć ta inicjatywa, szacowana jest na kilkaset.
- Użytkownicy końcowi (tj. pracownicy administracji publicznej). Dla użytkowników końcowych opracowywany jest oparty na sieci program typu e-learning. Ma on dotrzeć do około dwustu tysięcy osób. Rozpoczęcie inicjatywy planowane jest na koniec 2006 r.

Ponadto planowane jest wyprodukowanie około 50 godzin programów lekcyjnych dotyczących bezpieczeństwa ICT, które zostaną wyemitowane przez państwowy kanał telewizyjny DGTv. Główną grupą docelową, do której skierowane będą te „lekcje”, są obywatele o niskim lub średnim poziomie wiedzy na temat narzędzi ICT. „Lekcje” te będą także oglądać w godzinach pracy i na zasadzie dobrowolności pracownicy administracji publicznej.

Władze państwowe jako użytkownik systemów informacyjnych

Najnowsze inicjatywy i programy poszerzania wiedzy

Informacje znajdują się w części [Rząd jako twórca](#).

Władze lokalne jako użytkownik systemów informacyjnych

Najnowsze inicjatywy i programy poszerzania wiedzy

Informacje znajdują się w części [Rząd jako twórca](#).

Rząd jako partner społeczny

Najnowsze inicjatywy i programy poszerzania wiedzy

Inicjatywa Poszerzania Wiedzy Obywateli na Temat Bezpieczeństwa Informacji

“Master in Sicurezza dei Sistemi e delle Reti Informatiche per l’Impresa e la Pubblica Amministrazione” z Uniwersytetu „La Sapienza” w Rzymie i „Consorzio Interuniversitario per le Applicazioni di Supercalcolo per Università e Ricerca” (CASPUR) we współpracy z Krajowym Ośrodkiem Informatyki w Administracji Publicznej (Centro Nazionale per l’Informatica nella Pubblica Amministrazione, CNIPA) planują rozpoczęcie nowatorskiej inicjatywy promującej poszerzanie wiedzy w dziedzinie bezpieczeństwa informacji we Włoszech.

Wzorując się na wskazówkach zawartych w publikacji ENISA “Information Package: Raising Awareness in Information Security - Insight and Guidance for Member States” [Pakiet informacji: poszerzanie wiedzy na temat bezpieczeństwa informacji – analiza i wskazówki dla państw członkowskich], celem partnerstwa CNIPA, CASPUR i studiów “Master in Sicurezza dei Sistemi e delle Reti Informatiche per l’Impresa e la Pubblica Amministrazione” jest realizacja multimedialnego projektu transmitowania wskazówek dotyczących świadomego i bezpiecznego korzystania z Internetu. Projekt taki byłby użytecznym instrumentem usług informacyjnych, rozrywki, łączności i innych przydatnych i zróżnicowanych usług. W szczególności celem projektu jest wypełnienie luki między obywatelami a nowymi technologiami, którą wykazały inne trwające projekty.

Zawartość projektu będzie zorganizowana jako rzeczywisty i skuteczny kurs edukacyjny, ogólnie dostępny z sieciowych portali organizacji instytucjonalnych, np. ze strony CNIPA (<http://www.cnipa.gov.it>) i strony Ministerstwa Edukacji i Technologii (<http://www.italia.gov.it>).

Tematy tego kursu będą ustawicznie poprawiane i uzupełniane, ponieważ jest to konieczne w dynamicznym środowisku ICT. W przyszłości planowane jest udostępnienie kursu także za pośrednictwem innych mediów, na przykład bezpłatnych płyt CD lub książek.

Inicjatywę rozpoczęto w maju, ukończenie projektu planowane jest na początek sierpnia.

Grupą docelową projektu są użytkownicy prywatni, a konkretnie dorośli, jak ustalono w Pakiecie informacji ENISA na rok 2005, czyli obywatele urodzeni po latach 50-tych XX w, powyżej 16 roku życia. Ta grupa docelowa charakteryzuje się zróżnicowanym zakresem umiejętności i znajomości ICT, jak również wykazuje następujące potrzeby i cele:

- Płatności internetowe (e-handel, płatności, bankowość...)

- Pobieranie plików muzycznych i oprogramowania
- Rozrywka w Internecie
- Surfowanie w Internecie – wiadomości, hobby, organizacje, produkty

Aby sprostać zróżnicowanej skali umiejętności technicznych, których poziom być „żaden” lub „wysoki”, projekt porządkuje tematy kursu według różnych poziomów szczegółowych informacji: od prostego wprowadzenia dla nowicjuszy do szczegółowych technicznych objaśnień dla użytkowników o największym poziomie umiejętności. Po głównym kursie każdy temat można omówić bardziej dogłębnie, dając użytkownikowi możliwość wyboru czy zbadać temat dokładniej.

Zróżnicowana treść projektu będzie obejmowała główne zagadnienia dotyczące dostawców usług internetowych – od dostępu do Internetu do ochrony komputerów osobistych za pomocą narzędzi antywirusowych i chroniących przed złośliwym oprogramowaniem oraz osobistych zapór sieciowych. Zostanie także objaśniona konieczność ciągłej aktualizacji wszystkich składników oprogramowania komputera osobistego, zarówno systemu operacyjnego, jak i listy nowych wirusów i złośliwego oprogramowania. Część projektu będzie poświęcona uwierzytelnianiu i podpisom elektronicznym, a także certyfikatom cyfrowym i kartom typu smartcard. W innej części projektu zostaną opisane typowe zagrożenia internetowe i odpowiednie środki zaradcze chroniące komputery osobiste. Omówione zostaną także takie zagadnienia jak komunikacja natychmiastowa (instant messaging), wymiana plików w systemach peer-to-peer i społeczności sieciowe. Ostatnia część poświęcona będzie prawnym aspektom przeglądania sieci, gwarancjom prawnym dotyczącym uwierzytelnionych e-maili, a także instytucjom rządowym, których zadaniem jest pomoc obywatelom. Załączony zostanie glosariusz zawierający wszystkie stosowane terminy, jak również umotywowany wykaz wytycznych i najlepszych praktyk, mających na celu właściwe korzystanie z Internetu.

Obecność rządowego partnera, takiego jak CNIPA, gwarantuje projektowi dużą rozpoznawalność i wydaje się być zasadniczym czynnikiem warunkującym skuteczność inicjatywy.

Więcej informacji o innych inicjatywach znajduje się w części [Rząd jako twórca](#).

Kampanie

SaferInternet - Minors & the net [Bezpieczniejszy Internet - małoletni i sieć] (artykuł)¹²

Streszczenie

¹² <http://www.saferinternet.org/www/en/pub/insafe/news/articles/0606/it1.htm>, 12 czerwca 2006 r.

W dniu 19 listopada 2003 r. we Włoszech podpisano ustawę w sprawie „Internetu i małoletnich”. Była ona efektem współpracy między Ministerstwem Komunikacji, przemysłem internetowym i stowarzyszeniami zaangażowanymi w ochronę osób małoletnich.

Szczegóły

Instytucje te pracowały wspólnie w tematycznych podgrupach w najważniejszym do tej pory przedsięwzięciu we Włoszech, które miało na celu określenie standardów i wspólnych narzędzi zapewniających ochronę małoletnich w Internecie. Ustawa została podpisana przez główne stowarzyszenia włoskich dostawców usług internetowych.

Szczególną uwagę poświęcono narzędziom dla małoletnich do bezpiecznego przeszukiwania sieci, a zwłaszcza systemom filtrującym. Po raz pierwszy podjęto próbę usystematyzowania i sklasyfikowania istniejących narzędzi poprzez ocenę ich skuteczności. Przeprowadzono to na podstawie serii wskaźników dotyczących potencjalnych kontekstów zastosowania tych narzędzi.

Oczywiście ustawa jest nie tylko źródłem informacji: zmusza ona także sygnatariuszy do stosowania zróżnicowanych systemów nawigacji, które oddawane są do dyspozycji rodzin, nauczycieli, szkół, bibliotek itp.

Po trzech latach wydaje się, że jedynie kilku dostawców usług internetowych wprowadziło dyrektywę w życie, ze względu na powody finansowe lub dlatego, że ograniczenie nawigacji w sieci może być interpretowane jako zamach na wolność wypowiedzi. Problem ten ma podłoże kulturowe i niełatwo znaleźć jego rozwiązanie. Powszechna tendencja polega na zapewnieniu rodzicom i wychowawcom narzędzi umożliwiających interweniowanie poprzez systemy blokujące na szczelbu panelu kontrolnego lub poprzez tworzenie białych i/lub czarnych list.

Niektóre regiony włoskie wprowadziły takie systemy w celu uregulowania powszechnego dostępu do Internetu w szkołach i bibliotekach. Jednakże nauczanie w zakresie posługiwania się tymi narzędziami jest niewystarczające. Aby pomóc dzieciom w nabraniu zaufania i kształtowaniu umiejętności oceny konieczne są porady i edukacja.

15. Łotwa

Na podstawie odpowiedzi na kwestionariusz oraz uzupełniających informacji z przeprowadzonych rozmów, badań i dodatkowych materiałów dla Łotwy wyszczególniono następujące części:

[Rząd jako twórca prawnych, regulacyjnych i instytucjonalnych postanowień służących poszerzaniu wiedzy](#)

[Władze państwowe jako użytkownik systemów informacyjnych](#)

[Władze lokalne jako użytkownik systemów informacyjnych](#)

[Rząd jako partner przedsiębiorstw i przemysłu](#)

[Rząd jako partner społeczeństwa](#)

[Statystyki i kluczowe wskaźniki wydajności \(KPI\)](#)

Rząd jako twórca prawnych, regulacyjnych i instytucjonalnych postanowień służących poszerzaniu wiedzy

Krajowa strategia poszerzania wiedzy

Nie opracowano krajowej strategii wymagającej poszerzania wiedzy w odniesieniu do rosnącej liczby zagrożeń dla bezpieczeństwa informacji i jego naruszeń.

Prawne, regulacyjne i instytucjonalne postanowienia służące poszerzaniu wiedzy

Na Łotwie istnieją różne prawne, regulacyjne i instytucjonalne rozwiązania służące poszerzaniu wiedzy.

Do prawa karnego Republiki Łotewskiej wprowadzono postanowienia prawne Konwencji Rady Europy o cyberprzestępczości. Są to artykuły: 241. Nieuzasadniony dostęp do systemu komputerowego; 242. Niedozwolone nabycie oprogramowania komputerowego; 243. Niszczenie oprogramowania komputerowego; 244. Rozpowszechnianie wirusów komputerowych; 245. Naruszenie zasad bezpieczeństwa systemu informacyjnego.

Utworzono także wydział ds. cyberprzestępczości, który zajmuje się sprawami z tej dziedziny. Wydział ten podlega Policji Państwowej.

Na mocy decyzji nr 684 Rady Ministrów 19 października 2005 r. przyjęto podrozdział „2.1.3. Społeczeństwo informacyjne” krajowego programu lizbońskiego Łotwy na lata 2005-2008. Celem programu jest zapewnienie bezpieczeństwa sieci i informacji, a także

spójności i interoperacyjności tego bezpieczeństwa, aby utworzyć przestrzeń informacyjną bez granic, w tym:

- Tworzenie systemów bezpiecznego podpisu elektronicznego, co poprawi bezpieczeństwo informacji i zwiększy korzystanie z e-usług
- Tworzenie rządowych i prywatnych zespołów reagujących na naruszenia bezpieczeństwa w Internecie

W dniu 18 października 2005 r. Rada Ministrów ustaliła plan wdrażania posługiwania się nośnikiem bezpiecznego podpisu elektronicznego i stosowania tego rodzaju podpisu.

W dniu 25 maja 2006 r. ustalono i podano do wiadomości publicznej projekt rozporządzenia Rady Ministrów w sprawie procedur umieszczania przez instytucje informacji w Internecie. W projekcie rozporządzenia zawarto także wymogi dotyczące bezpieczeństwa i technicznych parametrów stron internetowych.

Ponadto przyjęto program rozwoju e-administracji na lata 2006-2009. Jedną z podstawowych zasad programu dotyczy bezpiecznych elektronicznych usług administracji rządowej.

„Program wdrażania wytycznych Republiki Łotewskiej w zakresie sektorów komunikacji elektronicznej w latach 2004-2008” obejmuje utworzenie zespołu reagującego na naruszenia bezpieczeństwa w Internecie (CERT/CSIRT), który współpracowałby z Europejską Agencją Bezpieczeństwa Sieci i Informacji (ENISA).

Ministerstwo Transportu planuje poszerzyć uprawnienia krajowego organu regulacyjnego, aby stworzyć odpowiednie regulacje prawne w zakresie zabezpieczania usług świadczonych przez dostawców publicznie dostępnych usług łączności elektronicznej.

Władze państwowe jako użytkownik systemów informacyjnych

Najnowsze inicjatywy i programy poszerzania wiedzy

Brak nowych inicjatyw i programów poszerzania wiedzy.

Planowane jest zrealizowanie projektu „Infrastruktura i usługi technologii informacyjnych i komunikacyjnych” przy wsparciu ze strony Europejskiego Funduszu Rozwoju Regionalnego. W ramach tego projektu zostaną poczynione znaczące inwestycje, które zapewnią bezpieczne przekazywanie informacji między rządem a instytucjami.

Władze lokalne jako użytkownik systemów informacyjnych

Najnowsze inicjatywy i programy poszerzania wiedzy

Brak nowych programów i inicjatyw poszerzania wiedzy; brak planów utworzenia programów i inicjatyw w najbliższej przyszłości.

Rząd jako partner przedsiębiorstw i przemysłu

Najnowsze inicjatywy i programy poszerzania wiedzy

Brak nowych programów i inicjatyw poszerzania wiedzy; brak planów utworzenia programów i inicjatyw w najbliższej przyszłości.

Partnerstwo publiczno-prywatne

Nie utworzono żadnego partnerstwa publiczno-prywatnego; obecnie brak planów utworzenia takiego partnerstwa w najbliższej przyszłości.

Rząd jako partner społeczeństwa

Najnowsze inicjatywy i programy poszerzania wiedzy

Przy wsparciu ze strony Komisji Europejskiej Sekretariat do Zadań Specjalnych ministra odpowiedzialnego za sprawy e-administracji opracował punkt Awareness łotewskiej sieci Insafe w ramach programu Bezpieczniejszy Internet Plus. Punkt ten został utworzony we współpracy z Łotewskim Stowarzyszeniem Internetowym.

Punkt Awareness rozpocznie działalność we wrześniu 2006 r. Do jego zadań będzie należało: kontrolowanie wiedzy o bezpiecznym korzystaniu z Internetu na Łotwie, badanie młodzieży, nauczycieli i rodziców, zapewnianie szkoleń i informowanie społeczeństwa (w szczególności młodzieży, nauczycieli i rodziców) o bezpiecznym korzystaniu z Internetu.

Projekt ten ma trwać 24 miesiące.

Partnerstwo publiczno-prywatne

Nie utworzono żadnego partnerstwa publiczno-prywatnego; obecnie brak planów utworzenia takiego partnerstwa w najbliższej przyszłości.

Statystyki i kluczowe wskaźniki wydajności (KPI)

Statystyki/KPI do oceny sukcesu inicjatywy poszerzania wiedzy

Jak na razie nie stworzono statystyk i KPI, gdyż nie opracowano jeszcze inicjatyw poszerzania wiedzy. Wraz z programami tego typu zostaną opracowane środki pomiaru sukcesu tych inicjatyw.

Znaczenie statystyk/KPI

Uważa się, iż opracowanie wspólnych statystyk i/lub wskaźników jest konieczne do pomiaru skuteczności różnych programów poszerzania wiedzy w danej zbiorowości.



Poradnik dla użytkowników: Jak poszerzyć wiedzę o bezpieczeństwie informacji

16. Liechtenstein

Nie dostarczono żadnych informacji.

17. Litwa

Na podstawie odpowiedzi na kwestionariusz oraz dodatkowych informacji z przeprowadzonych rozmów, badań i dodatkowych materiałów wyszczególniono w przypadku Litwy następujące części:

[Rząd jako twórca prawnych, regulacyjnych i instytucjonalnych postanowień służących poszerzaniu wiedzy](#)

[Władze krajowe jako użytkownik systemów informacyjnych](#)

[Rząd jako partner przedsiębiorstw i przemysłu](#)

[Rząd jako partner społeczeństwa](#)

Rząd jako twórca prawnych, regulacyjnych i instytucjonalnych uregulowań służących poszerzaniu wiedzy

Krajowa strategia poszerzania wiedzy

Krajową strategię bezpieczeństwa IT „Rządowa strategia bezpieczeństwa IT” podpisano 22 grudnia 2001 roku. Ministerstwo Spraw Wewnętrznych było odpowiedzialne za zapewnienie realizacji celów projektu. Jednym z głównych celów tej strategii było podniesienie poziomu kultury urzędników publicznych w kwestii bezpieczeństwa IT. Inne instytucje państwowe również miały motywację, aby zapewnić kształcenie urzędników publicznych w zakresie bezpieczeństwa IT. Aby osiągnąć ten cel, kształcenie przeprowadzono w dwóch etapach. W pierwszym etapie, który miał miejsce w drugim kwartale (Q2) 2003 roku, przygotowano specjalistów ds. bezpieczeństwa IT. W rezultacie piętnastu specjalistów otrzymało międzynarodowy certyfikat bezpieczeństwa. W drugim etapie miały być zorganizowane seminaria i zaplanowano go na okres od drugiego do czwartego kwartału (Q2-Q4) 2002 roku oraz kwartał trzeci (Q3) 2003 roku.

Obecnie obowiązuje nowa Strategia rządowa w zakresie bezpieczeństwa danych elektronicznych i ma być ona stosowana do 2008 roku. Szczególną uwagę przywiązuje się do podniesienia poziomu kultury bezpieczeństwa IT. Biorąc pod uwagę fakt, iż niemożliwe jest zapewnienie bezpieczeństwa IT wyłącznie dzięki staraniom kilku instytucji państwowych, konieczne jest również zwrócenie uwagi na podniesienie poziomu kultury bezpieczeństwa danych elektronicznych w sektorze prywatnym.

Odpowiednie materiały pomocnicze można znaleźć na stronach www.esaugumas.lt i www.vrm.lt (tylko w języku litewskim).

Prawne, regulacyjne i instytucjonalne ustalenia w celu poszerzania wiedzy

Projekt „Wzmocnienie kompetencji organów odpowiedzialnych za bezpieczeństwo IT i danych” wdrożono, korzystając z funduszy PHARE w 2005 roku.

Projektem zarządzał Departament ds. Polityki Informacyjnej Ministerstwa Spraw Wewnętrznych. Określono następujące cele:

- Poszerzenie administracyjnych i operacyjnych kompetencji instytucji państwowych odpowiedzialnych za bezpieczeństwo IT i danych
- Wyrównanie litewskiego systemu ochrony IT i danych z wymogami acquis i wymogami międzynarodowymi
- Zapewnienie odpowiedniego poziomu bezpieczeństwa IT i danych

Osiągnięto następujące rezultaty:

- Dokonano przeglądu przepisów i innych dokumentów ustawodawczych w sferze IT i bezpieczeństwa danych elektronicznych oraz przygotowano konieczne projekty
- Przyjęto i opublikowano metodologię w zakresie oceny IT i bezpieczeństwa danych elektronicznych (analiza ryzyka)
- Przedstawiono Ministerstwu Spraw Wewnętrznych projekt wymogów dotyczących IT i danych elektronicznych
- Przedstawiono projekt wymogów bezpieczeństwa w związku z bezpieczną siecią rządową Ministerstwu Spraw Wewnętrznych i przedsiębiorstwu państwowemu „Infostruktūra” - dostawcy usług dla Bezpiecznej Państwowej Sieci Przekazywania Danych (Secure State Data Communication Network - SSDCN)

Ministerstwo Transportu i Komunikacji, Departament ds. Polityki Informacyjnej Ministerstwa Spraw Wewnętrznych oraz Komitet ds. Rozwoju Społeczeństwa Informacyjnego podlegający Rządowi Republiki Litewskiej i Regulacyjny Organ ds. Komunikacji (RRT) pracują nad Ustawą o Bezpieczeństwie Sieci i Informacji (Network and Information Security (NIS) Law). Dostępny jest już projekt. Przyjęcie ustawy planowane jest przed końcem roku 2006. Do celów Ustawy NIS zalicza się m.in. koordynację polityki informacyjnej oraz poszerzanie wiedzy użytkowników.

Regulacyjny Organ ds. Komunikacji (RRT) razem z Ministerstwem Transportu i Komunikacji oraz Departamentem ds. Polityki Informacyjnej Ministerstwa Spraw Wewnętrznych są w trakcie tworzenia zespołu CERT w obrębie RRT, który będzie odpowiedzialny za koordynację działań istniejących litewskich CERT i ISP w zakresie zarządzania komputerowymi, sieciowymi i informacyjnymi incydentami z zakresu bezpieczeństwa.

Utworzenie CERT przewidziane jest na koniec 2006 roku. Jednym z zadań CERT będzie kształcenie użytkowników i poszerzanie wiedzy.

Regulacyjny Organ ds. Komunikacji Republiki Litewskiej, Stowarzyszenie Banków Litewskich i Stowarzyszenie Infobalt (ze 145 członkami sektora ICT) podpisały Memorandum dotyczące postępu w zakresie bezpieczeństwa informacji i sieci 23 listopada 2005 roku. Strony zgodziły się na utworzenie stałego Komitetu ds. Wdrażania Memorandum (dalej zwanego Komitetem), reprezentowanego przez upoważnionych przedstawicieli stron. Do głównych zadań Komitetu należy współpraca w dziedzinie przygotowywania i wdrażania publicznych kampanii mających na celu poszerzanie wiedzy w zakresie bezpiecznego korzystania z ICT, a także współpraca w zakresie zachęcania społeczeństwa do korzystania z narzędzi bezpieczeństwa (oprogramowanie antywirusowe i inne), które mogą chronić przed incydentami związanymi z bezpieczeństwem informacji i sieci.

Z inicjatywy RRT 29 i 30 marca 2006 roku odbyły się w Wilnie warsztaty szkoleniowe TRANSITS (*Training of Network Security Incident Teams Staff—Szkolenie członków zespołów ds. incydentów związanych z bezpieczeństwem sieci*) dla CSIRT (*Computer Security Incidents Response Team – Zespołu Reagowania na Incydenty związane z Bezpieczeństwem Komputerowym*). Warsztaty te zostały zorganizowane przez TERENA (*Trans-European Research and Education Networking Association - Ogólnoeuropejskie Stowarzyszenie Sieci Naukowo-Badawczych i Edukacyjnych*) i FIRST (*Forum of Incident Response and Security Teams - Forum Zespołów ds. Bezpieczeństwa i Reagowania na Wypadki*) przy współpracy z ENISA. Wydarzenie było sponsorowane przez ENISA. Kurs poświęcony był operacyjnemu, organizacyjnemu i prawnemu aspektom reagowania na incydenty. Był on skierowany do profesjonalistów, którzy albo są członkami (lub przyszłymi członkami) istniejących zespołów ds. bezpieczeństwa komputerowego lub którzy będą zaangażowani w tworzenie takiego zespołu w swoich organizacjach. 25 uczestników z 13 krajów, zarówno z sektora publicznego, jak i prywatnego wzięło udział w tym kursie: Litwa (7), Estonia (3), Polska (1), Finlandia (2), Austria (1), Holandia (2), Portugalia (1), Niemcy (1), Zjednoczone Królestwo (2), Białoruś (1), Azerbejdżan (2), Kirgistan (1), a nawet Afganistan (1). Pierwsza europejska konferencja poświęcona bezpieczeństwu sieci i informacji, pod hasłem *Gotowość radzenia sobie z incydentami związanymi z bezpieczeństwem sieci i informacji* odbyła się w dniach 24-25 listopada 2005 roku w Wilnie, na Litwie. Została ona zorganizowana przez ENISA, RRT i Ministerstwo Transportu i Komunikacji. W konferencji uczestniczyło około 160 osób z całej Europy i poświęcono jej wiele uwagi w mediach. Druga europejska konferencja poświęcona bezpieczeństwu sieci i informacji, pod hasłem *Zapewnienie bezpieczeństwa informacji i sieci – wskazówki dotyczące zarządzania bezpieczeństwem w środowiskach publicznych i biznesowych*, planowana jest na listopad 2006 roku na Litwie. W tym roku konferencję zorganizują ENISA, RRT, Ministerstwo Transportu i Komunikacji oraz Ministerstwo Spraw Wewnętrznych.

Materiały pomocnicze można znaleźć pod następującymi adresami: www.esaugumas.lt, www.vrm.lt (tylko po litewsku) i www.securityconference.rtt.lt.

Władze krajowe jako użytkownik systemów informacyjnych

Najnowsze programy i inicjatywy poszerzania wiedzy

Projekt „Wzmocnienie kompetencji organów odpowiedzialnych za bezpieczeństwo IT i danych” wdrożono, korzystając z funduszy PHARE, w 2005 roku.

Zgodnie z tym projektem, przeszkolono 15 ekspertów z różnych instytucji, którzy zajmują się oceną bezpieczeństwa IT i konsultingiem. Ponad 200 pracowników instytucji publicznych przeszkolono w dziedzinie bezpieczeństwa IT, korzystając z przygotowanego programu szkoleniowego (<http://www.esaugumas.lt/VRM/VRM/index.html>). Programy szkoleniowe stworzone w ramach projektu są dostępne dla personelu instytucji państwowych na płycie CD lub w Internecie.

Rządowa strategia bezpieczeństwa danych elektronicznych do 2008 roku ma na celu osiągnięcie następujących celów w zakresie wiedzy na temat bezpieczeństwa IT:

- Gruntowne wykształcenie urzędników i pracowników publicznych pracujących na umowę o pracę w dziale bezpieczeństwie danych elektronicznych. Ministerstwo Spraw Wewnętrznych jest odpowiedzialne za zorganizowanie seminariów i przygotowanie programu szkoleniowego (w tym treści szkolenia na odległość). Jest to planowane na okres od Q2 2006 roku do Q4 2007 roku.
- Promowanie wiedzy z zakresu znaczenia bezpieczeństwa danych elektronicznych. Należy to do obowiązków Ministerstwa Spraw Wewnętrznych, Ministerstwa Transportu i Komunikacji, Komitetu ds. Rozwoju Społeczeństwa Informacyjnego podlegającego Rządowi Republiki Litewskiej i Regulacyjnego Organu ds. Komunikacji. W okresie od Q2 2006 roku do Q4 2007 roku zamierza się udostępnić na płycie CD lub na stronie internetowej <http://www.esaugumas.lt> informacje dotyczące bezpieczeństwa danych elektronicznych oraz rosnącej liczby przypadków naruszenia bezpieczeństwa i liczby zagrożeń dla bezpieczeństwa. Ministerstwo Edukacji i Nauki, Ministerstwo Spraw Wewnętrznych oraz Regulacyjny Organ ds. Komunikacji zamierzają przedstawić nowe programy szkoleniowe z zakresu ochrony danych elektronicznych dla szkół średnich i uczelni wyższych. Jest to jeden z priorytetów, aby poszerzać wiedzę o bezpieczeństwie IT wśród uczniów i studentów (ta grupa stanowi głównych użytkowników Internetu i innych zaawansowanych technologii)

Rząd jako partner przedsiębiorstw i przemysłu

Dostawcy usług internetowych (ISP)

Spotkania krajowych ISP, uczestników rynku i przedstawicieli Regulacyjnego Organu ds. Komunikacji poświęcone NIS oraz utworzenie krajowego CERT miały miejsce w okresie od maja do lipca 2005 roku i nadal trwają.

Media

Należy zwrócić uwagę, że w poniższym przykładzie media wykorzystane są jako kanał dotarcia do innych grup docelowych i nie są przedstawione jako odrębna grupa docelowa.

Ankieta mająca na celu określenie sytuacji NIS rozpoczęła się w październiku 2005 roku. Objęła ona użytkowników Internetu, organizacje i ISP. Wyniki: 78% użytkowników Internetu miało w swoich komputerach wirusy, 63% otrzymywało spam. 29% organizacji i 45% ISP stosowało najnowszą strategię NIS, natomiast 23% ISP nie stosowało żadnej strategii NIS. Ankiecie wraz z komentarzami poświęcono dużo uwagi w mediach. Pełen raport dotyczący ankiety można ściągnąć z następującej strony internetowej: (http://www.esaugumas.lt/get_file.php?file=RDovTmV3UIJUL3NhdWcvbS9tX2ZpbGVzL3dmaWxlcY9maWxIOc5wZGY7SW1vbmVzX0lQVF9hcGtsYXVzYS5wZGY7Ow)

Ponadto odbyła się emisja programów telewizyjnych i radiowych dotyczących zagadnień NIS, z udziałem przedstawicieli RRT i innych państwowych instytucji.

Partnerstwo publiczno-prywatne

Skuteczne partnerstwo publiczno-prywatne (w dziedzinie poszerzania wiedzy i edukacji/szkolenia). Nowa strona internetowa poświęcona poszerzaniu wiedzy o NIS została uruchomiona w lutym 2006 roku. Strona ta, www.esaugumas.lt, jest przeznaczona dla użytkowników Internetu, MŚP i administratorów sieci instytucji państwowych i ma być interaktywnym forum dotyczącym NIS dla wszystkich zainteresowanych stron. Są tu dostępne artykuły, najświeższe wiadomości, forum dyskusyjne, porady w zakresie zagadnień NIS, narzędzia dla użytkowników służące do unikania incydentów związanych z NIS itd.

Przy współpracy z bankami RRT przygotował broszurę dla użytkowników zawierającą informacje o phishingu i sposobach rozpoznawania tych ataków oraz zabezpieczania się przed nimi. Rozprowadzono 200 000 broszur we wszystkich regionach litewskich.

RRT przy współpracy ze znanymi sprzedawcami systemów bezpieczeństwa pracował nad projektem „Chroń swój komputer!” w celu stworzenia narzędzia pomagającego użytkownikom prywatnym w zwiększeniu bezpieczeństwa ich komputerów. Opracowano i umieszczono na płycie CD zbiór niezbędnych programów zabezpieczających (przed wirusami, spamem, spyware i innymi) oraz odpowiednich informacji dotyczących bezpiecznego korzystania z Internetu. W czerwcu 2006 roku rozprowadzono bezpłatnie w regionach litewskich około 100 000 takich płyt CD. Końcowy etap projektu omówiono dokładnie w mediach.

W ramach programu „Bezpieczniejszy Internet” trwają projekty takie jak „Bezpieczniejsza Cyfrowa Litwa” (poszerzanie wiedzy użytkowników) i „Hotline - Litwa” (skierowany przeciwko szkodliwym informacjom w Internecie). Partnerami projektów są „Bitė Lietuva” s.a., Ministerstwo Edukacji i Nauki, Komitet ds. Rozwoju Społeczeństwa Informacyjnego podlegający Rządowi Republiki Litewskiej, Organ

Regulujący ds. Komunikacji i inne instytucje publiczne i rządowe. Rama czasowa projektów obejmuje okres od 2005 do 2007 roku.

Rząd jako partner dla społeczeństwa

Najnowsze programy i inicjatywy poszerzania wiedzy

Zobacz część [Rząd jako partner \(Przedsiębiorstw\)](#)

18. Luksemburg

W przypadku Luksemburga - na podstawie odpowiedzi na kwestionariusz i innych dodatkowych informacji z przeprowadzonych rozmów, badań i dodatkowego materiału – wyszczególniono następujące części:

[Rząd jako twórca prawnych, regulacyjnych i instytucjonalnych postanowień służących poszerzaniu wiedzy](#)

[Władze krajowe jako użytkownik systemów informacyjnych](#)

[Władze lokalne jako użytkownik systemów informacyjnych](#)

[Rząd jako partner przedsiębiorstw i przemysłu](#)

[Rząd jako partner społeczeństwa](#)

[Statystyki i kluczowe wskaźniki wydajności \(KPI\)](#)

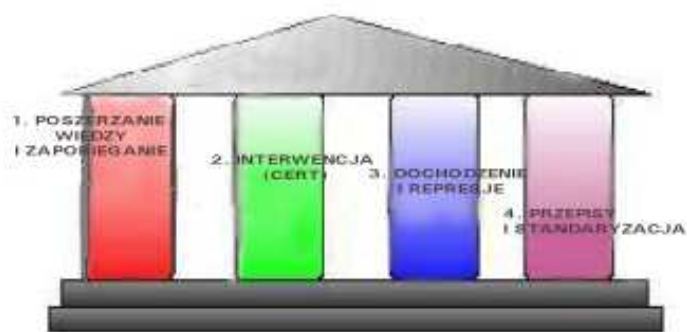
[Doświadczenia](#)

Rząd jako twórca prawnych, regulacyjnych i instytucjonalnych postanowień służących poszerzaniu wiedzy

Krajowa strategia poszerzania wiedzy

Luksemburg stosuje krajową strategię w zakresie bezpieczeństwa informacji od kilku lat. Strategia ta oparta jest na czterech filarach:

1. Poszerzanie wiedzy i zapobieganie
2. Interwencja (CERT)
3. Dochodzenie i represje
4. Przepisy i standaryzacja



Charakter i zakres strategii

Jest to krajowa strategia obejmująca możliwie jak największą liczbę kluczowych stron zainteresowanych. Strategia ta skierowana jest zarówno do sektora publicznego, jak i prywatnego, które jednocześnie pełnią rolę punktu docelowego i źródła.

Obowiązki

Rząd, a zwłaszcza Ministerstwo Gospodarki i Handlu Zagranicznego, koordynuje różne projekty. Obowiązki związane są z poszczególnymi stronami zainteresowanymi. Rząd luksemburski zdołał zgromadzić wiele różnych stron zainteresowanych. Wywodzą się one z rządu, środowiska akademickiego, instytutów badawczych i przemysłu. Koordynacja odbywa się za pośrednictwem wspólnej platformy. Platforma ta omawia priorytety, budżety i formułuje zalecenia dla rządu centralnego.

Cele

Celem jest osiągnięcie konsensusu w sprawie sposobu wdrożenia strategii w różnych regionach i w obrębie różnych zbiorowości Luksemburga. Ważne jest, aby poznać różne potrzeby po to, by zainwestować ograniczone budżety w najważniejsze projekty w różnych dziedzinach krajowego planu bezpieczeństwa. Bardzo ważna jest również możliwość wykorzystania synergii.

Sektory docelowe

Sektory docelowe są bardzo zróżnicowane, obejmują one rząd centralny, przemysł, MŚP i oczywiście obywateli, w tym dzieci.

Określone działania

Określone działania można uszeregować według następujących dziedzin:

- Poszerzanie wiedzy obywateli na temat zagrożeń związanych z Internetem, takich jak złośliwe oprogramowanie i ataki. Celem jest pomoc dla mieszkańców w zakresie właściwego zabezpieczania się po to, by mieć korzyść z Internetu. Powinni oni korzystać z usług e-rządu, e-zdrowia i e-handlu.
 - Podstawowa znajomość zagrożeń
 - Wdrażanie podstawowych środków bezpieczeństwa
 - Podstawowa znajomość analizy ryzyka
 - Skupienie się na Bluetooth i WiFi
- Poszerzanie wiedzy dzieci w zakresie zagrożeń związanych z Internetem przy pomocy specjalnych treści, dostosowanych do potrzeb dzieci. Dzieci powinny być poinformowane o istnieniu niedozwolonych i szkodliwych treści oraz o ryzyku związanym z chatem:
 - Szkodliwa treść
 - Chat
 - Podstawowa znajomość zagrożeń
 - Skupienie się na Bluetooth i WiFi
- Poszerzanie wiedzy MŚP. Zasadniczym celem jest uświadomienie MŚP prawdziwej wartości różnych aktywów, jakie mają w swoich firmach. Większość MŚP nie jest świadoma wpływu, jaki może mieć dany incydent. MŚP uczone są również tego, jak wdrażać środki bezpieczeństwa. Zaznajamia się je z pojęciem

zagrożeń i udostępnia się im materiały przydatne do opracowania strategii bezpieczeństwa (analiza ryzyka i zastosowanie strategii):

- Pojęcie analizy ryzyka
 - Ocena zasobów
 - Pojęcie strategii bezpieczeństwa (stałe polepszenie)
 - Znajomość zagrożeń
 - Znajomość zasad wdrażania środków bezpieczeństwa
- Poszerzanie wiedzy w sektorze przemysłowym, głównie w dziedzinie przemysłowego szpiegostwa. Większość luksemburskich firm nie jest świadoma tego zagrożenia. Przygotowywana jest duża kampania dotycząca tego problemu. Będzie ona skierowana do sektora przemysłowego i banków:
 - Świadomość szpiegostwa przemysłowego
 - Świadomość zagrożeń związanych z inżynierią społeczną
 - (bezpieczeństwo techniczne jest dobrze rozwinięte)

Ramy czasowe i podział obowiązków

Obywatele: wszystkie działania na ten rok. Obowiązki: Ministerstwo Gospodarki i Handlu Zagranicznego, kafejki internetowe.

Dzieci: wszystkie działania na ten rok. Obowiązki: Ministerstwo Gospodarki i Handlu Zagranicznego, Ministerstwo Edukacji, Serwis młodzieżowy

MŚP: Ministerstwo Gospodarki i Handlu Zagranicznego, Izby Gospodarcze, projekty badawczo-rozwojowe współfinansowane przez UE

Przemysł: Ministerstwo Gospodarki i Handlu Zagranicznego, Ministerstwo Stanu, Ministerstwa, Policja,

Strony internetowe i/lub odpowiednie materiały

Obywatele i MŚP: Strona internetowa CASES (Cyberworld Awareness Security Enhancement Structure): www.cases.lu. Szczegółowe informacje dotyczące zagrożeń, ostrzeżenia dotyczące decydujących słabych punktów, wskazówki odnoszące się do tego, jak właściwie skonfigurować [routery ADSL](#) wspierające standard WiFi sprzedawane w Luksemburgu i jak rozpoznawać ataki [phishingu](#). Wiele wskazówek jest dostępnych na stronie internetowej. Grupa ta jest bardzo dumna ze wskazówek dotyczących opracowania analizy ryzyka i stworzenia strategii bezpieczeństwa IT. Dostępne są specjalne ulotki poświęcone różnym tematom.

Ogólne informacje dotyczące: [CSRRT-LU](#) (Computer Security Research and Response Team - Luksemburg). Specjalnie zaprojektowany wcześniej ostrzegający wykrywacz złośliwego oprogramowania: na stronie [CSRRT-LU](#). Te dwa ostatnie zasoby nie są zaprojektowane dla obywateli i MŚP, lecz zawierają cenne informacje o zagrożeniach.

Opracowywane są ulotki i naklejki

Dzieci: www.mysecureit.lu; www.petitweb.lu, projekt zapoczątkowany przez TELINDUS i rząd: bezpieczniejszy Internet; powstaje również specjalny raport o bezpieczeństwie w Internecie dla dzieci w Luksemburgu. Duża kampania przeprowadzana we wszystkich szkołach razem z CLUSSIL (Club de la Sécurité des Systèmes d'Information Luxembourgais) i Ministerstwem Edukacji: [Prezentacja](#)

Przemysł: Nowe przedsięwzięcie; dostępne są wyłącznie projekty dotyczące szpiegostwa przemysłowego. Wkrótce będą dostępne specjalne ulotki dotyczące bezpieczeństwa i inżynierii społecznej.

Prawne, regulacyjne i instytucjonalne postanowienia służące poszerzaniu wiedzy

Rząd w Luksemburgu stworzył platformę z myślą o bezpieczeństwie informacji, której hostem jest instytut badawczy. Platforma ta gromadzi osoby związane z przemysłem, ośrodkami badawczo-rozwojowymi, rządem i działalnością badawczą.

W Luksemburgu obowiązują przepisy przeciwdziałające cyberprzestępczości. Luksemburg stara się kłaść większy nacisk na certyfikację niż na regulacje prawne. Certyfikat przyznawany w e-handlu został stworzony po to, by budować zaufanie do e-handlu i zwiększyć bezpieczeństwo w e-handlu.

Luksemburg chce uświadomić wszystkim zainteresowanym stronom ich obowiązki, a ustawodawstwo, zgodnie z panującym przekonaniem, nie jest właściwym podejściem; certyfikacja oparta na powszechnym konsensusie jest szybsza i bardziej skuteczna, gdyż jest pozytywnym podejściem. Łatwiej jest również zwiększyć bezpieczeństwo, zmieniając poziom certyfikacji niż przyjąć ustawodawstwo, co zazwyczaj jest bardzo powolnym procesem.

Władze państwowe jako użytkownicy systemów informacyjnych

Najnowsze programy i inicjatywy poszerzania wiedzy

Ministerstwo Gospodarki i Handlu Zagranicznego zainicjowało pierwszy projekt w pełni skupiający się na bezpieczeństwie w ministerstwach i organach administracji. W czasie tego projektu przeprowadzana jest analiza ryzyka w ministerstwie i sporządzana jest strategia bezpieczeństwa informacji. Do przeprowadzenia tej analizy ryzyka stosowana jest metodologia EBIOS. Doświadczenia zdobyte w czasie tego projektu przekazywane są do innych ministerstw, które chcą zainicjować ten proces.

W ramach tego projektu pracownicy administracji rządowej otrzymają zaprojektowane specjalnie dla



nich materiały poszerzające wiedzę. Wyniki analizy ryzyka wykazały, że Ministerstwo Gospodarki i Handlu Zagranicznego ma bardzo dużą potrzebę poufności informacji. Zostaną opracowane specjalne materiały poświęcone zagadnieniom inżynierii społecznej i bezpieczeństwa fizycznego, które stanowią dwa główne zagrożenia w rządzie luksemburskim. Dostęp do tych materiałów będzie ograniczony. W ministerstwie materiały będą udostępniane przy pomocy ulotek, plakatów i Internetu. Osoby zajmujące się dziedzinami objętymi szczególną poufnością przejdą specjalne kursy.

Celem tego projektu jest wdrażanie środków zwiększonego bezpieczeństwa w Ministerstwie Gospodarki i Handlu Zagranicznego oraz pokazanie innym instytucjom rządowym, jak postępować w tej dziedzinie. Przekazanie wiedzy jest jedną z głównych kwestii tego projektu.

Krajowy departament IT wdraża podobny projekt w celu napisania nowej strategii bezpieczeństwa IT. Praca ta oparta jest na innej metodologii: „BSI Grundschutzhandbuch” i metodzie MEHARI autorstwa CLUSIF (Club de la Sécurité de l'Information Francis). Obydwa projekty wdrażane są z pomocą Centre de Recherche Public Henri Tudor (CRP Henri Tudor) i Uniwersytetu Luksemburskiego. Przekazanie wiedzy uznawane jest za najważniejszą kwestię w tej dziedzinie.

To podwójne podejście wybrano po to, by móc porównać różne metody w praktyce i by móc opracować dla rządu centralnego podejście oparte na dobrych praktykach. W ostatnich kilku latach osiągnięto wysoki poziom wiedzy w dziedzinie analizy ryzyka i strategii bezpieczeństwa.

Władze lokalne jako użytkownik systemów informacyjnych

Najnowsze programy i inicjatywy poszerzania wiedzy

Jeszcze nie rozpoczęte. Trwają tylko małe projekty koordynowane przez departament IT zbiorowości luksemburskich. Koordynatorzy projektu czekają na doświadczenia zdobyte w ramach projektów wdrażanych w rządzie centralnym.

CRP Henri Tudor, Uniwersytet Luksemburski i projekt CASES otrzymają zadanie rozpowszechnienia wiedzy na poziomie władz lokalnych.

Rząd jako partner przedsiębiorstw i przemysłu

Małe i średnie przedsiębiorstwa (MŚP)

Dane statystyczne można znaleźć [na stronie internetowej STATEC](#).

Główną kwestią w zakresie poszerzania wiedzy MŚP jest przede wszystkim przekonanie MŚP do oszacowania rzeczywistej wartości aktywów, które posiadają i których powinny chronić. Dzięki licznym kontaktom z MŚP odkryto, że zbyt nisko szacują one prawdziwą wartość swoich aktywów. Zbyt nisko szacują również rzeczywiste zagrożenia. Szpiegostwo przemysłowe ma miejsce na najniższym poziomie; miały miejsce

przypadki, w których jeden sklep szpiegował sąsiadujący sklep ze względu na ceny i bazę danych klientów. Podejmowane są próby przekazania MŚP wiadomości dotyczących poznania rzeczywistej wartości aktywów oraz rzeczywistych zagrożeń.

Odbywa się to poprzez analizę ryzyka i wskazówki z zakresu strategii bezpieczeństwa informacji. Pełne zrozumienie pojęcia ryzyka: $RZYKO = \text{słaby punkt} * \text{zagrożenie} * \text{wpływ}$ jest kluczową kwestią. Jeśli MŚP rozumieją tę relację, zostaną przymuszone przez ograniczenie wpływów do ograniczenia słabych punktów oraz podjęcia środków zaradczych i zapobiegawczych przeciwko zagrożeniom. W rzeczywistości jest to, zgodnie z opisem zawartym w dokumencie OECD, problem kulturowy.

W związku z niskim poziomem bezpieczeństwa w dziedzinie WiFi opracowano wskazówki oparte na *flash movies* oraz na tym, jak zabezpieczyć routery sprzedawane w Luksemburgu. Procent niezabezpieczonych routerów WiFi stosowanych w Luksemburgu wciąż jest bardzo wysoki.

Na ten czas głównymi kanałami wykorzystywanymi do przekazywania informacji nadal są: strona internetowa, artykuły publikowane na łamach gazet i warsztaty.

Niestety nie znaleziono sposobu na zwiększenie motywacji jednostek rozpowszechniających wiedzę. Specjalistyczna wiedza tych jednostek nadal wydaje się być bardzo ograniczona i z tego powodu nie ośmielają się podejmować tematów z zakresu bezpieczeństwa informacji. Można również zauważyć, że często w mediach w sposób niepoprawny używane jest słownictwo, mylone są terminy takie jak hacker i cracker.

Dostawcy usług internetowych (ISP)

CASES [przeanalizował routery ADSL](#) sprzedawane przez luksemburskich ISP. Opublikowano mocne i słabe strony routerów. Na skutek tej publikacji główny ISP (P&T) zmienił jeden z routerów, gdyż nie był on wystarczająco bezpieczny.

Kampania pokazuje ludziom, jak zabezpieczyć router poprzez odpowiednią konfigurację WAN (odcięcie niepotrzebnych usług) i jak poprawnie i bezpiecznie złożyć sieć WiFi. CASES zwrócił się również podczas krajowej konferencji do ISP o współpracę z państwowymi władzami w zakresie lepszego informowania klientów o tym, jak zabezpieczać komputery.

Media

Należy zauważyć, że w poniższym przykładzie media wykorzystane są jako kanał, poprzez który można dotrzeć do innych grup, i nie są przedstawione jako oddzielna grupa docelowa sama w sobie. CASES nie znalazł jeszcze sposobu na to, jak przekonać media, żeby podjęły temat bezpieczeństwa informacji.

Jednak w ramach projektu zwrócono się do jednej z najpopularniejszych stron dla młodych ludzi o współpracę w dziedzinie poszerzania wiedzy. Nie doprowadziło to jeszcze do projektu, ale współpraca wygląda obiecująco.

Publiczno-prywatne partnerstwo

Skuteczne partnerstwo publiczno-prywatne (w dziedzinie poszerzania wiedzy i edukacji/szkolenia) Współpraca z następującymi inicjatywami prywatnymi przebiega bez problemów:

- www.petitweb.lu
- www.internetmonitor.lu
- www.mysecureit.lu
- www.party.lu

Projekt CASES nie przystąpił jeszcze do publiczno-prywatnego partnerstwa z głównymi sprzedawcami, ponieważ Luksemburg chce, aby jego inicjatywy pozostały niezależne.

Jednak główna kampania planowana jest razem z ISP. CASES jest odpowiedzialny za podstawową treść, taką jak bezpieczna konfiguracja routerów ADSL sprzedawanych w Luksemburgu. Treść ta będzie stanowiła podstawę bliskiej współpracy pomiędzy projektem CASES a ISP.

Jeśli chodzi o sektor finansowy, CASES planuje współpracę z ABBL (www.abbl.lu), stowarzyszeniem bankowców, aby promować certyfikację bezpieczeństwa ISO 27001. Współpraca ta rozpocznie się pod koniec maja 2006 roku. Takie samo podejście obrano w odniesieniu do przemysłu.

Zwiększa się znaczenie PPP, ale CASES nie koniecznie chce stowarzyszać się ze sprzedawcami systemów zabezpieczających, lecz ze zbiorowościami, które powoli zaczynają dostrzegać zalety wczesnej kampanii mającej na celu poszerzenie wiedzy. Z pewnością zwiększy się liczba inicjatyw w tej dziedzinie.

Rząd jako partner społeczeństwa

Najnowsze programy i inicjatywy poszerzania wiedzy

Projekt CASES w pełni obejmuje kampanie mające na celu poszerzanie wiedzy, skierowane do obywateli (dzieci i dorosłych; lecz nie do starszych użytkowników Internetu). CASES organizuje konferencje dla dorosłych w zbiorowościach lokalnych i organizuje pokazy na targach.

Wraz z Ministerstwem Edukacji zorganizowano dla dzieci kampanię mającą na celu poszerzanie wiedzy. Każde trzynastoletnie dziecko w Luksemburgu bierze udział w takiej kampanii, organizowanej we wszystkich szkołach w Luksemburgu. W czasie tych pokazów uświadamia się dzieciom zagrożenia dla bezpieczeństwa informacji

(zagrożenia techniczne, ale również bezpieczeństwo w odniesieniu do chatu). Informacje można znaleźć na stronie internetowej www.mysecureit.lu i na stronie [CASES](#).

CASES opracowuje portal poświęcony bezpieczeństwu informacji, przeznaczony do nauki drogą elektroniczną dla obywateli i MŚP. Opiera się on na obszernej treści strony CASES i powinien być publicznie dostępny pod koniec 2006 roku.

Statystyki i i kluczowe wskaźniki wydajności (KPI)

Statystyki/KPI do oceny sukcesu inicjatywy poszerzania wiedzy

Nie określono jeszcze KPI.

Zdobyte doświadczenie

Odkryto, że większość routerów ADSL sprzedawanych w kraju była w nieodpowiednim stanie (np. podstawowe ustawienia nie były wystarczająco zabezpieczone). Obecnie dzięki współpracy z ISP sytuacja ta zmienia się lub zmieniła. Ponadto ważne było, aby współpracować z ISP w celu usprawnienia procesu reagowania na zawiadomienia klientów, których komputery zostały zainfekowane.

19. Malta

Na podstawie odpowiedzi na kwestionariusz oraz dodatkowych informacji z przeprowadzonych rozmów, badań i dodatkowych materiałów w przypadku Malty wyszczególniono następujące części.

[Rząd jako twórca prawnych, regulacyjnych i instytucjonalnych postanowień służących poszerzaniu wiedzy](#)

[Władze państwowe jako użytkownik systemów informacyjnych](#)

[Władze lokalne jako użytkownik systemów informacyjnych](#)

[Rząd jako partner przedsiębiorstw i przemysłu](#)

[Rząd jako partner społeczeństwa](#)

[Statystyki i kluczowe wskaźniki wydajności \(KPI\)](#)

Rząd jako twórca prawnych, regulacyjnych i instytucjonalnych postanowień służących poszerzaniu wiedzy

Krajowa strategia poszerzania wiedzy

Ministerstwo Inwestycji, Przemysłu i Technologii Informacyjnej opracowało Krajową Strategię ICT, która trwała od 2004 do 2006 roku. Strategia ta obejmuje część poświęconą bezpieczeństwu informacji. Ta część strategii przewiduje kilka inicjatyw poszerzających wiedzę, skierowanych zarówno do dzieci, jak i rodziców oraz podmiotów handlowych. Jednym z celów jest poszerzanie wiedzy o rosnącej liczbie naruszeń bezpieczeństwa informacji.

Zobacz <http://www.miti.gov.mt/site/page.aspx?pageid=4>, żeby uzyskać więcej informacji.

Ponadto wcześniej w 2006 roku powołano Krajową Grupę Roboczą ds. e-bezpieczeństwa (składającą się z wielu różnych stron zainteresowanych), której głównym celem było opracowanie i wdrożenie krajowej Strategii i Planu Akcji poświęconych e-bezpieczeństwu na okres 2006 – 2008. Strategia ta będzie obejmowała działania mające na celu poszerzanie wiedzy, poruszając wszelkie aspekty e-bezpieczeństwa – od bezpieczeństwa sieci i informacji poprzez cyberprzestępczość do ochrony danych.

Prawne, regulacyjne i instytucjonalne postanowienia służące poszerzaniu wiedzy

Jak wcześniej wskazano, utworzona została Krajowa Grupa Robocza ds. e-bezpieczeństwa. Zakres działań planu strategicznego obejmuje między innymi

rozpoznanie wszelkich luk i przedstawienie zaleceń dotyczących rozwiązania problemu tych luk w odniesieniu do:

- struktur instytucjonalnych i mechanizmów administracyjnych koniecznych do zajęcia się kwestiami związanymi z e-bezpieczeństwem w sposób holistyczny
- kompetencji wymaganych w sektorze publicznym i prywatnym do tego, aby właściwie zajmować się sprawami bezpieczeństwa elektronicznego

Jeśli chodzi o poszerzanie wiedzy, grupa robocza ma ukończyć przegląd w zakresie bezpieczeństwa ICT, w ramach którego zostanie zmierzona świadomość e-bezpieczeństwa wśród obywateli i przedsiębiorstw i zostaną zalecone środki, które można podjąć w celu zminimalizowania ryzyka na różnych poziomach.

Władze państwowe jako użytkownik systemów informacyjnych

Najnowsze programy i inicjatywy poszerzania wiedzy

W następstwie ustanowienia różnych usług e-administracji, Ministerstwo Przemysłu, Inwestycji i Technologii Informacyjnej (MIIT) zainicjowało projekt eID. Przy pomocy elektronicznej karty identyfikacyjnej (eID), użytkownik będzie mógł mieć dostęp do wszystkich usług elektronicznych oferowanych przez rząd w bezpieczny sposób.

Władze lokalne jako użytkownik systemów informacyjnych

Najnowsze programy i inicjatywy poszerzania wiedzy

Dotychczas organizowane programy były głównie prowadzone przez rząd centralny. Jednak należy zwrócić uwagę na to, że dzięki niewielkiemu obszarowi Malty kampanie na poziomie krajowym są tam bardziej wykonalne niż w przypadku większych krajów.

Rząd jako partner przedsiębiorstw i przemysłu

Małe i średnie przedsiębiorstwa (MŚP)

Oczekuje się, że jedną z najbardziej wpływowych inicjatyw w tym zakresie będzie Micro-Enterprise Acceleration Programme (MAP), w wyniku którego zorganizowano kurs szkoleniowy poświęcony temu, jak przedsiębiorstwa mogą korzystać z ICT, aby zwiększyć swoją wydajność. Inicjatywa koordynowana jest przez MIIT i HP, wiodącą organizację w dziedzinie ICT, i powinna ruszyć w nadchodzących miesiącach.

Podstawowym celem tego kursu jest ukazanie, jak mikro-przedsiębiorcy mogą zwiększyć wydajność swoich firm korzystając z ICT. Aby osiągnąć ten cel, program Smart Technology for a Smarter Business™ koncentruje się na pomaganiu mikro-przedsiębiorcom w następujących dziedzinach:

- Zdobycie wiedzy w zakresie ICT i umiejętności swobodnego korzystania z ICT
- Zdobycie wiedzy i umiejętności w zakresie firmowych aplikacji ICT

- Wykorzystywanie ICT w celu zwiększenia wydajności i wzrostu firmy

Drugorzędnym celem tego kursu jest zapewnienie uczestnikom możliwości ocenienia własnych potrzeb w związku z dalszym szkoleniem i inwestowaniem w technologię. Wreszcie kurs ten oferuje uczestnikom możliwość wymienienia się między sobą pomysłami, doświadczeniami i poradami. Czerpanie ze zróżnicowanych doświadczeń innych uczestników jest ważnym elementem tego kursu.

Ponadto w celu poprawy umiejętności pracowników z zakresu ICT rząd rozpoczął program dla firm Moja Sieć. Ministerstwo ułatwiło rozpowszechnienie kursów poświęconych podstawowym umiejętnościom ICT dla pracowników w kilku przedsiębiorstwach, które przejawiały zainteresowanie kursem.

W tym przypadku uczestnicy szkoleni są pod kątem podstawowego wykorzystania komputerów osobistych i Internetu. Kurs ten obejmuje moduł poświęcony Bezpieczeństwu w Internecie, mający na celu poszerzenie wiedzy o zagrożeniach, które można napotkać w świecie internetowym.

MIIT pracuje nad inną inicjatywą, która ma nadzorować ustalenie lokalnego znaku firmowego. Oczekuje się, że znak ten zachęci firmy do wdrażania środków bezpieczeństwa do własnych systemów internetowych, jednocześnie przyczyniając się do zwiększenia zaufania do e-handlu.

Dostawcy usług internetowych (ISP)

MIIT, wraz z wiodącym dostawcą usług internetowych na Malcie, podjął wspólną kampanię dla dzieci, mającą na celu poszerzanie wiedzy. Kampania ta skierowana będzie do uczniów pierwszej klasy, którzy zostaną wprowadzeni w świat wirtualny i w tak wczesnym wieku poznają wskazówki i zakazy dotyczące Internetu oraz kwestie, do których powinni podchodzić z rozwagą. Inicjatywa ta sponsorowana jest przez zainteresowanego ISP, natomiast MIIT zapewnia wymagane zasoby ludzkie, specjalistów oraz ułatwia organizację takich wydarzeń w szkołach i innych instytucjach.

Ponadto Ministerstwo próbuje współpracować z różnymi publicznymi i prywatnymi podmiotami w celu podjęcia intensywnej kampanii mającej na celu poszerzanie wiedzy. Oczekuje się, że zostanie złożony wniosek o dofinansowanie w ramach programu Bezpieczniejszy Internet Plus. Kampania będzie skierowana do dzieci i rodziców i będzie się koncentrować na kwestiach bezpieczeństwa związanych z usługami świadczonymi za pośrednictwem telefonii komórkowej.

Media

Należy zwrócić uwagę na to, że w poniższych przykładach media wykorzystane są jako kanał, poprzez który dociera się do innych grup docelowych, i nie zostały przedstawione jako oddzielna grupa docelowa sama w sobie.

Ostatnia inicjatywa mająca na celu poszerzanie wiedzy, jaką podjęło ministerstwo, została zainicjowana w lutym 2006 roku. Trwająca miesiąc kampania była wspólnym przedsięwzięciem MIIT, Maltacom i Microsoft.

Kampania ta miała na celu poszerzenie wiedzy w zakresie zapewnienia bezpieczniejszego środowiska internetowego dla dzieci poprzez informowanie rodziców i opiekunów bez wszczynania niepotrzebnego alarmu.

Kampania oparta była na wynikach Krajowej Ankiety. W ankiecie tej wymienione były główne zagrożenia i trudności napotymane przez dzieci w świecie internetowym. Trudności te wzięto pod uwagę przy planowaniu kampanii w celu przedstawienia rozwiązań dla tych 'problemów' i przekazania właściwej wiadomości rodzicom, a także dzieciom.

W kampanii wykorzystano telewizję, radio i reklamy w gazetach, a także rozdawano ulotki i inne materiały uczniom ze szkół państwowych i prywatnych.

Partnerstwo publiczno-prywatne

Skuteczne partnerstwo publiczno-prywatne (w dziedzinie poszerzania wiedzy i edukacji/szkolenia)

Jednym z najbardziej skutecznych partnerstw publiczno-prywatnych było wspólne przedsięwzięcie MIIT i firmy Microsoft. Doprowadziło ono do intensywnej kampanii poszerzania wiedzy, która była skierowana do dzieci i rodziców i poświęcona była bezpiecznemu użyciu Internetu. Inicjatywa ta dała Ministerstwu możliwość poszerzenia wiedzy o najnowszych zagrożeniach dla bezpieczeństwa i zapewnienia rozwiązań umożliwiających radzenie sobie z tymi zagrożeniami. Na stronie internetowej Ministerstwa stworzono również sekcję (www.miti.gov.mt), która jest systematycznie aktualizowana i zawiera różne informacje przydatne zarówno dla rodziców jak i dzieci.

Ponadto Ministerstwo podpisało umowę z Childnet International, organizacją non-profit z siedzibą w Wielkiej Brytanii, która zezwoliła rządowi na korzystanie z różnych zasobów i materiałów należących do Childnet, przygotowanych przez ekspertów w dziedzinie bezpieczeństwa dzieci w kontekście Internetu. Ułatwiło to przygotowanie prezentacji i seminariów, które dostarczyły rodzicom informacje na temat tego, jak chronić dzieci przed zagrożeniami związanymi z bezpieczeństwem, napotykanymi w przypadku korzystania z technologii informacyjnej.

Zobacz również poprzedni tekst o inicjatywach z ISP, aby uzyskać więcej informacji o publiczno-prywatnych partnerstwach.

Przyszłe partnerstwa publiczno-prywatne

MIIT prowadzi obecnie rozmowy z Childnet International z myślą o zawarciu drugiej umowy z organizacją. Umowa ta będzie kontynuacją pierwszej i udostępni rządowi więcej aktualnych informacji na temat najnowszych zagrożeń dla użytkowników IT. Oczekuje się, że będzie to bardzo przydatne w przyszłych działaniach mających na celu poszerzanie wiedzy, które podejmie Ministerstwo.

Rząd jako partner społeczeństwa

Najnowsze programy i inicjatywy poszerzania wiedzy

Przez ostatnie 3 lata MIIT organizował regularne, ogólnodostępne (dla rodziców, dzieci, ludzi starszych itd.) kursy poświęcone podstawowej znajomości ICT. Ostatnio Ministerstwo zrewidowało program kursu, w wyniku czego kurs obejmuje teraz również moduł poświęcony bezpieczeństwu w Internecie oraz zaleceniom i zakazom dotyczącym Internetu. Moduł ten dostarcza uczestnikom kursu niezbędnych informacji dotyczących tego, czego powinni być świadomi oraz tego, jak radzić sobie z problemami, które można napotkać w świecie internetowym. MIIT współpracował również z różnymi organizacjami udzielającymi się na polu ICT w celu przeprowadzenia ogólnokrajowej ankiety dla dzieci i rodziców. Celem tej ankiety jest uzyskanie informacji na temat tego, jak dzieci korzystają z Internetu oraz na temat opinii rodziców w tej kwestii. Uzyskane wyniki wykorzystano do planowania i proponowania nowych inicjatyw w tym zakresie.

MIIT planuje również okresowe wydawanie „Przeglądu Społeczeństwa Informacyjnego”, który będzie obejmował konkretne obszary zainteresowania. Celem tej publikacji będzie przedstawienie ludziom obrazu osiągnięć w dziedzinie ICT. Pierwsze wydanie „Przeglądu Społeczeństwa Informacyjnego” będzie poświęcone e-bezpieczeństwu. Celem będzie poruszenie powszechnie znanych kwestii i zaproponowanie środków, które można by przyjąć w celu zapewnienia bezpiecznego korzystania z ICT.

Dzieci uważa się za najbardziej narażone na zagrożenia związane z IT. Dlatego też ostatnio MIIT rozpoczął intensywną kampanię skierowaną do rodziców i dzieci, mającą na celu poszerzanie wiedzy na temat tych zagrożeń i zalecenie rozwiązań, które ułatwiłyby wszystkim ochronę. Kampania ta była wspólnym przedsięwzięciem MIIT i Microsoft, z których ten drugi partner finansował kampanię, natomiast ten pierwszy zapewnił ekspertów i kadrę.

Publiczno-prywatne partnerstwo

Skuteczne partnerstwo publiczno-prywatne (w dziedzinie poszerzania wiedzy i edukacji/szkolenia)

Dalsze informacje na temat partnerstwa publiczno-prywatnego znajdują się we fragmencie dotyczącym inicjatyw realizowanych w ramach partnerstwa publiczno-prywatnego zamieszczonym w części Rząd jako partner (przedsiębiorstw).

Statystyki i kluczowe wskaźniki wydajności (KPI)

Statystyki/KPI do oceny skuteczności inicjatywy poszerzania wiedzy

Na tym etapie ministerstwo nie stosuje statystyk czy KPI; rząd jednak planuje opracowanie takich statystyk, ponieważ jest to zgodne z ustalonym programem na temat bezpieczeństwa w Internecie.

Znaczenie statystyk/KPI

Znaczenie statystyk i KPI zostało uznane i zaakceptowane. Wartości te pomogą rządowi lepiej zaplanować przyszłe inicjatywy i posłużą jako wskazówki dla potrzeb przyszłych projektów.

20. Holandia

Na podstawie odpowiedzi na kwestionariusz oraz uzupełnionych informacji z przeprowadzonych rozmów, badań i dodatkowych materiałów dla Holandii wyszczególniono następujące części:

[Rząd jako twórca prawnych, regulacyjnych i instytucjonalnych postanowień służących poszerzaniu wiedzy](#)

[Władze państwowe jako użytkownicy systemów informacyjnych](#)

[Władze lokalne jako użytkownicy systemów informacyjnych](#)

[Rząd jako partner przedsiębiorstw i przemysłu](#)

[Rząd jako partner społeczeństwa](#)

Rząd jako twórca prawnych, regulacyjnych i instytucjonalnych rozwiązań służących poszerzaniu wiedzy

Krajowa strategia poszerzania wiedzy

W październiku 2001 r. rząd holenderski rozpoczął krajową kampanię na rzecz poszerzania wiedzy zatytułowaną SurfopSafe (co w wolnym tłumaczeniu oznacza "bezpieczne surfowanie"). Kampania ta w czerwcu 2003 r. została połączona z europejskim projektem na rzecz poszerzania wiedzy zatytułowanym SafeBorders; w listopadzie 2004 r. utworzono holenderski punkt Awareness NaNSoS. Od 2002 r. rząd holenderski ułatwił realizację programu KWINT, krajowego programu partnerstwa publiczno-prywatnego w sprawie podatności Internetu na zagrożenia, koordynowanego przez ECP.NL. Program KWINT miał także na celu poszerzanie wiedzy.

W październiku 2005 r. rząd holenderski zwiększył nakłady na kampanię na rzecz poszerzania wiedzy przewidując środki finansowe na trzy lata (począwszy od 2006 r.) i zwracając się do ECP.NL o koordynowanie kampanii, prosząc jednocześnie krajowy punkt Awareness o dołączenie do ECP.NL. Wynikiem tego była ogólnokrajowa kampania Digibewust. Oznacza to, że kampania SurfopSafe (a zatem także obecny punkt Awareness) ma zostać połączona z kampaniami podjętymi przez podmioty prywatne, takie jak na przykład firmy Microsoft i KPN Internet, w celu zapewnienia maksymalnej synergii i optymalnych rezultatów.

Charakter i zakres strategii

- Podział obowiązków: Ministerstwo Gospodarki wyznaczyło ECP.NL do opracowania programu Digibewust i ułatwienia jego realizacji.

- Cele: określenie zakresu, w jakim docelowe sektory mogłyby działać w ramach partnerstwa publiczno-prywatnego na rzecz poszerzania wiedzy na temat bezpiecznego korzystania z elektronicznych systemów łączności.
- Grupy docelowe: użytkownicy prywatni (młodzież, kobiety i osoby starsze), MŚP i sektor przemysłowy; w tym punkt Awareness;
- Ramy czasowe: 2006-2008. ECP.NL pracuje na podstawie miarodajnych wskaźników. Poszczególne projekty muszą się opierać na danych rynkowych i muszą mieć możliwe do zmierzenia cele, które następnie zostaną ocenione.
- Ocena wpływu strategii: program musi być skuteczny, jego wyniki muszą być możliwe do zmierzenia, jak również musi być wspierany szeroko zakrojoną współpracą zainteresowanych podmiotów; Co roku zainteresowane podmioty będą otrzymywały kwestionariusz, w którym będą oceniały punktowo ogólny rezultat programu. Celem jest średni wynik na poziomie 7.5. Znajomość marki kampanii powinna wzrastać o 25 % rocznie w przypadku każdej grupy docelowej.

W celu uzyskania dalszych informacji należy odwiedzić stronę internetową www.digibewust.nl

Prawne, regulacyjne i instytucjonalne ustalenia w celu poszerzania wiedzy

Nie ma potwierdzenia na to, aby w Holandii istniały jakiekolwiek prawne, regulacyjne i instytucjonalne ustalenia mające na celu poszerzania wiedzy. Celem jest samoregulacja i partnerstwa publiczno-prywatne.

Prawne, regulacyjne i instytucjonalne ustalenia

- Promowanie bezpieczeństwa w przypadku zarządzania o charakterze prywatnym i publicznym: w ramach programu Digibewust dwa razy w roku będzie organizowane ogólnokrajowe wydarzenie, mające na celu podzielenie się wiedzą i dobrymi praktykami; omawiane będą wszystkie kwestie związane z bezpieczeństwem, w tym nauka, MŚP, przemysł i rząd.
- Promowanie dobrych praktyk: W ramach kilku platform dla sektora przemysłowego (badania i rozwój dotyczące wirtualnych infrastruktur, edukacji, certyfikacja i bezpieczeństwa) omawiane są dobre praktyki;
- Kampanie informacyjne i edukacyjne:
 - strona internetowa (po holendersku), www.digibewust.nl, jest podstawą kilkuset stron informacji na temat bezpieczeństwa Internetu skierowanych do poszczególnych grup docelowych (dzieci, rodzice, wychowawcy, MŚP). Strona internetowa zawiera lub będzie zawierała kilka testów on-line, port-scan, studia przypadków, materiały szkoleniowe, itd.
 - strona internetowa (po holendersku) www.ecp.nl, zawiera informacje na temat wielu zagadnień związanych z bezpieczeństwem. Ponadto co dwa tygodnie wydawany jest biuletyn, który dociera do tysięcy użytkowników;

- Międzynarodowa współpraca: wszystkie krajowe platformy bezpieczeństwa mają świadomość rozwoju, jaki ma miejsce na arenie międzynarodowej; ENISA może w tym przypadku odgrywać znaczącą rolę.

Dawne publikacje i inicjatywy SoS i KWINT są ponownie wykorzystywane:

- opracowano różne materiały informacyjne (takie jak broszury czy ulotki) skierowane do różnych grup docelowych; przykładami mogą być ulotki na temat zjawiska phishingu (których holenderskie organizacje konsumentów rozproszyły 800 000 sztuk) czy ulotki na temat netykiety przesłane do wszystkich holenderskich szkół;
- najbardziej popularne duńskie czaty podpisały kodeks postępowania w celu ochrony małoletnich; inicjatywa ta została zapoczątkowana i była koordynowana przez ECP.NL.;
- rozpoczęto prowadzenie różnego rodzaju działań związanych z europejską siecią Insafe; przykładem takiego działania może być konkurs na opowiadanie – zwycięzca nagrody będzie zaproszony na europejską ceremonię wręczenia nagród, która odbywa się w grudniu w Paryżu;
- organizowanie i uczestnictwo w różnego rodzaju ogólnokrajowych wydarzeniach; w tym kilka spotkań zainteresowanych podmiotów na temat bezpieczeństwa Internetu (w marcu 2002 r. spotkanie zorganizowane przez NaNSoS, a w październiku 2005 r. przez ECP.NL), stoisko na największych holenderskich targach edukacyjnych w lutym 2005 r. oraz stoisko na największych holenderskich targach technologii ITC w listopadzie 2005 r.;
- obchody drugiego Europejskiego Dnia Bezpiecznego Internetu 2005 i organizacja trzeciej edycji tego wydarzenia 7 lutego 2006 r. Tego dnia NaNSoS rozpocznie miesięczną kampanię, podczas której dzieci i młodzież będą zachęceni do poinformowania swoich nauczycieli, rodziców, dziadków i innych osób dorosłych o tym, co robią w Internecie i jakie są związane z tym zagrożenia; kampania ta będzie wspierana ze strony partnerstw publiczno-prywatnych organizowanych przez ECP.NL. w wyniku tego zorganizowana zostanie między innymi wspólna kampania na temat bezpieczeństwa Internetu rozpoczęta przez firmy Microsoft, KPN i inne.

Władze państwowe jako użytkownicy systemów informacyjnych

Najnowsze programy i inicjatywy poszerzania wiedzy

ICTU¹³

Fundacja ICTU została powołana 11 kwietnia 2001 r. przez Ministerstwo Spraw Wewnętrznych i Stosunków z Królestwem. Założeniem ICTU jest pomaganie rządowi w osiągnięciu lepszych wyników związanych z technologią informacyjną i komunikacyjną

¹³ Tekst pochodzi ze strony internetowej: <http://www.ictu.nl/profile.html>

ICTU łączy wiedzę i doświadczenie w zakresie technologii ICT i rządu. ICTU przy współpracy z organizacjami rządowymi prowadzi różne programy z tego zakresu. Polityka przybiera formę szczególnych projektów rządowych. Członkowie ICTU pochodzą ze wszystkich szczebli rządowych: władz państwowych, prowincji, gmin i okręgów wodnych.

Władze lokalne jako użytkownicy systemów informacyjnych

Najnowsze programy i inicjatywy poszerzania wiedzy

eGEM¹⁴

EGEM pomaga władzom poprawić ich usługi i sposób przetwarzania poprzez lepsze i skuteczniejsze korzystanie z technologii ICT. Nie ogranicza się to do opracowania różnych produktów czy usług, takich jak standardy i wzorce.

EGEM zwraca uwagę także na rzeczy już opracowane przez władze i zajmuje się rozpowszechnianiem istniejącej wiedzy: „Crib, imitate, EGEMulate”. Lokalne władze, które potrzebowałyby wsparcia w przypadku pewnych kwestii przy wdrażaniu projektów e-administracji mogą korzystać z EGEM-i (gdzie „i” oznacza wdrażanie (ang. implementation) lub wprowadzenie, (ang. introduction).

Rząd jako partner przedsiębiorstw i przemysłu

Małe i średnie przedsiębiorstwa (MŚP)

Od 2000 r. Syntens realizuje część MŚP programu „Nederland gaat digitaal”. Ochrona danych jest jednym z elementów programu e-biznesu. Akcent został przesunięty ze znaczenia dobrych stron internetowych dla przedsiębiorców korzystających z Internetu dla potrzeb niektórych działań organizacyjnych, na szersze zastosowanie z wykorzystaniem nowych możliwości technologii ICT. Na początku uwaga była skupiona na mikroprzedsiębiorstwach, obecnie skupia się na małych i średnich przedsiębiorstwach.

Przedmiotem zainteresowania firmy Syntens są mikroprzedsiębiorstwa o liczbie pracowników przekraczającej pięć osób (około 60 000 przedsiębiorstw) oraz małe i średnie przedsiębiorstwa (około 64 000 przedsiębiorstw). Punkt zainteresowania znajduje się w następujących sektorach: przemysł wytwórczy, spożywczy i rolniczy, logistyczny i handel hurtowy, przemysł twórczy, ICT, multimedia, budownictwo i zdrowie człowieka.

W 2005 r., Syntens zorganizowało około 350 warsztatów (przy udziale 5-15 przedsiębiorców). Dwadzieścia z nich poświęconych było ochronie, szczególnie w kontekście Internetu. Z warsztatów tych od czasu do czasu wynikały poszczególne

¹⁴ Tekst pochodzi ze strony internetowej: <http://www.ictu.nl/profile.htm>

zalecenia w sprawie ochrony danych. Nie było prawie żadnych wniosków o udzielenie rady lub przekazanie wiedzy na temat ochrony danych.

W ramach programu przedsiębiorcy mogli wypełnić on-line kwestionariusze, za pośrednictwem, których mogą przekazać pierwsze wrażenia na temat ich sytuacji. Pomocna w tym przypadku była broszura zatytułowana „Z poczuciem bezpieczeństwa, ochrona danych w praktyce”. Konkretnie dane dotyczące konsultowania broszury i związane z kwestionariuszem on-line nie są znane. Broszura jest nadal dostępna; wypełnienie kwestionariusza natomiast nie jest już możliwe. Aktualnie dostępny jest on-line skan nowej wersji, w której kładzie się nacisk na wprowadzenie do dokonywania płatności za pośrednictwem Internetu, jako część metody „gotowy na cyfrowy biznes” odnoszącej się do całego przedsiębiorstwa.

Poziom umiejętności technicznych jest niski. Warsztaty skierowane są przede wszystkim do przedsiębiorców. W praktyce widać, że w przypadku małych i średnich przedsiębiorstw uczestnikami warsztatów są osoby odpowiedzialne za marketing i/lub sprzedaż. Warsztaty na ogół są prowadzone przez doradców firmy Syntens specjalizujących się w technologii ICT; program warsztatów jest opracowywany centralnie i przygotowywany przez zewnętrznych ekspertów.

Z doświadczenia wynika, że zainteresowanie rośnie w okresie natężenia zagrożenia wirusami i wtedy, gdy temat ten poruszany jest w mediach. Uczestnicy są zadowoleni, gdy słyszą, że problem nie jest aż tak zasadniczy i że nie muszą inwestować w różne środki. Dużym zainteresowaniem cieszą się darmowe skanery do wykrywania wirusów, praktyczne rady dotyczące ustawień komputerów i oprogramowania, jak również standardowe porozumienia z kreatorami stron internetowych lub hostami.

Nowe będące w trakcie realizacji działanie mierzy aktualny poziom doświadczenia związanego z cyberprzestępczością, wiedzę i rzeczywistą ochronę danych w ramach grupy piętnastu losowo wybranych organizacji należących do strefy przemysłowej. W tym przypadku wykorzystywane są następujące narzędzia: kwestionariusz, wywiad, warsztaty i prezentacje; usługi naprawcze są oferowane przez „dostawców klientów indywidualnych” ICT. Wyniki zostaną ekstrapolowane do holenderskiego MKB (październik 2006) i zostaną wykorzystane na potrzeby propozycji projektu.

NPAC

W ramach programu Digibewust pod koniec kwietnia 2006 r. zostanie przeprowadzone doświadczenie, w którym weźmie udział piętnaście małych i średnich przedsiębiorstw, w celu większego uwrażliwienia na ataki cyberprzestępstw w sektorze MŚP.

Celem doświadczenia jest określenie powodów lub odpowiedzi na pytania takie, jak „czy cyberprzestępstwo jest dla nich problemem” i „czy ich komputery są wystarczająco zabezpieczone”. Wyniki analiz zostaną wykorzystane jako punkt odniesienia

dla przyszłych działań. Ostatecznym celem tych działań jest możliwie największe zmniejszenie szkód spowodowanych cyberprzestępstwami.

Dostawcy usług internetowych (ISP)

Wydaje się że, z wyjątkiem holenderskiego punktu kontaktowego hotline, nie istnieje żadna współpraca między ISP a rządem. Oddział holenderskiego dostawcy Internetu NLIP już nie istnieje i bez wsparcia ze strony rządu, punkt kontaktowy w sprawie niezgodnych z prawem treści nie funkcjonuje.

Na następujących stronach internetowych znajdują się szczegóły dotyczące analizy przeprowadzonej przez Ministerstwo Gospodarki oraz inne analizy dotyczące rynku internetowego:

<http://www.onderzoeksdatabank.minez.nl/onderzoeken/onderzoekkaart.aspx?onderzoekID=2934> oraz
<http://www.onderzoeksdatabank.minez.nl/rapporten/Rapport.aspx?rapportId=485>

Szczegółowe informacje na temat kampanii poszerzania wiedzy wspieranej przez holenderską linię informacyjną znajdują się na stronie internetowej www.surfsafe.nl.

Partnerstwo publiczno-prywatne

Skuteczne partnerstwo publiczno-prywatne (w dziedzinie poszerzania wiedzy i edukacji/szkolenia)

Dalsze informacje na temat partnerstwa publiczno-prywatnego znajdują się we fragmencie dotyczącym inicjatyw realizowanych w ramach partnerstwa publiczno-prywatnego zamieszczonym w części [*Rząd jako partner \(społeczeństwa\)*](#).

Rząd jako partner społeczeństwa

Najnowsze programy i inicjatywy poszerzania wiedzy

Holenderska organizacja konsumentów jest instytucją niezależną od organów administracji państwowej.

Partnerstwo publiczno-prywatne

Skuteczne partnerstwo publiczno-prywatne (w dziedzinie poszerzania wiedzy i edukacji/szkolenia)

Masowe korzystanie z Internetu i nowych technologii on-line spowodowało, że także w Holandii istnieją problemy on-line. Sytuacja ta upodabnia się do sytuacji, jakie mają miejsce w innych krajach o stosunkowo wysokich umiejętnościach społeczeństwa

korzystania z Internetu, a mianowicie obecność wirusów komputerowych, spamu, niepożądanych kontaktów (np. chaty lub zastraszanie on-line), oszustw on-line i kradzieży tożsamości, piractwa komputerowego i nieodpowiednich treści. W ciągu ostatniego roku ilość omawianych tego typu zdarzeń w prasie zwiększyła się, a to z kolei spowodowało, że szkoły, rodzice i politycy coraz częściej zwracają się z prośbą o dostarczenie im informacji. Aby oddalić te zagrożenia, w 2005 r. holenderskie Ministerstwo Gospodarki podjęło decyzję o nasileniu istniejącej kampanii SurfopSafe i uzgodnieniu jej z innymi działaniami, zarówno tymi jakie są prowadzone przez rząd, jak i tymi które są realizowane przez podmioty prywatne. Program Digibewust, który będzie realizowany przez trzy lata począwszy od 2006 r. i który będzie koordynowany przez ECP.NL, ma na celu kształcenie i wzmocnienie pozycji użytkowników końcowych, od dzieci do odbiorców ogółem i MŚP. Celem tego programu jest nie tylko uświadomienie istnienia zagrożeń, ale także spowodowanie aby podmioty te korzystały z Internetu w taki sposób, który pozwoli na zminimalizowanie istniejących zagrożeń. Jest to krok naprzód w porównaniu do istniejącego holenderskiego podejścia.

Aktualnie w Holandii główne kwestie związane z bezpieczeństwem Internetu to:

- Nauczanie dzieci, nauczycieli i rodziców o potencjalnych zagrożeniach, jakie niesie za sobą korzystanie z Internetu. Jest to konsekwencją kilku przypadków zastraszania i niepożądanych doświadczeń on-line, w jakich uczestniczyli małoletni i pedofile. Podjęte zostały pewne inicjatywy skierowane do dzieci, nauczycieli i rodziców, do których należy kodeks postępowania w przypadku korzystania z chatów (koordynowany przez ECP.NL), strony internetowe dla rodziców i nauczycieli (uruchomione przez głównego holenderskiego dostawcę Internetu, firmę KPN Internet) i działania prowadzone przez holenderski punkt Awareness NaNSoS. Do tego rodzaju działań należy przesyłanie materiałów informacyjnych do wszystkich holenderskich szkół, obecnych na głównych holenderskich targach edukacyjnych i organizowanie Dnia Bezpiecznego Internetu 2006 (pod hasłem „Dzieci uczą dorosłych bezpieczeństwa w Internecie”). Ponadto NaNSoS aktywnie promuje holenderski certyfikat internetowy (opracowany pod marką punktu Awareness przez ministra gospodarki) dla szkół podstawowych, który oficjalnie został wprowadzony w październiku 2005 r. Zastosowanym podejściem nie jest podejście „zakaz i kontrola” ale „kształcenie i uczenie odpowiedzialnych zachowań”.
- Zorganizowana przestępczość komputerowa, taka jak zjawisko phishing, czyli nieuczciwe pozyskanie poufnej informacji osobistej i kradzież tożsamości. Kilka, raczej amatorskich przypadków, zostało ostatnio odnotowanych w Holandii, jednak oczekuje się że tego typu zagrożenia będą występowały coraz częściej i że będą miały bardziej profesjonalny charakter. Korzystanie z sieci zainfekowanych komputerów znanych jako „botnets” (np. w celu dokonania oszustwa lub wymuszenia) jest coraz poważniejszym zagrożeniem, czego przykładem może być ostatni nalot policji na trzech młodych ludzi, którzy byli „właścicielami” takiej sieci botnet liczącej ponad milion komputerów zombie.

Od 2001 r., kiedy rozpoczęła się kampania holenderskich władz państwowych SurforSafe, wiele instytucji w Holandii przyjęło rozwiązanie mające na celu bezpieczne korzystanie z Internetu. Należą do nich główni dostawcy Internetu (którzy obecnie wykorzystują bezpieczeństwo Internetu jako narzędzie marketingowe), holenderska organizacja konsumentów i kilka fundacji (takich jak NICAM, Safe Internet Foundation, Bits of Freedom, organizacja konsumentów na rzecz dzieci). Rząd ponadto finansował ECP.NL w celu przeprowadzenia programu na temat bezpieczeństwa Internetu, wprowadził system wczesnego ostrzegania o zagrożeniach dla bezpieczeństwa dla Internetu (www.waarschuwingsdienst.nl, związany z rządową organizacją CERT) i wprowadził program certyfikatów internetowych w szkołach podstawowych. Szczegóły dotyczące tej rządowej kampanii informacyjnej znajdują się poniżej:

We wrześniu 2005 r. opublikowano wyniki dużego rządowego badania mającego na celu zmierzenie poziomu wiedzy na temat bezpieczeństwa Internetu w Holandii. Ogólną konkluzją wynikającą z badania jest to, że podczas gdy świadomość istnienia zagrożeń związanych z korzystaniem z Internetu jest stosunkowo wysoka, ograniczona liczba osób decyduje się na podjęcie stosownych środków ochrony. Ponadto poziom akceptacji problemów związanych z Internetem jest raczej wysoki. Poczynając od utraty pieniędzy dochodząc do niezręcznych sytuacji związanych z publikacją prywatnych zdjęć w Internecie. Jeśli chodzi o dzieci, wyraźnie zauważono, że istnieje duża przepaść między dziećmi a ich otoczeniem, do którego należą rodzice i nauczyciele. Potwierdziły to inne badania (np. działanie przeprowadzone przez Planet Internet, największego holenderskiego dostawcę Internetu). Wszystkie badania wskazują na potrzebę bardziej ukierunkowanych działań mających na celu poszerzanie wiedzy, dzięki którym poszczególne grupy docelowe będą otrzymywały specjalnie narzędzia. Ponadto należy uświadomić społeczeństwu, że nie tylko należy być świadomym istnienia niebezpieczeństw, ale także zwalczać je.

Wyniki

Pierwszym namacalnym wynikiem krajowej kampanii Digibewust były wspólne obchody Dnia Bezpiecznego Internetu 2006, podczas którego miało miejsce wiele działań zorganizowanych przez krajowy punkt Awareness, jak również przez podmioty prywatne takie jak Microsoft, UPC, KPN, ANWB, TPG, IBM. Niektóre organy publiczne/organizacje pozarządowe, w tym holenderska organizacja konsumentów, Govcert i ICTU zorganizowały różne działania; rozpoczęto masową multimedialną kampanię, która aktywnie będzie uczestniczyła w promowaniu i organizowaniu działań.

Rola proponowanego punktu Awareness

Proponowany punkt Awareness będzie nadal prowadził prace w ramach kampanii na rzecz poszerzania wiedzy NaNSoS. W celu zapewnienia silniejszej obecności w Holandii, zostanie połączony z publiczno-prywatnymi partnerstwami, jakie są organizowane przez ECP.NL w związku z bezpieczeństwem Internetu w ramach Digibewust. Jest to wspierane zarówno przez rząd holenderski, główne gałęzie

przemysłu, jak również publiczne organizacje takie jak NICAM (w ramach instytucji, jaką jest Kijkwijzer) i Kennisnet.

Punkt będzie ściśle współpracował z wszystkimi znaczącymi podmiotami i w szczególności z holenderskim rządem, jednostką finansującą punkt Awareness. Ponadto, prowadzona będzie aktywna współpraca z państwami europejskimi.

Mimo że nie wszystkie działania są możliwe do przewidzenia na tym etapie, niektóre konkretne działania zostały już rozpoczęte w ramach obecnie prowadzonych projektów lub są na etapie przygotowań. Do działań tych należą:

- promocja „Certyfikatu Bezpiecznego Internetu” skierowana do dzieci starszych klas szkoły podstawowej;
- rada dzieci (DigiRaad) mająca na celu udzielanie porad i odpowiedzi;
- Quest;
- kampania na temat haseł;
- udział organizacji na rzecz ochrony dzieci w holenderskiej kampanii na rzecz poszerzania wiedzy;
- bliższa współpraca MŚP w ramach kampanii; grupa docelowa jest często zaniedbywana i aktualnie ma problemy w związku z kwestiami dotyczącymi bezpieczeństwa Internetu;
- coroczne obchody Dnia Bezpiecznego Internetu, którego temat jest zmieniany co roku.

W ramach projektu punktu Awareness rozpoczęta zostanie holenderska długoterminowa kampania i zbadana zostanie możliwość przystosowania punktu (np. przez Komitet Sterujący, łącząc ze sobą kilka organizacji aktywnie działających w kontekście zagadnień bezpiecznego korzystania z Internetu).

21. Norwegia

Na podstawie odpowiedzi na kwestionariusz oraz uzupełniających informacji z przeprowadzonych rozmów, badań i dodatkowych materiałów dla Norwegii wyszczególniono następujące części:

[Rząd jako twórca prawnych, regulacyjnych i instytucjonalnych postanowień służących poszerzaniu wiedzy](#)

[Rząd jako partner przedsiębiorstw i przemysłu](#)

[Rząd jako partner społeczeństwa](#)

Rząd jako twórca prawnych, regulacyjnych i instytucjonalnych ustaleń służących poszerzaniu wiedzy

Krajowa strategia poszerzania wiedzy

Norweska strategia opiera się na dokumencie OECD 2002 zawierającym wskazówki na temat bezpieczeństwa systemów i sieci informacji zatytułowanym „Guidelines for the security of information systems and networks”. W ramach strategii wprowadzono pojęcie „kultura bezpieczeństwa” odnoszące się do IT i korzystania z Internetu, stworzone w związku z rozwojem i rozmieszczeniem systemów informacyjnych i elektronicznej wymiany informacji w Norwegii. Bezpieczeństwo IT powinno być jednym z kluczowych czynników regulujących korzystanie z IT przez norweskich przedsiębiorców i konsumentów.

Charakter i zakres strategii

- Podział obowiązków: rząd i organy nadzorujące;
- Cele: potencjalne zagrożenia, rozwiązania, ograniczenia i konieczne działania służące ustanowieniu kultury bezpieczeństwa IT;
- Grupy docelowe: zgodnie ze strategią wszystkim uczestnikom należy uświadomić istnienie zagadnienia, jakim jest bezpieczeństwo informacji; obecnie uwaga koncentruje się na zwiększeniu świadomości MŚP i gospodarstw domowych;
- Ramy czasowe: działanie jest w trakcie realizacji.

W celu uzyskania dalszych informacji por. www.norsis.no i www.nettvett.no.

Prawne, regulacyjne i instytucjonalne rozwiązania służące poszerzaniu wiedzy

W 2004 r. utworzono organ koordynujący ds. bezpieczeństwa informacji (prowadzony przez Ministerstwo Administracji Rządowej i Reform). W jego składzie znajdują się członkowie z ministerstw i agencji, które formalnie odpowiadają za opracowywanie regulacji, jak również odgrywają role operacyjne w kontekście śledzenia informacji na temat zagadnień związanych z bezpieczeństwem w szerszym tego wyrażenia

znaczeniu. W Norwegii utworzenie takiego organu było postrzegane jako konieczność wynikająca ze zwiększonego stopnia korzystania z technologii, ICT, co także może stanowić zagrożenie „atakami” i spowodować uszkodzenie systemów IT. Prace prowadzone przez ten organ dotyczą ogólnych i szeroko zakrojonych zagadnień dotyczących bezpieczeństwa ICT, które związane jest z bezpieczeństwem państwowym, takich jak na przykład kluczowe interesy bezpieczeństwa narodowego i ważne funkcje społeczne. Organizacja będzie koordynowała przyszłe prace nad ustawodawstwem dotyczącym bezpieczeństwa ICT, opracowywała nowe standardy, normy, metody i narzędzia służące bezpieczeństwu ICT, jak również koordynowała działania monitorowania bezpieczeństwa. Powinna także zwrócić uwagę na bieżące zagadnienia i słabe punkty zagrożeń dla bezpieczeństwa i koordynować inicjatywy dotyczące bezpieczeństwa informacji i planowania gotowości na wypadek pojawienia się zagrożenia.

Norweski ośrodek ds. bezpieczeństwa informacji (NorSIS) został formalnie utworzony 1 stycznia 2006 r. Do jego głównych zadań należą:

- rozpowszechnianie informacji, doświadczeń i wiedzy na temat potencjalnych zagrożeń i stosownych środków zaradczych;
- nawiązywanie kontaktów i współpracy z organizacjami świadczącymi podobne usługi w innych państwach.

Norweski Urząd Poczty i Telekomunikacji (NPT) sprawuje nadzór nad sektorem łączności elektronicznej. Odpowiada on za wprowadzanie w życie ustawy o łączności elektronicznej, która zawiera kilka przepisów związanych z bezpieczeństwem informacji. NPT aktualnie akcentuje prowadzone przez siebie inicjatywy dotyczące promowania bezpieczeństwa.

Norwegia dwukrotnie zorganizowała Dzień Bezpiecznego Internetu (w 2005 i 2006 r.). Planuje się coroczne organizowanie tego wydarzenia.

Rząd jako partner przedsiębiorstw i przemysłu

Małe i średnie przedsiębiorstwa (MŚP)

Aktualnie nie są prowadzone żadne inicjatywy na rzecz poszerzania wiedzy, które byłyby skierowane do MŚP lub które byłyby prowadzone przy ich współpracy, z wyjątkiem wymienionych poniżej.

Dostawcy usług internetowych (ISP)

Najnowszą i najskuteczniejszą rządową inicjatywą mającą na celu poszerzenie wiedzy wśród użytkowników było uruchomienie strony internetowej www.nettvett.no, która zawiera informacje na temat sposobu korzystania z Internetu i związanych z nim usług. Strona ta, uruchomiona 26 kwietnia 2005 r., była wspólnym projektem powstałym dzięki współpracy kilku rządowych instytucji i przedsiębiorstw ICT, w tym dostawców

usług internetowych. Za uruchomienie strony odpowiada norweski organ nadzorujący, jakim jest Norweski Urząd Poczty i Telekomunikacji (NPT), który odpowiada także za prowadzenie strony.

Na stronie internetowej znajdują się informacje, porady i wskazówki dotyczące bezpiecznego wykorzystywania informacji i technologii łączności za pośrednictwem Internetu i aplikacji internetowych. W związku z tym, że jest to inicjatywa mająca na celu podnoszenie świadomości, celem jej jest zwiększenie wiedzy społeczeństwa i MŚP w zakresie bezpieczeństwa informacji. Niektóre z podejmowanych kwestii:

- bezpieczne połączenia w Internecie;
- bezpieczne korzystanie z poczty elektronicznej;
- spam;
- phishing
- ochrona przed utratą danych;
- kwestie dotyczące poufności;
- ochrona przed atakami z Internetu;
- zabezpieczenie sieci bezprzewodowej;
- stosowanie elektronicznych podpisów.

Informacje zawarte na stronie internetowej są zamieszczone w logiczny sposób za pomocą tematów podzielonych na kilka kategorii. Informacje są także podzielone pod względem poziomu wiedzy, na przykład „dla początkujących”, „dla średnio zaawansowanych” i „dla przedsiębiorstw”. Dla większości kategorii lub zagadnień na stronie zamieszczone są krótkie i łatwe do zapamiętania zasady dotyczące tego, co należy wiedzieć podczas korzystania z różnych aplikacji internetowych. Użytkownik ma także możliwość zadania pytania na stronie internetowej, jeżeli pytanie to dotyczy treści zamieszczonej na stronie lub jest z nią związane.

Strona została uruchomiona w dniu, w którym na temat technologii ICT wydano komunikat prasowy i w którym w związku z tym zorganizowano spotkanie z udziałem prasy. Ogólnokrajowa prasa została wykorzystana jako główny kanał przekazywania informacji o uruchomieniu strony. Do promocji strony internetowej wykorzystano także inne środki, takie jak krajowy Dzień Bezpiecznego Internetu, który odbył się 7 lutego 2006 r. Aby dowiedzieć się, jakim zainteresowaniem cieszyła się strona, policzono ile razy została ona odwiedzona. Aktualnie stopień korzystania ze strony wzrasta, dochodząc do około 1000 użytkowników dziennie. Aby dowiedzieć się, jak bardzo użytkownicy są zadowoleni z zasobów strony, planowane jest przeprowadzenie ankiety on-line zawierającej prosty zestaw pytań.

Ostatnio na stronie zamieszczono animację (wyjaśniającą mechanizmy wirusów i firewalli) i interaktywną grę/quiz, dzięki której użytkownicy mogą sprawdzić poziom swojej wiedzy na bezpieczeństwie IT. Oczekuje się, że quiz zachęci użytkowników do poszerzenia wiedzy na tematy zamieszczone na stronie internetowej. Planem na przyszłość co do strony internetowej jest to, aby stała się ona wiodącą stroną władz

państwowych, która dostarcza społeczeństwu i MŚP najnowsze informacje, porady i wskazówki na temat bezpieczeństwa informacji.

Media

Należy zwrócić uwagę, że poniżej wskazany przykład wykorzystuje media jako kanał dotarcia do innych grup docelowych, i nie przedstawia ich jako odrębnej grupy docelowej.

W związku z Dniem Bezpiecznego Internetu, jaki został zorganizowany w lutym 2006 r. niektóre ministerstwa, organy nadzorcze i większe prywatne przedsiębiorstwa ICT opracowały (i sfinansowały) wspólnie specjalny, 24 stronicowy dodatek do jednej z największych norweskich gazet. Oprócz tej inicjatywy żadna inna nie została przeprowadzona przy współpracy mediów.

Partnerstwo publiczno-prywatne

Skuteczne partnerstwo publiczno-prywatne (w dziedzinie poszerzania wiedzy i edukacji/szkolenia)

Koszty NorSIS są pokrywane w ramach partnerstwa publiczno-prywatnego zawartego pomiędzy Ministerstwem Administracji Rządowej i Reform i lokalnym przedsiębiorstwem.

Rząd jako partner społeczeństwa

Partnerstwo publiczno-prywatne

Skuteczne partnerstwo publiczno-prywatne (w dziedzinie poszerzania wiedzy i edukacji/szkolenia)

W celu uzyskania informacji na temat inicjatyw skierowanych do społeczeństwa por. część [Rząd jako partner \(przedsiębiorstw\)](#).

22. Polska

Na podstawie odpowiedzi na kwestionariusz oraz uzupełniających informacji z przeprowadzonych rozmów, badań i dodatkowych materiałów dla Polski wyszczególniono następujące części:

[Rząd jako twórca prawnych, regulacyjnych i instytucjonalnych regulacji służących poszerzaniu wiedzy](#)

[Władze państwowe jako użytkownik systemów informacyjnych](#)

[Władze lokalne jako użytkownik systemów informacyjnych](#)

[Rząd jako partner społeczeństwa](#)

Rząd jako twórca prawnych, regulacyjnych i instytucjonalnych regulacji służących poszerzaniu wiedzy

Krajowa strategia poszerzania wiedzy

W kontekście ochrony konsumenta, prezes Urzędu Ochrony Konkurencji i Konsumentów opiera zakres działań na dokumencie rządowym zatytułowanym „Krajowa Strategia Ochrony Konsumentów na lata 2004-2006”. Jednym z celów strategii jest zbudowanie przyjaznego konsumentom rynku. Cel powinien zostać osiągnięty poprzez monitorowanie handlu elektronicznego i prowadzenie proaktywnej edukacji i promocji.

Prawne, regulacyjne i instytucjonalne ustalenia w celu poszerzania wiedzy

Jednym z bardziej znaczących przykładów współpracy z centralnymi władzami państwowymi skierowanej przeciwko zjawisku, jakim jest spam jest specjalna grupa zadaniowa ds. spamu. Jest ona ważnym przykładem współpracy horyzontalnej między organami administracji centralnej. Współpraca została ustanowiona decyzją Europejskiego Komitetu Rady Ministrów jesienią 2005 r. Koordynator lub punkt kontaktowy został ustanowiony na szczeblu krajowym lub międzynarodowym, podczas gdy w przypadku innych władz (takich jak prezes Urzędu Komunikacji Elektronicznej, prezes Urzędu Ochrony Konkurencji i Konsumentów i Generalny Inspektor Ochrony Danych Osobowych) powołane zostały właściwe władze. Wszystkie wyżej wspomniane władze współpracują ze sobą i wspólnie prowadzą kontrole, jednak każda z nich zajmuje się konkretną dziedziną. Ważnym elementem każdej decyzji jest współpraca sektora publiczno-prywatnego. Minister transportu i budownictwa został zobligowany do podpisania umowy z instytutem NASK o pomoc techniczną i pomoc w prowadzeniu kontroli w Internecie.

Władze państwowe jako użytkownik systemów informacyjnych

Najnowsze programy i inicjatywy poszerzania wiedzy

Krajowy Plan Informatyzacji (KPI) na rok 2006¹⁵ określa szczegółowo poziom rozwoju e-administracji i jest punktem wyjścia dla dyskusji na temat priorytetów planu informatyzacji na lata 2007-2010. KPI jest wynikiem Ustawy z 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne.

KPI jest instrumentem wykorzystywanym do zaplanowania i koordynowania działań służących informatyzacji organów publicznych w odniesieniu do zadań wypełnianych przez te organy. W 2006 r. działania w ramach KPI będą dotyczyły głównie opracowania założeń dotyczących zmian dokumentów prawnych w celu zapewnienia warunków dla skutecznej modernizacji administracji publicznej opierającej się na technologii ICT. W tym: zwrócenie uwagi na przekształcenie procesów; opracowanie metod służących koordynowaniu i monitorowaniu głównych projektów e-administracji; opracowanie Krajowych Ram Interoperacyjności w celu zapewnienia skutecznego dostarczania publicznych usług elektronicznych. W ramach KPI zakłada się dwa priorytety dotyczące informatyzacji w 2006 r. i kolejnych latach: usprawnienie publicznych wydatków na projekty IT w ramach administracji publicznej i stworzenie nowoczesnego i przyjaznego obywatelom państwa.

W kontekście bezpieczeństwa, priorytetem KPI jest zwiększenie zaufania w środowisku przedsiębiorstw i w społeczeństwie do korzystania z elektronicznych urządzeń służących świadczeniu usług publicznych. Aby zrealizować ten priorytet należy najpierw w kontekście administracji publicznej wprowadzić spójną politykę bezpieczeństwa. Określono następujące cele:

- zapewnienie odpowiednich poziomów bezpieczeństwa w systemie IT administracji publicznej – jest to niezbędne dla zbudowania zaufania wśród użytkowników;
- popularyzacja elektronicznych form identyfikacji – w odniesieniu do regulacji prawnych dotyczących ochrony danych osobowych;
- zwalczanie spamu i innych złośliwych elementów stanowiących zagrożenie dla systemów IT, w tym niezgodne z prawem operacje;
- stworzenie warunków służących podniesieniu świadomości i poszerzaniu wiedzy użytkowników w odniesieniu do ochrony ich systemów przed złośliwym oprogramowaniem i spamem - w tym powiadamianie stosownych organów o zauważonych zagrożeniach.

Należy zauważyć, że w przeciwieństwie do poprzednich strategicznych dokumentów, KPI zostało opracowane na podstawie przepisów prawa i przypuszcza się, że będzie miało większy wpływ niż poprzednie strategie.

Zgodnie z inicjatywą *i2010 – Europejskie społeczeństwo informacyjne na rzecz wzrostu i zatrudnienia*, każde państwo członkowskie powinno opracować swój własny plan

¹⁵ Krajowy Plan Informatyzacji na rok 2006 (projekt), Biuletyn Informacji Publicznej Ministerstwo Spraw Wewnętrznych i Administracji. KPI ma zostać przyjęty przez radę Ministrów w maju 2006 r.

działania na rzecz bezpieczeństwa. Sugestie te mogą zostać rozważone w przyszłym KPI na lata 2007-2010.

W marcu 2006 r. prezes Urzędu Ochrony Konkurencji i Konsumentów (UOKiK) wziął udział w projekcie ICPEN zatytułowanym *Miesiąc Przeciwdziałania Oszustwom*. Projekt ten był w szczególności poświęcony prawnym, ekonomicznym i społecznym aspektom niechcianej korespondencji i spamu.

Cały projekt został zrealizowany we współpracy z partnerami z sektora biznesu. Ponadto UOKiK zaprosił inne władze publiczne odpowiadające za ochronę konsumentów w Polsce. W wyniku tego, w marcu 2006 r. prezes UOKiK we współpracy z partnerami ze świata biznesu zorganizował trzy szeroko zakrojone wydarzenia:

- Pierwsze z nich zostało zorganizowane wspólnie z Polską Izbą Informatyki i Telekomunikacji (PIIT). Prezes UOKiK i PIIT zaprosili wiodących polskich dostawców Internetu i operatorów usług telekomunikacyjnych. Celem projektu było omówienie potencjalnych obszarów współpracy między władzami a dostawcami usług internetowych i możliwości opracowania kodeksu postępowania ze spamem.
- Drugim projektem była konferencja zorganizowana wspólnie z instytutem NASK (Naukowa i Akademicka Sieć Komputerowa kontrolowana przez polskie władze i wiodący operator sieci). UOKiK i NASK zaprosili przedstawicieli ze świata nauki, biznesu i kręgów administracyjnych oraz rozpoczęli dialog w sprawie możliwości i konieczności wprowadzenia zmian w polskim systemie prawnym dotyczącym spamu. UOKiK i NASK zaznajomili gości z inicjatywami ICPEN, takimi jak londyński plan przeciwdziałania spamowi (London Action Plan), Dzień Przeszukiwania Internetu (Internet Sweep Day), Spam Zombie i innymi międzynarodowymi projektami takimi jak zestaw narzędzi antyspamowych OECD (OECD Spam Toolkit) (Spam Task Force) i procedura współpracy CNSA.
- Ostatnim ważnym wydarzeniem, jakie zostało zorganizowane przez UOKiK były warsztaty szkoleniowe dla prokuratorów na temat prowadzenia dochodzeń w związku z Internetem. Warsztaty zostały przygotowane we współpracy z NASK i wiodącymi polskimi dostawcami usług internetowych (Interia i Onet.pl), jak również z czołowym polskim internetowym serwisem aukcyjnym Allegro.

W marcu 2006 r. eksperci UOKiK ds. spamu udzielili wielu wywiadów zarówno prasowych, jak i radiowych czy telewizyjnych. Dotarli do różnych mediów, w tym do prasy codziennej, prasy lokalnej, specjalistycznych portali internetowych i popularnych magazynów kobiecych.

Władze lokalne jako użytkownik systemów informacyjnych
Najnowsze programy i inicjatywy poszerzania wiedzy

Jeśli chodzi o programy mające na celu poszerzanie wiedzy przygotowane przez władze lokalne, należy podkreślić następujące inicjatywy:

- Inicjatywa na rzecz poszerzania wiedzy podjęta przez Związek Powiatów Polskich i trzech liderów sektora technologii IT na polskim rynku (Symantec, Microsoft i Polkomtel). Związek Powiatów Polskich, utworzony w lutym 1999 r., skupia 313 członków. Miasta powiatowe w 2005 i 2006 r. zorganizowały serię seminariów i sesji szkoleniowych na temat poszerzania wiedzy. Więcej informacji na ten temat można znaleźć na stronie internetowej www.zppp.pl (strona tylko w języku polskim).
- Inicjatywa na rzecz poszerzania wiedzy podjęta przez Klub e-Administracja, organizację zrzeszającą jednostki administracji samorządowej i instytucje centralne. Misją tej organizacji, która została ustanowiona w październiku 2003 r., jest upowszechnianie zarówno wiedzy jak i doświadczeń z wdrażania rozwiązań teleinformatycznych w administracji. Klub e-Administracja zorganizował samodzielnie i wraz z innymi organizacjami kilka kursów szkoleniowych na temat technologii IT. Dwa razy do roku klub e-Administracja organizuje konferencję zatytułowaną „Forum Informatyki w Administracji”. W tym roku VI Forum Informatyki w Administracji zostało zorganizowane w Toruniu w dniach 25-16 kwietnia. Ważnym punktem konferencji było poszerzanie wiedzy na temat technologii ICT. Klub e-Administracja zorganizował także specjalne konferencje mające na celu poszerzanie wiedzy, w tym seminarium, jakie odbyło się we wrześniu 2004 r. zatytułowane „Audyt systemów teleinformatycznych w administracji - jako wymóg prawny i podstawa certyfikacji jakości i bezpieczeństwa”; na 23 maja 2006 r. planowane jest także zorganizowanie warsztatów. Główne tematy warsztatów to: obiektywna wartość posiadanych informacji; najważniejsze akty i normy dotyczące zarządzania dokumentami; polityka bezpieczeństwa informacji jako podstawowy element systemów IT; ochrona przed zagrożeniami dla stacji roboczych PC i urządzeń przenośnych; metody i techniki służące uwierzytelnianiu dokumentów; socjotechniczne ataki i sposoby zapobiegania im. Szczegółowe informacje znajdują się na stronie internetowej: <http://www.e-administracja.org.pl/konferencje/2006/sbi3/index.php>

Rząd jako partner społeczeństwa

Najnowsze programy i inicjatywy poszerzania wiedzy

Od 2005 r. w Polsce prowadzone są dwa projekty, stanowiące część programu Komisji Europejskiej zatytułowanego *Safer Internet Action Plan*. Oba projekty są prowadzone pod auspicjami Ministerstwa Edukacji i Nauki, Ministerstwa Spraw Wewnętrznych i Administracji, Rzecznika Praw Dziecka i Komendę Główną Policji, Urząd Ochrony Konkurencji i Konsumentów i UNESCO.

Pierwszy projekt to NIFC Hotline Polska (<http://hotline.org.pl/>). Projekt ten jest zarządzany przez zespół Dyżurnet instytutu NASK (*Naukowa i Akademicka Sieć Komputerowa*). Celem projektu jest zorganizowanie i prowadzenie punktu Hotline, który

otrzymywałby informacje na temat nielegalnych treści zamieszczonych w Internecie. Punkt Hotline współpracuje z policją przy śledzeniu przestępstw polegających na zamieszczaniu nielegalnych treści w Internecie i następnie usuwaniu ich we współpracy z ISP. 28 stycznia 2005 r. polski zespół NIFC Hotline—Dyżurnet.pl został członkiem stowarzyszenia INHOPE i w ciągu roku uzyskał status pełnoprawnego członka. W marcu 2005 r. Dyżurnet.pl powołał Komitet Konsultacyjny, który ma przyczynić się do stworzenia w Polsce lepszych warunków do rozwijania się kultury bezpieczeństwa w Internecie. Wiele władz publicznych, ministerstw i organizacji uczestniczy w dyskusjach w ramach Komitetu Konsultacyjnego.

Drugi projekt jest prowadzony przez konsorcjum „Awareness” utworzone z NASK i Fundacji Dzieci Niczyje. Projekt utworzenia punktu „Awareness” został przedstawiony w ramach zaproszenia Komisji Europejskiej do składania wniosków „Call for Proposals 2003/2004” oraz w oparciu o wytyczne Unii Europejskiej zawarte w dokumencie „Safer Internet Action Plan, Work Programme 2003-2004”. W grudniu 2004 r. podpisana została umowa i zgodnie z założeniami programu Komisji Europejskiej, NASK i Fundacja Dzieci Niczyje stały się partnerami konsorcjum INSAFE, prowadzonego przez European Schoolnet, które z ramienia Komisji koordynuje działania punktów „Awareness” na poziomie europejskim. Projekt Awareness ma na celu stworzenie ośrodka zajmującego się podnoszeniem świadomości na temat istnienia zagrożeń, na jakie mogą napotkać młodzi Polacy korzystając z Internetu. Projekt jest prowadzony od stycznia 2005 r. W ramach projektu będą prowadzone sesje szkoleniowe dla różnych grup docelowych w tym dla sektora edukacji, dostawców usług internetowych, prokuratorów i funkcjonariuszy policji biorących udział w zwalczaniu cyberprzestępstw. W ramach projektu w 16 dużych miastach zorganizowano kampanie mające na celu promowanie bezpiecznych treści i zmniejszenie skali zagrożeń, których źródłem może być Internet. Na rok 2006 planuje się także przeprowadzenie kampanii medialnej pro bono. Punkt Awareness wysunął pomysł utworzenia Ogólnopolskiej Koalicji na rzecz Bezpiecznego Internetu, czyli inicjatywy, w której każdy może wziąć udział, zgłaszając chęć uczestnictwa na stronie internetowej www.saferInternet.pl. W projekcie Awareness uczestniczą także instytucje, prowadzące działania na rzecz bezpiecznego korzystania z Internetu. Ostatnio konsorcjum zostało zaproszone do wzięcia udziału we wstępnych negocjacjach w sprawie wkładu/pracy na rzecz kolejnego programu *Safer Internet*, który będzie prowadzony w latach 2007/2008. Projekt jest współfinansowany przez NASK i Fundację Dzieci Niczyje, oraz w 50% przez Unię Europejską.

Wcześniej, w roku 2004, Fundacja rozpoczęła program „Dziecko w sieci”, którego celem jest podnoszenie świadomości wśród dzieci na temat zagrożeń, jakie czyhają w Internecie. Więcej szczegółów na temat programu znajduje się na stronie internetowej www.dzieckowsieci.pl (tylko w języku polskim).

Kolejną inicjatywą prowadzoną przez wiele lat pod auspicjami ministra nauki i informatyzacji (obecnie minister edukacji i nauki) przez NASK jest seria corocznie organizowanych konferencji „SECURE”, których celem jest propagowanie wiedzy na temat systemu bezpieczeństwa komputerów i sieci. Konferencje są organizowane

od 1997 r. i są uważane za najbardziej poważane tego typu wydarzenie w Polsce. Organizatorami tego przedsięwzięcia są NASK i CERT Polska, a od 2005 r. także ENISA. Podczas ceremonii inaugurującej konferencję, przedstawiciel ministra zazwyczaj wygłasza wykład dotyczący zagadnień związanych z zaangażowaniem sektora publicznego w rozwój e-administracji w Polsce.

NASK i CERT Polska prowadzą także bardzo ważną stronę internetową mającą na celu poszerzanie wiedzy specjalistów IT i użytkowników prywatnych; na stronie znajdują się informacje na temat nowych zagrożeń, słabych punktów i incydentów, jak również środków zapobiegawczych i ostrzeżeń na temat możliwych ataków.

Zob. <http://www.cert.pl/>

23. Portugalia

Na podstawie odpowiedzi na kwestionariusz oraz uzupełniających informacji z przeprowadzonych rozmów, badań i dodatkowych materiałów dla Portugalii wyszczególniono następujące części:

[Rząd jako twórca prawnych, regulacyjnych i instytucjonalnych uregulowań służących poszerzaniu wiedzy](#)

[Władze państwowe jako użytkownik systemów informacyjnych](#)

[Władze lokalne jako użytkownik systemów informacyjnych](#)

[Rząd jako partner przedsiębiorstw i przemysłu](#)

[Rząd jako partner społeczeństwa](#)

[Statystyki i kluczowe wskaźniki wydajności \(KPI\)](#)

Rząd jako twórca prawnych, regulacyjnych i instytucjonalnych uregulowań służących poszerzaniu wiedzy

Krajowa strategia poszerzania wiedzy

Koordynowanie strategii informacyjnej na temat bezpieczeństwa należy do obowiązków UMIC (portugalska agencja społeczeństwa wiedzy www.umic.pt). Ogólnym celem jest zdefiniowanie Krajowej Polityki Bezpieczeństwa Informacji.

UMIC opublikował dokument, który zawiera szeroki zestaw strategicznych celów związanych z tworzeniem kultury informacji i sieci bezpieczeństwa w kluczowych sektorach społeczeństwa portugalskiego. Z powodu charakteru społeczeństwa informacji i odpowiedzialności rządu strategia jest bardziej ukierunkowana na sektor publiczny.

Niektóre działania są już realizowane przez rząd i inne publiczne i prywatne instytucje, działające na podstawie upoważnienia i pod nadzorem rządu.

Prawne, regulacyjne i instytucjonalne ustalenia w celu poszerzania wiedzy

Nie zostały podjęte żadne prawne i regulacyjne środki na rzecz poszerzania wiedzy. Jednakże kilka inicjatyw już zostało wdrożonych. Są to inicjatywy takie, jak:

- utworzenie portugalskiego CERT (www.cert.pt); działania stworzone początkowo na potrzeby sektora badawczego i naukowego, obecnie dotyczą większego zakresu użytkowników;

- zorganizowano kursy szkoleniowe mające na celu poszerzanie wiedzy we wszystkich sektorach portugalskiego społeczeństwa;
- kursy zorganizowane szczególnie z myślą o pracownikach technicznych administracji publicznej Instituto Nacional de Administração (www.ina.pt)
- Ministerstwo Edukacji podjęło specjalną inicjatywę skierowaną do studentów (www.crie.minedu.pt).

Dodatkowe informacje można uzyskać odwiedzając wyżej wymienione strony internetowe.

Władze państwowe jako użytkownik systemów informacyjnych

Najnowsze programy i inicjatywy poszerzania wiedzy

Inicjatywy rządowe w zakresie tego obszaru miały raczej ograniczony charakter.

Tematem Międzynarodowego Dnia Telekomunikacji, jaki miał miejsce w maju 2006 r. była cyberprzestępczość. Zorganizowano specjalne wydarzenie, podczas którego głos zabrali przedstawiciele administracji publicznej, przedstawiciele portugalskiej agencji ENISA i sektora przemysłu. Wydarzenie było szeroko relacjonowane w mediach.

W związku z sukcesem, jaki odniosło wydarzenie, FCCN (www.fccn.pt) – organizacja obsługująca CERT – podpisała ostatnio umowę z rządową agencją finansującą w celu zwiększenia ilości i zakresu działań w mediach.

W celu uzyskania dalszych informacji na temat inicjatyw skierowanych do administracji publicznej por. część [Rząd jako twórca](#).

Władze lokalne jako użytkownik systemów informacyjnych

Najnowsze programy i inicjatywy poszerzania wiedzy

Władze lokalne, ze względu na charakter politycznej organizacji państwa, nie prowadzą żadnych działań w tym zakresie.

Rząd jako partner przedsiębiorstw i przemysłu

Małe i średnie przedsiębiorstwa (MŚP)

Dotychczas nie zorganizowano żadnej znaczącej inicjatywy na rzecz poszerzania wiedzy, która byłaby promowaną przez rząd.

Sprzedawcy i pośrednicy oprogramowania prowadzą pewne inicjatywy na rzecz poszerzania wiedzy na temat bezpieczeństwa informacji, jednak rząd w nich nie bierze w nich bezpośrednio udziału.

Dostawcy Usług Internetowych (ISP)

Współpraca między rządem i ISP nie została zorganizowana bezpośrednio przez rząd ale przez FCCN, organizację prowadzącą portugalską Krajową Sieć Badawczą i Edukacyjną NREN.

W Portugalii działa wielu dostawców usług internetowych; w ostatnich latach miał też miejsce znaczny wzrost stopnia korzystania z technologii szerokopasmowych (kablowych i ADSL). Stale rośnie też liczba hotspotów, czyli miejsc w których możliwy jest dostęp szerokopasmowy. Ze względu na charakter tych technologii, ISP przekazywały informacje swoim klientom na temat szczególnych problemów związanych z tymi technologiami z powodu rosnącego zagrożenia, które jest wynikiem stale wzrastającego stopnia korzystania z sieci i dostępności szerszego pasma przepustowości łącza.

FCCN przez około 2 lata organizowało okresowe spotkania z dostawcami usług internetowych w celu omawiania środków, jakie powinien podjąć sektor gospodarczy, do którego należą, aby móc kontrolować problemy. Dla ISP najbardziej znaczącym problemem jest spam i problemy związane ze złośliwymi e-mailami. Uruchomione zostało forum, na którym dostawcy usług internetowych dzielą się informacjami na temat problemów związanych z bezpieczeństwem oraz technik i rozwiązań, jakie stosują żeby rozwiązać owe problemy. Mimo że na rynku konkurują ze sobą, obszar ten jest miejscem, w którym współpraca jest postrzegana w kategoriach korzyści dla wszystkich stron.

W ramach projektu rozpoczęto tworzenie platformy służącej wymianie informacji między dostawcami usług internetowych na temat czarnych list spammerów. FCCN będzie koordynatorem tego projektu. Wraz z tą inicjatywą każdy ISP podejmuje (skierowane do swoich klientów) pewne inicjatywy mające na celu poszerzanie wiedzy na temat kwestii bezpieczeństwa, a mianowicie przekazywania informacji na temat szczegółów dotyczących dobrych praktyk w tym zakresie.

Media

Należy zauważyć, że zamieszczone poniżej przykłady wykorzystują media jako kanał dotarcia do innych grup docelowych i nie przedstawiają mediów jako odrębnej grupy docelowej.

Inicjatywy nie były zorganizowane z myślą o mediach, jednak niektóre z nich zostały nagłośnione w mediach, a mianowicie w prasie. W ten sposób przyjęta strategia miała na celu rozpoczęcie projektów (np. finansowany przez rząd projekt CERT.PL) przy czym inicjatywy organizowane w ramach projektu były relacjonowane w prasie.

Znaczącym problemem, jaki istnieje w tym sektorze jest to, że zazwyczaj tylko prasa (specjalistyczna lub niespecjalistyczna) śledzi tego typu wydarzenia. Telewizja, która mogłaby mieć dużo większy zasięg, mimo podjętych starań nie relacjonowała żadnego z przeprowadzonych działań.

Zorganizowanie Dnia Cyberbezpieczeństwa, w którym uczestniczyli specjaliści z rządu i sektora przemysłu, było najbardziej widoczną inicjatywą ponieważ przewodniczył jej minister odpowiedzialny za ten obszar. Więcej projektów na rzecz poszerzania wiedzy ma być prowadzonych zgodnie z tą inicjatywą.

Także niektóre specjalistyczne magazyny (dla informatyków) poświęcają uwagę temu zagadnieniu; specjaliści przygotowują artykuły na temat zagadnień związanych z bezpieczeństwem sieci.

Publiczno-prywatne partnerstwo

Skuteczne partnerstwo publiczno-prywatne (w dziedzinie poszerzania wiedzy i edukacji/szkolenia)

W związku z wysokim stopniem korzystania z platform Microsoftu, rząd podpisał umowę o współpracy z firmą Microsoft i FCCN w sprawie wymiany informacji na temat bezpieczeństwa komputerów. Umowa ta została podpisana niedawno (lipiec 2006 r.) i oczekuje się, że będzie miała duży wpływ na poszerzanie wiedzy i kształcenie użytkowników.

Powód ustanowienia współpracy między rządem, Microsoftem i FCCN jest związany z wykorzystaniem synergii tych podmiotów.

Pierwszym krokiem będzie comiesięczna publikacja raportów zawierających informacje na temat bezpieczeństwa z odniesieniem do ataków, zagrożeń i metod ich zwalczania. Raport będzie publikowany na stronach internetowych firmy Microsoft i CERT.PL (www.cert.pl). Komunikaty prasowe będą pojawiały się okresowo, aby umożliwić dostęp do tych informacji szerszemu gronu odbiorców.

Przyszłe partnerstwa publiczno-prywatne

Istnieją plany dotyczące uruchomienia podobnych inicjatyw we współpracy z innymi podmiotami działającymi w tym sektorze, ale do chwili obecnej nie zawarto żadnych umów i informacje nie mogą być aktualnie udostępnione.

Rząd jako partner społeczeństwa

Najnowsze programy i inicjatywy poszerzania wiedzy

Jeszcze nie ma inicjatyw skierowanych bezpośrednio do użytkowników prywatnych. Wszystkie inicjatywy opisane w poprzednich częściach pośrednio są skierowane do tych odbiorców.

Statystyki i kluczowe wskaźniki wydajności (KPI)

Statystyki/KPI do oceny skuteczności inicjatywy poszerzania wiedzy

Jedyne istniejące statystyki pochodzą z portugalskiego zespołu CERT (www.cert.pt) wraz z klasyfikacją incydentów naruszenia bezpieczeństwa, zgłoszonych zespołowi CERT.

Istnieją również statystyki stworzone przez dostawców usług internetowych, ale są oni niechętni wobec podania tych informacji do wiadomości publicznej.

Znaczenie statystyk/KPI

Stworzenie pewnych wspólnych statystyk mogłoby być przydatne, ale ze względu na dynamiczny charakter problemów związanych z bezpieczeństwem statystyki takie są ciągle nieaktualne.

24. Słowacja

Na podstawie odpowiedzi na kwestionariusz oraz uzupełniających informacji z przeprowadzonych rozmów, badań i dodatkowych materiałów dla Słowacji wyszczególniono następujące części:

[Rząd jako twórca prawnych, regulacyjnych i instytucjonalnych uregulowań służących poszerzaniu wiedzy](#)

[Władze państwowe jako użytkownik systemów informacyjnych](#)

[Władze lokalne jako użytkownik systemów informacyjnych](#)

[Rząd jako partner przedsiębiorstw i przemysłu](#)

[Rząd jako partner społeczeństwa](#)

[Statystyki i kluczowe wskaźniki wydajności \(KPI\)](#)

Rząd jako twórca prawnych, regulacyjnych i instytucjonalnych uregulowań służących poszerzaniu wiedzy

Krajowa strategia poszerzania wiedzy

Nie ma dostępnych informacji na temat strategii poszerzania wiedzy prowadzonych w chwili obecnej na szczeblu krajowym.

Prawne, regulacyjne i instytucjonalne uregulowania służące poszerzaniu wiedzy

Planowane jest utworzenie zbioru informacji na płycie CD lub w wersji online, obejmujących takie tematy jak poszerzanie wiedzy w dziedzinie bezpieczeństwa informacji i słowniki techniczne. Ponadto istnieją inicjatywy dotyczące projektów edukacyjnych skierowanych do takich grup jak rządowi pracownicy techniczni i prawnicy.

Pod koniec 2005 r. utworzono Komisję ds. Bezpieczeństwa Informacji, będącą organem doradczym Rządowego Pełnomocnika ds. Społeczeństwa Informacyjnego. W skład Komisji wchodzi odpowiedni specjaliści z sektora rządowego, prywatnego i środowiska akademickiego.

Władze państwowe jako użytkownik systemów informacyjnych

Najnowsze programy i inicjatywy poszerzania wiedzy

Do chwili obecnej nie było żadnego oficjalnego programu dotyczącego poszerzania wiedzy użytkowników będących pracownikami władz państwowych.

Władze lokalne jako użytkownik systemów informacyjnych

Najnowsze programy i inicjatywy poszerzania wiedzy

Do chwili obecnej nie było żadnego oficjalnego programu dotyczącego poszerzania wiedzy użytkowników będących pracownikami władz lokalnych.

Rząd jako partner przedsiębiorstw i przemysłu

Małe i średnie przedsiębiorstwa (MŚP)

Obecnie nie są realizowane żadne inicjatywy dotyczące poszerzania wiedzy w grupie docelowej MŚP.

Dostawcy usług internetowych (ISP)

Obecnie nie są realizowane żadne inicjatywy dotyczące poszerzania wiedzy w grupie docelowej ISP.

Media

Należy zwrócić uwagę, że we wskazanym niżej przykładzie media wykorzystane są jako kanał dotarcia do innych grup docelowych, i nie są przedstawione jako odrębna grupa docelowa.

Obecnie nie są realizowane żadne inicjatywy dotyczące poszerzania wiedzy w grupie docelowej media.

Planowane jest dotarcie do społeczeństwa poprzez takie kanały medialne jak telewizja, prasa i radio. Kanały te są uważane za najskuteczniejsze pod względem możliwości dostarczenia wiadomości promujących kulturę bezpieczeństwa.

Partnerstwo publiczno-prywatne

Skuteczne partnerstwo publiczno-prywatne (w dziedzinie poszerzania wiedzy i edukacji/szkolenia)

Wyższe uczelnie techniczne wykorzystywane są do kształcenia młodych ludzi w dziedzinie kultury bezpieczeństwa, mogą one także edukować społeczeństwo za pośrednictwem kilku programów szkoleniowych i edukacyjnych.

Możliwe jest także stworzenie programów edukacyjnych we współpracy z sektorem prywatnym.

Przyszłe partnerstwa publiczno-prywatne

Planowane są partnerstwa z sektorem naukowym w zakresie pracy nad projektami edukacyjnymi w dziedzinie bezpieczeństwa informacji.

Rząd jako partner społeczeństwa

Najnowsze programy i inicjatywy poszerzania wiedzy

Planowane jest utworzenie zbioru informacji na płycie CD lub w wersji online, obejmujących takie tematy jak poszerzanie wiedzy w dziedzinie bezpieczeństwa informacji i słowniki techniczne. Główną grupą docelową będą użytkownicy prywatni; głównymi wykorzystywanymi kanałami medialnymi będą: telewizja, prasa i radio.

Partnerstwo publiczno-prywatne

Skuteczne partnerstwo publiczno-prywatne (w dziedzinie poszerzania wiedzy i edukacji/szkolenia)

Planowane są partnerstwa z sektorem naukowym w zakresie pracy nad projektami edukacyjnymi w dziedzinie bezpieczeństwa informacji.

Statystyki i kluczowe wskaźniki wydajności (KPI)

Statystyki/KPI do oceny skuteczności inicjatywy poszerzania wiedzy

Ponieważ w kraju nie istnieją żadne oficjalne inicjatywy poszerzania wiedzy, brak jest możliwości zastosowania statystyk lub wskaźników KPI. W przyszłości planuje się stosować je do oceny skuteczności kampanii.

25. Słowenia

Na podstawie odpowiedzi na kwestionariusz oraz uzupełniających informacji z przeprowadzonych rozmów, badań i dodatkowych materiałów dla Słowenii wyszczególniono następujące części:

Obecna sytuacja

Rząd jako twórca prawnych, regulacyjnych i instytucjonalnych uregulowań służących poszerzaniu wiedzy

Władze państwowe jako użytkownik systemów informacyjnych

Władze lokalne jako użytkownik systemów informacyjnych

Rząd jako partner przedsiębiorstw i przemysłu

Rząd jako partner społeczeństwa

Statystyki i kluczowe wskaźniki wydajności (KPI)

Obecna sytuacja

- W Słowenii odsetek użytkowników Internetu jest wyższy niż w wielu innych państwach członkowskich UE. Według danych Urzędu Statystycznego Republiki Słowenii¹⁶ w pierwszym kwartale 2005 r. ponad 840 tys. osób w wieku od 10 do 74 lat regularnie (w ciągu ostatnich trzech miesięcy) korzystało z Internetu. Z tej liczby 440 tys. stanowili mężczyźni, a 400 tys. – kobiety. W pierwszym kwartale 2005 r. 87% gospodarstw domowych posiadało co najmniej jeden telefon komórkowy, 61% posiadało komputer osobisty, a 48% dostęp do Internetu. Z tej liczby 40% posiadało łącze szerokopasmowe (np. ADSL, łącze kablowe, UMTS). W Słowenii odsetek gospodarstw domowych z dostępem do Internetu był równy średniej w UE-25. W tym samym okresie 50% ludności w wieku od 10 do 74 lat regularnie (w ciągu ostatnich trzech miesięcy) korzystało z Internetu, natomiast 12% ludności dokonało zakupów przez Internet.
- W Słowenii dostęp do Internetu posiada duża liczba dzieci. Około 40% dzieci/młodzieży z grupy ludności w wieku od 10 do 15 lat korzysta z Internetu codziennie lub prawie codziennie. Około 33% dzieci/młodzieży korzysta z Internetu co najmniej raz w tygodniu. Około 8% dzieci/młodzieży korzysta

16 Urząd Statystyczny Republiki Słowenii: Stosowanie technologii ICT w gospodarstwach domowych, I kwartał 2005 r.: http://www.stat.si/eng/novice_poglej.asp?ID=893

z Internetu co najmniej raz w miesiącu, a około 2% dzieci/młodzieży korzysta z Internetu rzadziej niż raz w miesiącu¹⁷.

Dane te dobrze wróżą, ponieważ z jednej strony oznaczają, że Słowenia posiada duży potencjał rozwoju, ale z drugiej strony budzą obawy w kwestiach związanych z bezpiecznym korzystaniem z Internetu i obawy co do kontaktu młodzieży ze szkodliwą i nielegalną treścią. Badania Eurobarometr 2004¹⁸ zawierają bardziej szczegółowe informacje na temat tych zagadnień:

- Około 45% słoweńskich rodziców informuje, że stosują ograniczenia dotyczące korzystania z Internetu (średnia w UE-25 wynosi 45%). Można je podzielić na pięć kategorii: ograniczenia dotyczące prywatności, dostępu do nieprzystoitych treści, przesyłania plików, ograniczenia czasowe i zgłaszanie problemów
- Blisko 46% słoweńskich rodzin twierdzi, że nie odczuwają potrzeby poszerzania wiedzy w zakresie szkodliwych i nielegalnych treści zamieszczanych w Internecie
- Zgodnie z wynikami badań przeprowadzonych przez RIS w 2004 r.¹⁹ około 54% słoweńskich rodziców wyraża niepokój w odniesieniu do bezpieczeństwa dzieci podczas korzystania z Internetu. Jednakże w społeczeństwie poziom wiedzy o problemie szkodliwych i nielegalnych treści przedstawianych w Internecie i nowych technologiach sieciowych jest wciąż stosunkowo niski. Zainteresowanie budzi fakt, że 52% słoweńskich rodzin uważa, że ich dzieci wiedzą, jak należy postąpić w szkodliwej sytuacji sieciowej (średnia w EU-25 wynosi 60%)

Rząd jako twórca prawnych, regulacyjnych i instytucjonalnych uregulowań służących poszerzaniu wiedzy

Krajowa strategia poszerzania wiedzy

Nie istnieje dobrze zdefiniowany program, który można byłoby uznać za strategię krajową. Jednakże miały miejsce pewne działania wspierane przez rząd, których celem było poszerzenie wiedzy społeczeństwa o rosnącej liczbie naruszeń bezpieczeństwa informacji i zagrożeń dla tego bezpieczeństwa. Aby rozwiązać problem przyjęto podejście oddolne, które przeważało w przeszłości. W sytuacji gdy nie istniała żadna jasna strategia, uważano, że poprzez wspieranie różnych inicjatyw i działań różnych stron osiągnie się przynajmniej jakieś efekty synergii. Rząd zdaje sobie sprawę z tego problemu i stara się być aktywny, ale jego aktywność nie jest proporcjonalna do rozmiaru problemu. Na przykład phishing nie stanowi jeszcze zagrożenia w Słowenii, więc nie ma potrzeby rozpoczynania wielkiej kampanii, która rozwiązałaby praktycznie nieistniejący problem.

17 Badania RIS: Badanie stosowania technologii ICT w gospodarstwach domowych i przez osoby fizyczne w 2005 r., pod adresem: (<http://www.ris.org>); Wyniki będą publicznie dostępne za kilka miesięcy.

18 EuroBarometer (2004 r.): Nielegalne i szkodliwe treści w Internecie:

http://europa.eu.int/information_society/activities/sip/docs/pdf/reports/eurobarometer_EU25_highlights.pdf

19 Raport RIS: Działania sieciowe w 2004 r., pod adresem: <http://www.ris.org>

Prawne, regulacyjne i instytucjonalne ustalenia w celu poszerzania wiedzy

Z perspektywy prawnej Słowenia uznaje łączność elektroniczną i formularze elektroniczne. Stosowane środki prawne i regulacyjne przewidują i definiują wykorzystanie określonych środków do osiągnięcia odpowiednich poziomów bezpieczeństwa, zarówno w sektorze przedsiębiorczości, jak i w sektorze rządowym. Ramy prawne regulują kwestie bezpieczeństwa na różnych szczeblach. Najczęściej kwestie bezpieczeństwa są wdrażane poprzez regulacje prawne dotyczące ochrony praw konsumentów, a także elektronicznej przedsiębiorczości i łączności. Istnieją również określone dla rządu regulacje prawne dotyczące kwestii bezpieczeństwa, np. ZUP.

Do tej pory nie określono żadnych konkretnych kampanii na szczeblu krajowym. Zazwyczaj propagowanie najlepszych praktyk odbywa się za pomocą różnorodnych metod, w tym ukierunkowanych badań i projektów rozpowszechniania wiedzy (CRP). Do przykładów należą: Računalniška kriminaliteta, warsztaty takie jak warsztaty NATO dotyczące zaawansowanego bezpieczeństwa i publikacje takie jak forum Varnostni. Najpowszechniejsze kwestie dotyczące bezpieczeństwa są traktowane jako zagadnienia wertykalne w konkretnej dziedzinie, np. fakturowanie elektroniczne.

Zapewnianie bezpieczeństwa na kolejnym stopniu jest wykonywane poprzez dostawców usług na dwóch poziomach: jako gotowe (out-of-the-box) rozwiązanie połączone z aktywacją usług (np. dostarczanie usług internetowych wraz z ochroną antywirusową i zaporą sieciową) lub jako integralna część usług (np. osobista ochrona antywirusowa i zaporą sieciową na poziomie sieci).

Inicjatywy o międzynarodowym poparciu są realizowane poprzez dedykowany rozwój lub poprzez projekty badań i rozwoju na skalę europejską.

Zarząd ds. Społeczeństwa Informacyjnego Ministerstwa Szkolnictwa Wyższego, Nauki i Technologii jest odpowiedzialny za bezpieczeństwo e-handlu i zapobieganie niewłaściwemu wykorzystaniu Internetu.

Uwzględnione sektory obejmują tworzenie warunków dla bezpiecznego i sprawnego handlu elektronicznego, a także rozwijanie strategii i środków do walki z nadużyciami Internetu.

Ministerstwo Administracji Publicznej jest zakorzenione w Rządowym Centrum Informatycznym Republiki Słowenii, które zostało utworzone w styczniu 1993 r. na mocy Ustawy o rządzie Republiki Słowenii (Dz.U. Republiki Słowenii, nr 4/93).

Ministerstwo Administracji Publicznej współpracuje przy wykonywaniu zadań z organizacjami państwowymi, międzynarodowymi, krajowymi i zagranicznymi organizacjami rządowymi i pozarządowymi, a także z wyspecjalizowanymi instytucjami z zakresu technologii ICT.

Za stworzenie właściwej strategii w zakresie bezpieczeństwa i ochrony danych odpowiedzialna jest Służba Bezpieczeństwa i Ochrony. Strategia ta ma służyć jako baza do praktycznego wdrożenia i zintegrowania poszczególnych procesów we wspólny system bezpieczeństwa i ochrony danych. Łączy ona poprzednie doświadczenia i rozwiązania stosowane przez poszczególne instytucje z nowoczesnymi tendencjami, a także z obecnymi, rozwijanymi i europejskimi standardami. Poza zintegrowaniem strategii bezpieczeństwa na szczeblu organizacji państwowych i administracji publicznej, do zadań bezpieczeństwa i ochrony danych należy wdrażanie systemów i rozwiązań. Badania obejmują także koordynację innych wykonawców (takich jak organizacje, usługi i instytucje), nadzór nad wdrażaniem i, w zależności od wyników wdrażania, stworzenie dalszych kierunków/działań.

Plan aktywności publicznej (zatytułowany „Plan działań e-administracji do 2004 roku”) zawiera kilka działań ukierunkowanych na bezpieczeństwo IT. Obejmują one strategię bezpieczeństwa informacji i polityki certyfikacyjne rządowych organów certyfikacyjnych: SIGEN-CA i SIGOV-CA. Tematy związane z edukacją i szkoleniem w dziedzinie bezpieczeństwa IT zaplanowano w „Planie działań e-administracji na lata 2005-2008”.

Skuteczność inicjatyw jest monitorowana poprzez strukturę 0-4, złożoną z czterech etapów, opartą na metodologii „eGovernment indicators for benchmarking eEurope” [Wskaźniki e-administracji do analizy porównawczej eEurope]. Poziom osiągnięty w tym momencie definiuje się jako obecny poziom „CLx” (gdzie x oznacza poziom od 0 do 4), natomiast poziom, którego osiągnięcie jest planowane, definiuje się jako poziom docelowy „TLx”.

Niektóre elementy „Planu działań e-administracji do 2004 roku” mogą być uznane za dobre praktyki, ponieważ kierują się one międzynarodowymi standardami. Na przykład, strategia bezpieczeństwa informacji jest zgodna ze standardem ISO/IEC 17799. Ponadto polityki certyfikacyjne organów certyfikacyjnych, SIGOV-CA i SIGEN-CA, oparte są na takich standardach jak ETSI TS 101 456. Opublikowano również dokument zatytułowany „Security requirement for applications using digital certificates” [Wymogi bezpieczeństwa dla aplikacji korzystających z certyfikatów cyfrowych].

Policja

Policja jako organ Ministerstwa Spraw Wewnętrznych wykonuje swoje zadania w ramach jednostek organizacyjnych na szczeblu krajowym, regionalnym i lokalnym. Generalna Dyrekcja Policji, składająca się z dziesięciu wewnętrznych jednostek organizacyjnych, działa na szczeblu krajowym. Na szczeblu regionalnym funkcjonuje 11 regionalnych dyrekcji policji, a na szczeblu lokalnym działa 99 lokalnych komisariatów policji.

Wydział ds. Przestępczości Komputerowej jest jednostką organizacyjną policji do walki z cyberprzestępczością. Jednostki organizacyjne na szczeblu regionalnym zajmują się dochodzeniami w poważnych i zorganizowanych przestępstwach z wykorzystaniem

technologii IT, takich jak hakerstwo lub niszczenie stron internetowych, uniemożliwianie wykonywania usług internetowych lub wywoływanie infekowania wirusami komputerowymi.

Policja wykonuje również pewne stałe działania, które można wykorzystać do poszerzania wiedzy w społeczeństwie na temat zagadnień dotyczących bezpieczeństwa informacji. Zazwyczaj po zakończeniu dochodzenia w bardziej złożonej sprawie karnej związanej z cyberprzestępczością, oficjalni przedstawiciele policji udzielają wywiadów podczas konferencji prasowych. W prasie i w Internecie często publikowane są komunikaty prasowe dotyczące danego tematu. Policyjni eksperci wygłaszają także wywiady w trakcie różnych konferencji związanych z bezpieczeństwem informacji. Obecnie trwają prace nad ulotką zatytułowaną "Ali se zavedate nevarnosti Interneta?" [Czy jesteś świadom zagrożeń w sieci?].

Szkolnictwo podstawowe i ponadpodstawowe

Podczas różnych seminariów nauczyciele gromadzą konkretną wiedzę związaną z zagadnieniami bezpieczeństwa informacji, co ma na celu promowanie technologii informacyjnych i komunikacyjnych w szkołach. Istnieje specjalna grupa nauczycieli, zwanych „multiplikatorji” (tj. „mnożniki” – osoby rozpowszechniające wiedzę), którzy są specjalnie wykształceni i wykwalifikowani przez Państwowy Instytut Edukacji Republiki Słowenii (<http://www.zrss.si/>) do kształcenia innych nauczycieli. Grupa ta przekazuje wiedzę na temat zagadnień związanych z ICT, w tym dotyczących bezpieczeństwa. W słoweńskim szkolnictwie istnieje kilka innych instytucji, które aktywnie uczestniczą w europejskich programach, takich jak Comenius, Leonardo da Vinci, Gruntvig i eLearning. Wiele projektów w ramach programów obejmuje zagadnienia związane z bezpieczeństwem informacji. Na Słowenii strategia bezpieczeństwa informacji jest niemal wyłącznie przygotowywana przez ARNES (Słoweńską Sieć Naukowo-Akademicką).

ARNES

ARNES (Słoweńska Sieć Naukowo-Akademicka) świadcząca usługi SI-CERT została uznana przez słoweńskie Ministerstwo Społeczeństwa Informacyjnego za ośrodek ekspercki w dziedzinie bezpieczeństwa sieci i informacji. Ponieważ ministerstwo dostrzegło rosnące znaczenie bezpieczeństwa sieci, sporządzono projekt i przydzielono go ARNES. Projekt ten umożliwił stworzenie szczegółowej bazy wiedzy, zawierającej różne ujęcia problemów i rozwiązania w zależności od docelowych odbiorców (np. ogół społeczeństwa, pracownicy techniczni dostawców usług internetowych i organów ochrony porządku publicznego).

SI-CERT

Słoweński zespół reagujący na naruszenia bezpieczeństwa w Internecie został utworzony w 1995 r. w ramach Słoweńskiej Sieci Naukowo-Akademickiej (ARNES)

w celu stworzenia centralnego ośrodka koordynującego obsługę incydentów naruszenia bezpieczeństwa w sieci. SI-CERT świadczy usługi zarówno instytucjom, jak i osobom fizycznym.

Miesięcznie zespół SI-CERT zajmuje się około 100 incydentami. Aby móc świadczyć usługi, każdy zespół CERT musi zgromadzić znaczna wiedzę w zakresie różnych zagadnień dotyczących bezpieczeństwa. Wiedza ta jest wykorzystywana przy badaniu incydentów, bezpośrednio w roli doradczej lub w celu przeprowadzenia konkretnych działań poszerzania wiedzy w społeczeństwie. Działania poszerzania wiedzy obejmują także wydawanie biuletynów i poradników.

Są to publikacje SI-CERT bezpośrednio odnoszące się do problemów dotyczących bezpieczeństwa, zaobserwowanych w społeczeństwie. Poradniki zawierają krótkie omówienia nowo odkrytych luk w bezpieczeństwie wraz z dostępnymi rozwiązaniami tymczasowymi i trwałymi. Skierowane są one zarówno do ogółu społeczeństwa, jak i do administratorów systemów.

Biuletyny zawierają bardziej ogólne artykuły, opisujące konkretny rodzaj problemu dotyczącego bezpieczeństwa na szerszym tle. Przeznaczone są one raczej dla ogółu społeczeństwa, ale zawierają także odniesienia do szczegółów technicznych. Biuletyny SI-CERT zawierają np. artykuły na temat phishingu i dialerów. Celem biuletynów jest nie tyle dostarczenie konkretnych rozwiązań technicznych danego problemu, co poszerzanie wiedzy na temat określonych zagadnień i sugerowanie działań i zachowań, które umożliwiają użytkownikom uniknięcie danych zagrożeń. Często odbywa się to poprzez wykłady lub prezentacje.

Członkowie zespołu CERT korzystają z różnych możliwości, aby dotrzeć do rozmaitych grup społecznych, przedstawić im zagadnienia dotyczące bezpieczeństwa i poszerzyć w ten sposób wiedzę na dany temat. Wykłady i prezentacje uwzględniają lokalne wydarzenia społeczne, a także specjalistyczne kursy dla nauczycieli szkół podstawowych i ponadpodstawowych, którzy przekazują dalej informacje innym nauczycielom w danym regionie.

Uniwersytet w Mariborze, Wydział Prawa Karnego

Wydział Prawa Karnego posiada sześć instytutów: nauk społecznych, prawa, nauk informatycznych i metodologii, dochodzeniowy i kryminologii oraz prawa karnego, bezpieczeństwa, a także zarządzania i administracji w policji. Instytuty odpowiedzialne za kształcenie i Instytut Badań nad Prawem Karnym mają znaczący udział w badaniach nad kwestiami dotyczącymi bezpieczeństwa w nowoczesnym społeczeństwie. Członkowie instytutów świadczą także usługi związane z poradami i szkoleniem w różnych dziedzinach systemu bezpieczeństwa. Instytut informatyki i metodologii zajmuje się informatyką, statystyką i metodologią. Głównym celem prac instytutu jest przekazanie studentom podstawowej wiedzy potrzebnej do zajmowania się badaniami naukowymi i analizowania zjawisk związanych z bezpieczeństwem. Kolejną ważną

funkcję instytutu stanowią prace nad bazami danych i programami do projektów badawczych. Instytut zapewnia także wsparcie informatyczne, obejmujące różne zagadnienia z dziedziny bezpieczeństwa informacji, w całym procesie badawczym i naukowym wydziału. Wydział Prawa Karnego po raz pierwszy oferuje możliwość specjalistycznych studiów w dziedzinie bezpieczeństwa informacji. Studia skupiają się na wszystkich aspektach zagrożeń dla bezpieczeństwa informacji i na narzędziach zapobiegających takim zagrożeniom.

Grupę docelową stanowią absolwenci (prawie wszystkich kierunków studiów), którzy będą stosować systemy informacyjne jako główne narzędzie, a także osoby już zatrudnione i pracujące w dziedzinach, w których taka wiedza jest obowiązkowa.

Władze państwowe jako użytkownik systemów informacyjnych

Najnowsze programy i inicjatywy poszerzania wiedzy

Na szczeblu krajowym nie istnieją żadne określone programy poszerzające wiedzę w dziedzinie bezpieczeństwa IT, ponieważ kwestie bezpieczeństwa uwzględnione są w ustawodawstwie lub zajmują się nimi wyspecjalizowane programy realizowane przez osoby prywatne lub wspólne przedsięwzięcia (typu joint venture) sektora rządowego i sektora przemysłu. Kultura bezpieczeństwa jest także rozwijana poprzez „tematyczne” inicjatywy w różnych sektorach, np. zaufana i bezpieczna przedsiębiorczość elektroniczna.

Przykładem indywidualnej inicjatywy poszerzania wiedzy w dziedzinie bezpieczeństwa jest samodzielne promowanie kluczowej infrastruktury publicznej poprzez różne usługi e-administracji lub e-biznesu. W wyniku adresowanych działań, takich jak warsztaty NATO dla regionu dotyczące zaawansowanego bezpieczeństwa w łączności sieciowej, zajęto się indywidualnymi programami poszerzania wiedzy. Ponadto w przeszłości zdefiniowano wspólne przedsięwzięcia sektora rządowego i sektora przemysłu, dotyczące głównie współpracy technicznej (np. e-Slog lub moja.posta).

Obserwacja kultury bezpieczeństwa przeprowadzana jest poprzez badania rynkowe i technologiczne wykonywane przez osoby prywatne i programy finansowane ze środków rządowych, np. Raba Interneta v Sloveniji (RIS - Badania nad Słoweńskim Internetem). Kwestie bezpieczeństwa stają się integralną częścią infrastruktury społeczeństwa informacyjnego i jako takie powinny być propagowane. Czynniki bezpieczeństwa informacji stanowi więc równoległą lub zintegrowaną sekcję tematyczną w programach takich jak e-zdrowie, e-administracja, e-biznes i e-learning.

Władze lokalne jako użytkownik systemów informacyjnych

Najnowsze programy i inicjatywy poszerzania wiedzy

Nie ma konkretnych programów lub inicjatyw, których celem byłoby poszerzanie wiedzy użytkowników we władzach lokalnych.

Rząd jako partner przedsiębiorstw i przemysłu

Małe i średnie przedsiębiorstwa (MŚP)

Na szczeblu technologicznym istnieją przynajmniej dwa przypadki: Rządowy CA (SIGOV-CA) jest promowany jako najczęściej stosowana infrastruktura klucza publicznego (PKI) w usługach e-administracji i e-biznesu, a e-Slog, projekt Słoweńskiej Izby Handlowej, promowany jest jako powszechny standard wiadomości handlowych. Jako część inicjatywy dotyczącej bezpiecznego e-biznesu, bezpieczeństwo zostało uwzględnione w wytycznych i zaleceniach technicznych dla zaufanej wymiany wiadomości przez przedsiębiorstwa. Inicjatywa e-Slog była wspólnym przedsięwzięciem sektora przemysłu i sektora rządowego (DURS, CVI/MJU), mającym na celu rozpowszechnianie informacji na szczeblu krajowym za pośrednictwem technicznego portalu promującego zaufaną przedsiębiorczość elektroniczną. Obecnie inicjatywa jest nadzorowana przez GS1, lokalną grupę EAN.

Usługi e-administracji są kolejnym przykładem współpracy między przemysłem a rządem w działaniach B2G (ang. *business to government*), np. deklaracje podatkowe oparte na usługach bezpieczeństwa świadczonych przez krajowych i komercyjnych certyfikowanych dostawców usług (ang. *Certified Service Provider*, CSP). Usługi e-administracji są również promowane w kontaktach między obywatelami a sektorem publicznym (ang. *citizen to government*, C2G).

Media

Należy zwrócić uwagę, że poniżej wskazany przykład wykorzystuje media jako kanał dotarcia do innych grup docelowych, i nie przedstawia ich jako odrębnej grupy docelowej.

Nie istniała żadna określona ogólnokrajowa promocja medialna prowadzona przez rząd. Miały miejsce promocje skierowane do określonych grup, przeprowadzone przez Stowarzyszenie Praw Klienta, pewne sektory publiczne (np. CVI/MJU) i organizacje prywatne (np. IDC).

Rząd jako partner społeczeństwa

Najnowsze programy i inicjatywy poszerzania wiedzy

Punkt Awareness SAFE-SI (<http://www.safe.si>)

Rząd Słowenii, a zwłaszcza Zarząd ds. Społeczeństwa Informacyjnego Ministerstwa Szkolnictwa Wyższego, Nauki i Technologii, aktywnie uczestniczy w programie Bezpieczny Internet (http://ec.europa.eu/information_society/activities/sip/index_en.htm). Jako element spójnego podejścia Unii Europejskiej, inicjatywa ta ma na celu

propagowanie bezpieczniejszego korzystania z Internetu i nowych technologii sieciowych, szczególnie wśród dzieci, a także walkę z nielegalnymi treściami i treściami niepożądanymi przez użytkownika końcowego. Zarząd ds. Społeczeństwa Informacyjnego Ministerstwa Szkolnictwa Wyższego, Nauki i Technologii jest członkiem Komisji Doradczej SAFE-SI (<http://www.safe.si>). SAFE-SI (program Bezpieczny Internet w Słowenii) jest *słoweńskim narodowym punktem Awareness*, który propaguje i wspiera poszerzanie wiedzy mające na celu ochronę i kształcenie dzieci i nastolatków w zakresie korzystania z Internetu i nowych technologii sieciowych. Partnerami w konsorcjum są *Wydział Nauk Społecznych Uniwersytetu w Lublanie* i *ARNES*. Projekt jest współfinansowany przez Dyрекję Generalną ds. Społeczeństwa Informacyjnego i Mediów w ramach Komisji Europejskiej.

Program rozpoczęto 1 marca 2005 r., a zakończy się on 28 lutego 2006 r.

Rząd Słowenii w dalszym ciągu będzie uczestniczył w programie Bezpieczny Internet poprzez współfinansowanie utworzenia punktu kontaktowego (STOPLINE.SI), który zajmowałby się zgłoszeniami dotyczącymi nielegalnych i niebezpiecznych treści w Internecie w Słowenii. Utworzenie punktu kontaktowego jest uznawane w Słowenii za ważny i konieczny krok, szczególnie, że żaden taki słoweński punkt nie istnieje. Głównym powodem utworzenia słoweńskiego punktu kontaktowego jest walka z pornografią dziecięcą, rasistowskimi i obraźliwymi treściami w Internecie, zgodnie ze słoweńskimi regulacjami prawnymi. Projekt rozpocznie się we wrześniu 2006 r.

Celem Słoweńskiego Punktu Awareness SAFE-SI (<http://www.safe.si>) są następujący odbiorcy:

- dzieci w wieku od 7 do 12 lat
- nastolatki w wieku od 13 do 17 lat
- rodzice
- nauczyciele

Pod względem dostępu do Internetu i korzystania z niego dzieci często posiadają więcej umiejętności niż ich rodzice. Jednakże, chociaż Internet daje zupełnie nowe możliwości edukacyjne, jak również dostarcza rozrywki i przydatnych informacji, to daje także dostęp do ukrytych zagrożeń, o których dzieci i rodzice nie są w pełni poinformowani. Celem jest dostarczenie rodzicom narzędzi umożliwiających kontrolowanie oraz sprawdzanie czy dzieci w domu i w szkole korzystają z Internetu w odpowiedni sposób, a także udzielenie pewnych psychologicznych/pedagogicznych porad dotyczących najlepszego radzenia sobie z zagrożeniami związanymi z Internetem. Właściwe informacje i wiedza powinny wzmocnić ich zaufanie do Internetu jako korzystnej możliwości dla dzieci i zapobiec nieuzasadnionym zakazom korzystania z jego zasobów. Celem projektu jest ponadto przekazanie wychowawcom podstawowej wiedzy na temat Internetu. Dostępne są również seminaria szkoleniowe, które zachęcają do korzystania z Internetu w szkołach w celu wykorzystywania jego możliwości jako zbiorowego narzędzia komunikacji i rozwoju kulturalnego.

Projekt SAFE-SI dotyczy poszerzania wiedzy dzieci o technologiach ICT poprzez kierowanie działań do rodziców, dzieci i nauczycieli. Celem jest służenie pomocą w kształceniu użytkowników Internetu i umożliwianiu im bezpiecznego komunikowania się, a także w rozpoznawaniu i unikaniu internetowych oszustw, przestępczości, naruszenia prywatności i niepożądanych treści.

Kampania była realizowana zgodnie z zasadą, że wiedzę należy poszerzać bez wzbudzania lęku. Poszerzanie wiedzy powinno więc działać na rzecz pozytywnego wyobrażenia. Zgodnie z przesłaniem Internet sam w sobie nie jest szkodliwy, ale istnieją pewne jego aspekty, które mogą być niebezpieczne. Wiadomość ta powinna być przekazana zarówno dorosłym, jak i dzieciom. Działania projektu ukierunkowane są na rozwijanie stron internetowych, opracowanie i rozpowszechnianie materiałów promocyjnych (np. broszur i plakatów), organizowanie prezentacji medialnych i wzbudzanie zainteresowania ze strony wszystkich mediów. Do najsukuteczniejszych inicjatyw należały:

- Projekt strony internetowej
- Konkurs narracyjny 2005
- Działania rozpowszechniające
- Dzień Bezpiecznego Internetu 2006

Na Słowenii Dzień Bezpiecznego Internetu 2006 był bardzo ważnym wydarzeniem. Obchody i imprezy organizowane przez punkt Awareness wywołały duże zainteresowanie mediów. W efekcie działania związane z Dniem Bezpiecznego Internetu były relacjonowane w całym kraju za pośrednictwem większości kanałów radiowych i telewizyjnych, a także prasy.

Priorytetem punktu Awareness jest wzmocnienie współpracy z odpowiednimi słoweńskimi mediami (cyfrowymi i tradycyjnymi) w celu zapewnienia obszernych relacji w mediach. Ma to nastąpić poprzez traktowanie kanałów medialnych jak odbiorców i omawianie z nimi zagadnień związanych z bezpiecznym korzystaniem z Internetu, także w odpowiednich programach radiowych i telewizyjnych.

Statystyki i kluczowe wskaźniki wydajności (KPI)

Statystyki/KPI do oceny skuteczności inicjatywy poszerzania wiedzy

Informacje na temat projektu RIS (Research on Internet in Slovenia – główne źródło danych o społeczeństwie informacyjnym na Słowenii) można znaleźć pod adresem: <http://www.ris.org/index.php?fl=0&p1=276&p2=285&p3=&id=334>

26. Hiszpania

Nie dostarczono żadnych informacji.

27. Szwecja

Na podstawie odpowiedzi na kwestionariusz oraz uzupełniających informacji z przeprowadzonych rozmów, badań i dodatkowych materiałów dla Szwecji wyszczególniono następujące części:

[Obecna sytuacja](#)

[Rząd jako twórca prawnych, regulacyjnych i instytucjonalnych uregulowań służących poszerzaniu wiedzy](#)

[Władze państwowe jako użytkownik systemów informacyjnych](#)

[Władze lokalne jako użytkownik systemów informacyjnych](#)

[Rząd jako partner przedsiębiorstw i przemysłu](#)

[Rząd jako partner społeczeństwa](#)

[Statystyki i kluczowe wskaźniki wydajności \(KPI\)](#)

[Doświadczenia](#)

[Kampanie](#)

Obecna sytuacja

Według corocznych badań przeprowadzanych przez Krajową Agencję ds. Poczty i Telekomunikacji (pod auspicjami instytutu Temo)²⁰

- Od 2003 r. Szwedzi stali się bardziej ostrożni w odniesieniu do własnego bezpieczeństwa w Internecie
- Szwedzkie gospodarstwa domowe w większym stopniu nauczyły się stosować podczas korzystania z Internetu zapory sieciowe i aktualizowane programy antywirusowe. W 2003 r. 23% szwedzkich gospodarstw domowych posiadało zapórę sieciową. W 2004 r. odsetek ten wzrósł do 47%. W 2002 r. 53% stosowało aktualizowane programy antywirusowe, a w 2004 r. odsetek ten wzrósł do 78%.
- Badanie²¹ oparte na losowo wybranej, warstwowej próbie z 2000 firm i organizacji zatrudniających co najmniej 50 pracowników wykazało, że:
 - 28% szwedzkich organizacji doświadczyło w ciągu ostatnich 12 miesięcy jednego z czterech następujących incydentów związanych z IT: incydenty naruszenia bezpieczeństwa skutkujące możliwością odczytu, zmiany

²⁰ Informacje można znaleźć w pliku [2005_33_sakerhetsinfo_internetanv.pdf](#)

²¹ Informacje można znaleźć w pliku [sweden_survey.pdf](#)

lub usunięcia informacji lub składników systemu przez osobę nieupoważnioną; incydenty naruszenia bezpieczeństwa skutkujące poważnym rozpoznaniem systemu; incydenty naruszenia bezpieczeństwa skutkujące brakiem dostępu do systemu lub jego części (tzw. atak typu DoS (Denial of Service); incydenty naruszenia bezpieczeństwa skutkujące poważnym atakiem złośliwego kodu, mającym znaczące następstwa dla organizacji

- Spośród organizacji, które doświadczyły jednego z czterech incydentów związanych z bezpieczeństwem IT, jedynie 4% poinformowało o incydencie policję, a 37% stwierdziło, że zgłoszenie incydentu może być złą reklamą dla organizacji

Rząd jako twórca prawnych, regulacyjnych i instytucjonalnych uregulowań służących poszerzaniu wiedzy

Krajowa strategia poszerzania wiedzy

Krajowa strategia dotycząca bezpieczeństwa informacji znajduje się w chwili obecnej na bardzo wysokim poziomie, jednak wiadomo jak istotną kwestią jest poszerzanie wiedzy. Strategia będzie realizowana poprzez pracę kilku agencji. Do konkretnych akcji poszerzających wiedzę należą strony internetowe Krajowej Agencji ds. Poczty i Telekomunikacji, poświęcone bezpieczeństwu w Internecie, oraz utworzenie Szwedzkiego Centrum Obsługi Incydentów (Sitic) zespołu CERT. Więcej informacji można znaleźć pod adresem:

Krajowa Agencja ds. Poczty i Telekomunikacji (Post- och telestyrelsen, PTS)

<http://www.pts.se/Default.asp?Sectionid=&Itemid=&Languageid=EN>

Swedish IT Incident Centre (Sitic) – Szwedzkie Centrum Obsługi Incydentów IT

<http://www.sitic.se/eng/index.html>

Należy również zwrócić uwagę na fakt, że poszerzanie wiedzy często stanowi naturalną część planu prac w agencji bądź przedsiębiorstwie i byłoby realizowane niezależnie od istnienia krajowej strategii. Przykładami są urzędy ochrony konsumenta, agencje sektorowe (łączność elektroniczna, usługi finansowe itp.) oraz organy ochrony porządku publicznego.

Na przykład szwedzki Urząd Ochrony Konkurencji i Konsumentów zapewnia informacje na temat bezpiecznego e-handlu, oferuje narzędzia chroniące użytkowników IT przed nowoczesnymi atakami typu hijacking, polegającymi na przejęciu kontroli (co przez pewien czas stanowiło bardzo poważny problem) i umożliwia pomiar rzeczywistej przepustowości łącza zapewnianego przez dostawcę usług internetowych. Więcej informacji można znaleźć pod adresem:

Szwedzki Urząd Ochrony Konkurencji i Konsumentów

<http://www.konsumentverket.se/mallar/en/startsidan.asp?IngCategoryId=646> (w języku angielskim)

<http://www.konsumentverket.se> (w języku szwedzkim)

Szwedzki Urząd Ochrony Konkurencji i Konsumentów: bezpieczny e-handel

<http://www.konsumentverket.se/mallar/en/startsidan.asp?IngCategoryId=646>

Szwedzki Urząd Ochrony Konkurencji i Konsumentów: IT i Internet

http://www.konsumentverket.se/mallar/en/lista_artiklar.asp?IngCategoryId=922 (w języku angielskim)

<http://www.internetit.konsumentverket.se> (w języku szwedzkim)

Prawne, regulacyjne i instytucjonalne ustalenia w celu poszerzania wiedzy

W szwedzkich ramach prawnych wyznacza się różne zadania organom rządowym takim jak szwedzka Krajowa Agencja ds. Poczty i Telekomunikacji, szwedzka Rada Kontroli Danych i szwedzki Urząd Ochrony Konkurencji i Konsumentów. Organy te posługują się ustawami takimi jak Ustawa o łączności elektronicznej i Ustawa o danych osobowych.

Inne agencje, np. SEMA (zob. poniżej) także mają obowiązki.

Rada Kontroli Danych

Artykuły 31-32 Ustawy o danych osobowych poświęcone są bezpiecznej ochronie prywatności. Rada Kontroli Danych wydała wytyczne dotyczące bezpieczeństwa, udziela ona także porad i organizuje seminaria dla administratorów danych i dla społeczeństwa. Aby poszerzyć wiedzę administrator danych może wykorzystać wytyczne jako ogólny opis działań zapewniających bezpieczeństwo.

Ustawa o ochronie danych definiuje pojęcie przedstawiciela ds. danych osobowych w sposób następujący: „Osoba fizyczna, wyznaczona przez administratora danych osobowych, która niezależnie gwarantuje, że dane osobowe przetwarzane są w sposób prawidłowy i zgodny z prawem. W kontekście ochrony prywatności podczas przetwarzania danych osobowych przedstawiciel ds. danych osobowych stanowi zasób źródłowy dla administratora danych.

Rada Kontroli Danych pomaga przedstawicielowi ds. ochrony danych poprzez rady i seminaria dotyczące bezpieczeństwa. Do 28 kwietnia 2006 r. administratorzy danych mianowali i zgłosili 3467 przedstawicieli ds. ochrony danych, a 80% lokalnych władz

samorządowych w Szwecji zgłosiło przedstawiciele ds. ochrony danych do Rady Kontroli Danych. Przedstawiciele ds. ochrony danych są funkcjonariuszami Rady Kontroli Danych.

Władze państwowe jako użytkownik systemów informacyjnych

Najnowsze programy i inicjatywy poszerzania wiedzy

Na temat skuteczności różnych inicjatyw ze strony agencji bądź rządu istnieje mało informacji. Poniższe informacje nie powinny być traktowane jako wyczerpujący wykaz wszystkich najskuteczniejszych działań. Zasadnicza odpowiedzialność za bezpieczne korzystanie z technologii informacyjnych spoczywa na każdej agencji.

Szwedzka Agencja Rozwoju Administracyjnego

Szwedzka Agencja Rozwoju Administracyjnego (Verva) jest ekspertem w dziedzinie rozwoju administracji publicznej. Agencja promuje i wspiera rozwój administracji publicznej, a także poprawia koordynację w administracji rządowej, w tym w zakresie nabywania i stosowania IT. Więcej informacji można znaleźć pod adresem:

http://www.verva.se/web/t/Page____492.aspx

Krajowa Agencja ds. Poczty i Telekomunikacji

O działaniach informacyjnych Krajowej Agencji ds. Poczty i Telekomunikacji, jak również agencji Sitic wspomniano we wcześniejszej części tego dokumentu.

Szwedzka Agencja Zarządzania Kryzysowego (SEMA)

Szwedzka Agencja Zarządzania Kryzysowego (SEMA) dwa razy w roku organizuje wspólnie z innymi agencjami seminaria mające na celu polepszenie bezpieczeństwa informacji w społeczeństwie i poszerzenie wiedzy kadry kierowniczej w szwedzkich agencjach. Agencja wydaje także miesięczny biuletyn, zrealizowała ponadto film na DVD z najważniejszymi osobami z kierownictwa publicznego i prywatnego, mający na celu poszerzenie wiedzy na wyższych szczeblach organizacji. SEMA opracowuje interaktywny produkt do e-learningu mający na celu poszerzenie wiedzy w dziedzinie bezpieczeństwa informacji, a także organizuje kursy z tej dziedziny.

Ponadto SEMA wydaje zalecenia dotyczące poziomu bezpieczeństwa stanowiącego punkt odniesienia. Określony poziom stanowi najniższy poziom bezpieczeństwa systemów IT konieczny dla podstawowych usług społecznych. Zalecenia mogą być stosowane w przypadku organów publicznych i prywatnych. Więcej informacji można znaleźć pod adresem:

http://www.krisberedskapsmyndigheten.se/EPiBrowser/Publikationer/KBMs%20publikationer/Rekommenderar/bits_eng_recomm_2003-2.pdf

W celu wdrożenia bezpieczeństwa stanowiącego punkt odniesienia SEMA opracowała poradnik z zakresu bezpieczeństwa IT, służący jako narzędzie analizy bezpieczeństwa w systemach IT. Ponadto SEMA przeprowadza roczną krajową ocenę ryzyka. Więcej informacji można znaleźć pod adresem:

<http://www.krisberedskapsmyndigheten.se/6193.epibrw>

Władze lokalne jako użytkownik systemów informacyjnych

Najnowsze programy i inicjatywy poszerzania wiedzy

Zbadanie poszczególnych władz lokalnych, których jest ok. 290, nie było możliwe. Poniżej ujęto niektóre zebrane szczegółowe informacje.

Szwedzkie Stowarzyszenie Władz Lokalnych i Regionalnych

Szwedzkie Stowarzyszenie Władz Lokalnych i Federacja Szwedzkich Rad Powiatowych reprezentują rządowe, zawodowe i dotyczące pracodawców interesy 290 szwedzkich władz lokalnych, 18 rad powiatowych i dwóch regionów. Więcej informacji znajduje się pod adresem: <http://kikaren.skl.se/artikel.asp?C=756&A=180>.

Celem stowarzyszenia i federacji jest promowanie i wzmacnianie samorządów lokalnych i tworzenia jak najlepszych warunków pracy dla ich członków. Działania w dużym stopniu finansowane są ze składek członkowskich.

Stowarzyszenie opublikowało informacje na temat polityki bezpieczeństwa informacji dostosowanej do władz lokalnych i regionalnych. Kwestie bezpieczeństwa są omawiane na konferencjach; możliwe jest także zwrócenie uwagi na najlepsze praktyki władz lokalnych. Na stronie internetowej publikowane są takie informacje jak porady dotyczące nowych i istotnych aktów prawnych.

Inicjatywa filmowa miasta Sztokholm

Obywatele muszą mieć pewność co do sposobu przetwarzania informacji osobowych na ich temat i sposobu oferowania usług. Polegają oni na fakcie, że osoby zatrudnione przez miasto Sztokholm są dobrze wyszkolone i świadome znaczenia bezpieczeństwa podczas świadczenia usług.

Miasto Sztokholm zrealizowało film oparty na nowych wytycznych i strategii w zakresie bezpieczeństwa informacji (ustalonych jesienią 2005 r.). Ma on na celu uświadomienie użytkownikom końcowym czym jest bezpieczeństwo informacji z ich własnej perspektywy. Film zawiera wywiady z pracownikami i partnerami miasta Sztokholm; każdy wywiad oparty jest na temacie dotyczącym nowych wytycznych i strategii.

Tematy różnych wytycznych przedstawione w filmie obejmują takie obszary jak administracja, odpowiedzialność i metody, a także bardziej techniczne zagadnienia.

Jeden z uwzględnionych tematów dotyczył systemu opieki społecznej, który jest jednym z najważniejszych systemów miasta Sztokholm. Niektórzy pracownicy opisują obowiązki wynikające z ich funkcji, są to między innymi: właściciel systemu, administrator systemu i lokalny urzędnik odpowiedzialny za dane kwestie.

Bezpieczeństwo fizyczne lub ochrona brzegowa (ang. *perimeter security*) to kolejne zagadnienia opisane w filmie; dotyczy on także aspektów mobilności takich jak praca z palmtopami i zagrożeń podczas korzystania z połączeń bezprzewodowych.

Przedstawiona jest także analiza ryzyka dla jednej z dzielnic miasta. W tym rozdziale podkreślono znaczenie bezpieczeństwa i konieczność wspierania działań przez ścisłe kierownictwo.

Rząd jako partner przedsiębiorstw i przemysłu **Małe i średnie przedsiębiorstwa (MŚP)**

Państwowy Urząd Pocztowy i Telekomunikacyjny

Państwowy Urząd Pocztowy i Telekomunikacyjny jest hostem stron internetowych zawierających informacje na temat bezpieczeństwa w Internecie. Strony internetowe są zazwyczaj skierowane do gospodarstw domowych i sektora publicznego/prywatnego (zwłaszcza mniejszych firm lub urzędów, które dysponują ograniczonymi zasobami, jeśli chodzi o bezpieczeństwo informacji). Treść tych stron obejmuje również interaktywne testy dla konkretnego komputera (przeprowadzane w Internecie) oraz interaktywne programy edukacyjne dotyczące haseł dostępu.

Szwedzkie Centrum ds. Incydentów IT (Sitic) w 2005 przeprowadziło ankietę „Niezgłaszane incydenty związane z bezpieczeństwem – ukryte statystyki dotyczące incydentów związanych z bezpieczeństwem w Szwecji”. Celem tego studium było zgromadzenie aktualnych informacji o tym, jak często w szwedzkich organizacjach mają miejsce typowe incydenty w zakresie bezpieczeństwa IT, w jakim stopniu takie incydenty zgłaszane są wewnątrz organizacji - do działów ds. bezpieczeństwa, a w jakim stopniu zgłaszane są na zewnątrz – na policji i w Sitic; oraz uzyskanie informacji dotyczących powodów, dla których pewne osoby gotowe są zgłaszać takie incydenty na policji i w Sitic.

W ramach studium wysunięto hipotezę, że niezgłaszanie incydentów można zaobserwować w czterech dziedzinach: zlecenie usług na zewnątrz, zgłaszanie incydentów wewnątrz organizacji, zgłaszanie incydentów na zewnątrz organizacji i rzeczywiste zgłaszanie incydentów.

Studium to zostało przeprowadzone w ramach współpracy Sitic z Państwowym Departamentem ds. Śledztw w Sprawach Karnych. Temo – firma badająca rynek – prowadziła prace w terenie. Ankieta oparta jest na losowo wybranej próbie o strukturze warstwowej, obejmującej firmy i organizacje zatrudniające co najmniej 50 pracowników.

Aby uzyskać więcej informacji, zobacz

<http://www.pts.se/Nyheter/pressmeddelande.asp?ItemId=4718>

Zobacz część [Rząd jako partner \(Społeczeństwa\)](#), aby uzyskać więcej informacji na temat inicjatyw podejmowanych przez Państwowy Urząd Pocztowy i Telekomunikacyjny.

Dostawcy usług internetowych (ISP)

Nie ma obecnie dostępnych informacji w odpowiednim formacie. Wielu operatorów zamieszcza informacje dotyczące bezpieczeństwa na swoich stronach internetowych.

Media

Należy zauważyć, że w poniższym przykładzie wykorzystano media jako kanał dotarcia do innych grup docelowych i nie przedstawiono ich jako odrębną grupę docelową.

Prawdopodobnie media stanowiłyby część wielu strategii w tej dziedzinie, jednak niekoniecznie byłyby celem same w sobie. W ostatnich latach media donosiły o problemach związanych z bezpieczeństwem informacji, takich jak wirusy komputerowe, phishing itd. Biorąc pod uwagę dużą liczbę komputerów w gospodarstwach domowych, szwedzkie media są prawdopodobnie zainteresowane relacjonowaniem pewnych wydarzeń poprzez zasięganie informacji w urzędach i u ekspertów z sektora prywatnego.

Zobacz część [Rząd jako partner \(Społeczeństwa\)](#), aby uzyskać więcej informacji na temat inicjatyw podejmowanych przez Państwowy Urząd Pocztowy i Telekomunikacyjny.

Partnerstwo publiczno-prywatne

ISO/IEC 17799:2005

Szwedzki Instytut Normalizacyjny opublikował ISO/IEC 17799:2005 w październiku 2005 roku. Poruszono w nim następujące tematy: technologia informacyjna, techniki bezpieczeństwa i kodeks postępowania dotyczący zarządzania bezpieczeństwem informacji.

Rada ds. Kontroli Danych zachęca organy publiczne, sektor opieki zdrowotnej, organizacje przemysłowe i normalizacyjne do opracowania i stosowania kontroli prywatności i zapewnienia koniecznej poufności i bezpieczeństwa.

ISO/IEC 17799:2005 Część 15 „Przestrzeganie wymogów prawnych” zawiera informacje na temat ochrony danych i prywatności danych osobowych, o których mowa w części

15.1.4. Normę tę wykorzystywano również jako wzór do przeprowadzania audytów wewnętrznej działalności agencji rządowych w związku z bezpieczeństwem informacji.

Carelink – Krajowa inicjatywa mająca na celu opracowanie zastosowania IT w szwedzkiej służbie zdrowia

Carelink współpracuje ze wspomagającymi usługami takimi jak SJUNET (krajowa sieć komunikacji szerokopasmowej), usługi katalogowania i bezpieczeństwo informacji. Do ważnych zadań należy przekazywanie informacji i rozpowszechnianie najlepszych praktyk i dobrych przykładów. Carelink jest koordynującym partnerem krajowych projektów i sieci, dotyczących większości zagadnień rozwoju IT w opiece zdrowotnej. Aby uzyskać więcej informacji, zobacz: <http://www.carelink.se/pages/newsbill.asp?VersionID=1&Pages=1,124>

Rząd jako partner społeczeństwa

Najnowsze programy i inicjatywy poszerzania wiedzy

Państwowy Urząd Pocztowy i Telekomunikacyjny

Według rocznej krajowej ankiety Państwowego Urzędu Poczowego i Telekomunikacyjnego („Individundersökningen”) 78% szwedzkich gospodarstw domowych ma dostęp do Internetu. Ostatnią ankietę przeprowadzono we wrześniu i październiku 2005 roku, rozsyłając drogą pocztową kwestionariusz do 4000 losowo wybranych Szwedów w wieku od 16 do 75 lat. Ankietę wdrożono w 2002 roku.

W okresie od grudnia 2002 roku do sierpnia 2005 roku rząd wyznaczył Państwowy Urząd Pocztowy i Telekomunikacyjny do skompilowania informacji o bezpieczeństwie w Internecie i udostępnienia ich w Internecie.

Strategia polegała na tym, by jednym głównym kanałem dostarczyć grupom docelowym łatwo dostępne informacje dostosowane do poszczególnych grup. Cel był również taki, aby dostarczyć informacje jednym dodatkowym kanałem i rozpowszechnić informacje poprzez wybrane organizacje, aby zwiększyć zasięg i opłacalność.

W późniejszej fazie zadania przeznaczono również środki na rozpowszechnienie informacji poprzez kampanie z wykorzystaniem banerów reklamowych w celu zapewnienia jak największego zasięgu.

Grupami docelowymi byli:

- Użytkownicy prywatni
- MŚP
- Małe i średnie organy rządowe

Ogólnym celem było zwiększenie świadomości i wiedzy grup docelowych w zakresie bezpieczeństwa w Internecie, aby korzystały one z Internetu w sposób bardziej bezpieczny i nie narażały siebie lub innych na niepotrzebne zagrożenia.

W listopadzie 2003 roku Państwowy Urząd Pocztowy i Telekomunikacyjny uruchomił stronę internetową poświęconą bezpieczeństwu (www.pts.se/internetsakerhet) i zorganizował interaktywny kurs, na którym zapewniono drukowane pomoce. Drukowane materiały obejmowały fiszki informacyjne (z podstawkami), broszury z przydatnymi wskazówkami i specjalne wydania urzędowego czasopisma. Nową wersję strony internetowej zawierającą interaktywną pomoc sieciową i nową usługę sieciową dla konsumentów wykorzystywaną do sprawdzania bezpieczeństwa komputerów osobistych uruchomiono w połowie kwietnia 2005 roku.

Materiały drukowane rozprowadzono wśród lokalnych doradców konsumenckich, bibliotek, szkół i uczelni, różnych organizacji handlowych, ISP, banków i władz samorządowych. Media również uzyskały informacje o bezpieczeństwie w Internecie dzięki relacjom prasowym i bezpośrednim kontaktom z dziennikarzami.

Zagadnienia na stronie internetowej były skierowane do dwóch kategorii użytkowników: użytkownika prywatnego (För hemmet) i zakładów pracy (För arbetsplatsen).

Użytkownicy prywatni mogą znaleźć na stronie informacje dotyczące następujących zagadnień: Internet, połączenie, surfowanie, e-mail, ściąganie plików, współdzielenie plików, chat, gry sieciowe, załatwianie spraw bankowych, e-zakupy, piętnaście przydatnych wskazówek, interaktywna nauka, popularne pytania, popularne terminy i inne odsyłacze.

Dla zakładów pracy przeznaczone są następujące informacje: przygotowanie strategii, zasady dotyczące infrastruktury, połączenie z Internetem, konfigurowanie systemów, tworzenie kopii bezpieczeństwa, połączenie na odległość, połączenie z partnerami biznesowymi, ochrona przed szkodliwymi kodami, radzenie sobie z incydentami związanymi z IT, e-identyfikacja i transakcje, kupowanie systemów bezpieczeństwa, przydatne wskazówki dla zakładu pracy i inne odsyłacze.

Osiągnięcia związane tymi działaniami były następujące (końcowe sprawozdanie opisujące cały projekt jest dostępne po szwedzku, ze streszczeniem po angielsku):

- Przeprowadzono ponad 180 000 testów poprzez sieciową usługę kontroli bezpieczeństwa komputerowego. Zobacz www.testadatorn.se i <http://www.pts.se/Nyheter/pressmeddelande.asp?Itemid=5201>
- Odnotowano ponad 250 odwiedzin na stronie
- Interaktywny kurs na stronie odwiedzono 30 000 razy
- W czerwcu 2005 roku największe szwedzkie czasopismo poświęcone komputerom osobistym (PC för alla) przyznało tej stronie tytuł „Strony miesiąca”

- Wirtualni asystenci strony odpowiedzieli na ponad 25 000 pytań
- Ukazało się ponad 150 wycinków prasowych
- Rozdano 100 000 fiszek informacyjnych z podstawkami
- Rozdano 60 000 broszur „Surfuj bezpiecznie”
- Rozdano 10 000 czasopism „Połącz się”
- Szwedzki Urząd ds. Konsumentów i Państwowy Urząd Pocztowy i Telekomunikacyjny wraz z kilkoma operatorami podjęły wspólną inicjatywę informacyjną związaną z przechwytywaniem modemów
- W 2005 roku Państwowy Urząd Pocztowy i Telekomunikacyjny wraz z 14 innymi organizacjami uczestniczył w SurfaLugnt – krajowej kampanii dotyczącej bezpieczeństwa w Internecie

Państwowy Urząd Pocztowy i Telekomunikacyjny postanowił włączyć kampanię poszerzania wiedzy w swoją codzienną pracę po zakończeniu projektu rządowego. Wiele strategii, grup docelowych i wiadomości jest podobnych i dlatego mogą być ponownie wykorzystane.

W listopadzie 2005 roku Państwowy Urząd Pocztowy i Telekomunikacyjny uruchomił tester haseł dostępu (www.testalosenord.se). Test ten uczy, jak tworzyć hasła dostępu, aby były trudne do przełamania. Oczekuje się, że grupy docelowe wykorzystają tę wiedzę przy tworzeniu haseł dostępu w domu lub w pracy. Na stronie internetowej umieszczona jest informacja, że test ten nie powinien być wykorzystywany do testowania haseł dostępu będących w użyciu lub do tworzenia nowych haseł. Powinien być stosowany wyłącznie do testowania różnych kombinacji znaków w celu sprawdzenia, czy byłyby one mocne czy słabe, gdyby użyto ich jako haseł dostępu.

Państwowy Urząd Pocztowy i Telekomunikacyjny przeprowadził również kampanię z wykorzystaniem banerów reklamowych, aby rozpowszechnić usługi dostępne na stronie poświęconej bezpieczeństwu w Internecie - kontrolę bezpieczeństwa komputera i tester hasła dostępu. Kampania ta trwała sześć tygodni na przełomie października i listopada 2005 roku. Wskaźnik CTR (click-thru-rate: stosunek liczby odwiedzin reklamy do liczby jej wyświetleń) wynosił 0.15 %, co – według doradców medialnych – jest bardzo dobrym wynikiem. Zarejestrowano 84 000 odwiedzających związanych z kampanią.

Obydwa testy okazały się sukcesem. Na początku kwietnia 2006 roku przeprowadzono ponad 250 000 testów haseł dostępu. Z kolei w ramach kontroli bezpieczeństwa komputera przeprowadzono ponad 410 000 testów. Stronę poświęconą bezpieczeństwu w Internecie odwiedziło ponad 600 000 osób.

Oprócz programu opisanego powyżej Państwowy Urząd Pocztowy i Telekomunikacyjny sporządził również dwa raporty dotyczące zagrożeń związanych z bezpieczeństwem telefonii komórkowej i spyware:

Raport: Zagrożenia związane z bezpieczeństwem telefonii komórkowej (PTS-ER-2006:18)

W raporcie tym opisano zagrożenia dla bezpieczeństwa telefonii komórkowej z perspektywy użytkownika i zawarto ocenę sytuacji w zimie 2005/2006 roku. Raport ten oparty jest na rozmowach z operatorami, producentami telefonów komórkowych, producentami systemów zabezpieczających i innymi ekspertami w tej dziedzinie, oraz na warsztatach, w czasie których wyżej wspomniani doradcy zgromadzili się, aby wspólnie ocenić różne możliwe zagrożenia związane z bezpieczeństwem, na jakie narażeni są użytkownicy telefonii komórkowej. Raport ten skupił się na technologiach GSM i UMTS.

Obecnie ryzyko zagrożeń dla bezpieczeństwa telefonii komórkowej uważane jest za niskie. Według operatorów telefonii komórkowej odkryto tylko kilka przypadków telefonów komórkowych zainfekowanych szkodliwymi kodami. Jednak można rozróżnić pewne ogólne trendy, które w przyszłości mogą prowadzić do rosnących zagrożeń dla bezpieczeństwa telefonii komórkowej i użytkowników telefonii komórkowej. W przyszłości telefony komórkowe będą coraz bardziej przypominały komputery osobiste. Będą zawierały cenne informacje; zwiększy się zakres ich działania; telefon komórkowy będzie miał interfejs związany z kilkoma różnymi rodzajami sieci komunikacyjnych i będzie stale podłączony do sieci danych. Ponadto więcej telefonów będzie wyposażonych w otwarty interfejs programistyczny, dzięki czemu niezależni programiści będą mogli tworzyć nowe aplikacje dla tych telefonów. Na skutek tych tendencji telefony komórkowe stają się coraz bardziej zagrożone. Szkodliwe kody staną się głównym zagrożeniem dla bezpieczeństwa zwłaszcza wtedy, gdy inteligentne telefony, wykorzystujące otwarte systemy operacyjne, staną się bardziej powszechne. W tej sytuacji ważne jest, aby:

- wzrósł udział inteligentnych telefonów (około 10% w 2007 roku)
- wzrosła prędkość transmisji pomiędzy telefonami komórkowymi a sieciami danych
- więcej telefonów komórkowych było na stałe połączonych z usługami transmisji danych (GPRS, UMTS, WLAN, itd.)
- coraz więcej usług komunikacyjnych dostarczano za stałą opłatą

Państwowy Urząd Pocztowy i Telekomunikacyjny oczekuje, że uczestnicy rynku będą współpracować w celu zminimalizowania zagrożeń związanych z bezpieczeństwem i wykorzystania doświadczenia i wiedzy w zakresie problemów z bezpieczeństwem w Internecie po to, by uniknąć – w takim stopniu, w jakim to możliwe – powtarzających się problemów, które mają niekorzystny wpływ na telefony komórkowe. Ponadto głównym środkiem, który może zminimalizować ryzyko przyszłych zagrożeń dla bezpieczeństwa telefonii komórkowej jest poszerzanie wiedzy użytkowników w zakresie tych zagrożeń i sposobów ochrony przed tymi zagrożeniami.

Raport: Spyware i zjawiska ściśle związane z nim (PTS-ER-2005:15)

Wraz z przekształcaniem się społeczeństwa w społeczeństwo informacyjne, w którym znaczne obszary działalności przedsiębiorstw i rządu są w różnym stopniu zależne od komputerów i sieci komunikacyjnych, obserwuje się zjawisko coraz większej zależności od działania i bezpieczeństwa tych komputerów. Przez wiele lat wirusy i inne szkodliwe kody stanowiły poważne zagrożenie dla takich funkcji. Jednakże istnieją również programy i systemy techniczne, które w inny sposób - niż poprzez zwykłe zniszczenie - mogą stanowić zagrożenie zarówno dla funkcjonalności sieci komunikacyjnych jak i zaufania, jakie mają do nich użytkownicy. Raport ten jest poświęcony grupie takich programów, które w różny sposób (począwszy od bardziej szkodliwego przechowywania opcji menu w plikach cookie, a skończywszy na rzeczywistym przechwyceniu całych sieci komputerów) mogą stanowić zagrożenie, naruszając prywatność użytkowników. Programy i ich funkcje mogą w pojedynczych przypadkach powodować poważne naruszenie prywatności indywidualnego użytkownika, ale mogą również w szerszej perspektywie stanowić zagrożenie dla zaufania i gotowości społeczeństwa do korzystania z elektronicznych usług komunikacyjnych. Kolejnym problemem jest to, że niektóre z tych programów ułatwiają złośliwym stronom tworzenie - za pośrednictwem zdalnie sterowanych komputerów - platform przeznaczonych do następnych ataków, których użytkownik jest zupełnie nieświadomy.

Część dotycząca spyware jest ogólnie skierowana do każdego, kto chce poznać te zjawiska i kto, na poziomie mniej zaawansowanym technicznie, chce posiąść ogólną wiedzę o ich występowaniu, potencjalnych zagrożeniach i możliwościach ochrony się przed nimi. Część dotycząca kwestii prawnych jest głównie skierowana do prawników i innych osób zainteresowanych tymi kwestiami, które – przede wszystkim na podstawie Ustawy o Komunikacji Elektronicznej (EkomL) – wynikają w związku z pojawieniem się spyware.

Partnerstwo publiczno-prywatne

Krajowa kampania SurfaLugnt promująca bezpieczniejszy Internet jest jednym z najbardziej udanych partnerstw pomiędzy przemysłem IT i właściwymi organami. Aby uzyskać więcej informacji, zobacz: <http://www.surfalugnt.se>

W partnerstwie tym położono nacisk na kompetencje i dostęp do kanałów. Jako sojusz postrzegane jest ono jako bardziej wiarygodne oraz ma większą możliwość przyciągnięcia uwagi grup docelowych i mediów. W 2006 roku strategia partnerstwa zmieni się z „dlaczego” na „jak” i kampania bardziej skoncentruje się na młodych ludziach.

Uzgodniono ze stronami zainteresowanymi projekt planu na okres od kwietnia 2005 roku do grudnia 2005 roku i w ramach projektu kontraktu stworzono Kodeks Postępowania. Przedstawiono również projekt wytycznych.

Zgodnie z pierwotnym planem kampania miała objąć 100 miast – rok później liczba miast wzrosła do 200. Również początkowa liczba planowanych działań wzrosła z 1500 do 2000. Liczba około 2000 osób kontaktowych jest dwa razy większa od tej, którą przewidywano na wstępie. Stronę skierowaną do 1,5 miliona docelowych odbiorców odwiedziło 300 000 osób.

W inicjatywę tę zaangażowani są następujący partnerzy: Państwowy Urząd Pocztowy i Telekomunikacyjny, Szwedzki Urząd Zarządzania Nagłymi Wypadkami, Delegacja Urzędowa 24/7, Stowarzyszenie Bankierów Szwedzkich, Szwedzka Konfederacja Przedsiębiorstw, Fundacja na rzecz Infrastruktury Internetowej, Szwedzkie Stowarzyszenie Przemysłu IT i Telekomunikacyjnego, F-Secure, Microsoft, TeliaSonera i Symantec. Rada Kontroli Danych i IBM uczestniczyły jako pomniejsi partnerzy finansowi.

Aby uzyskać więcej informacji, zobacz [ppp_for_a_safer_internet.pdf](#).

Statystyki i kluczowe wskaźniki wydajności (KPI)

Statystyki/KPI do oceny skuteczności inicjatywy poszerzania wiedzy

Państwowy Urząd Pocztowy i Telekomunikacyjny

Państwowy Urząd Pocztowy i Telekomunikacyjny wykorzystał swoją roczną krajową ankietę ("Individundersökningen") w różnych późniejszych kampaniach. Ankieta ta nie była zaprojektowana specjalnie z myślą o ocenie projektów poszerzania wiedzy, a mimo to okazała się przydatna w tym zakresie. Ostatnią ankietę przeprowadzono we wrześniu i październiku 2005 roku przy pomocy kwestionariusza wysłanego pocztą do 4000 przypadkowo wybranych Szwedów w przedziale wiekowym od 16 do 75 lat. Ankietę tę wdrożono w 2002 roku.

Ankieta ma na celu – między innymi - zmierzenie zastosowania zapór sieciowych i oprogramowania antywirusowego (z funkcją aktualizacji) w szwedzkich gospodarstwach domowych, w których zainstalowane jest łącze internetowe. Państwowy Urząd Pocztowy i Telekomunikacyjny uruchomił stronę internetową poświęconą bezpieczeństwu w Internecie w listopadzie 2003 roku. Jedną z informacji umieszczonych na stronie mówiła, że użytkownicy Internetu powinni korzystać zarówno z zapory sieciowej jak i oprogramowania antywirusowego oraz aktualizować je.

W grudniu 2003 roku ankieta wykazała, że 34% użytkowników stosowało zaporę sieciową; liczba ta wzrosła do 47% w 2004 roku i do 64% w 2005 roku. Jeśli chodzi o oprogramowanie antywirusowe z funkcją aktualizacji, analogiczne liczby wynoszą odpowiednio 66, 78 i 80%.

Kampania poszerzania wiedzy Surfa Lugnt

W ramach SurfaLugnt dokonano pomiaru stanu wiedzy i nastawienia docelowych MŚP i użytkowników prywatnych. Kryteria ilościowe obejmowały liczbę podjętych działań, liczbę odwiedzonych miejsc i liczbę zaangażowanych osób.

Z perspektywy rządu najważniejszą rzeczą jest znalezienie sposobu pomiaru efektów różnych inicjatyw poszerzania wiedzy. Następnie można by wykorzystać takie statystyki do pomiaru wartości inicjatyw i środków przeznaczonych na te inicjatywy oraz na ulepszanie ich.

Zdobyte doświadczenia

ENISA ułatwiła zorganizowanie posiedzeń poświęconych zdobytym doświadczeniom z przedstawicielami Państwowego Urzędu Pocztowego i Telekomunikacyjnego oraz Szwedzkim Stowarzyszeniem Przemysłu IT i Telekomunikacyjnego.

Strona internetowa Państwowego Urzędu Pocztowego i Telekomunikacyjnego

Wyzwania dla projektu

- Szeroki zakres projektu (tj. liczba grup docelowych)
- Stosowanie różnych języków w kontaktach z różnymi grupami docelowymi

Sukcesy

- Współpraca z SITIC (CERT) przy opracowywaniu materiału technicznego
- Wiedza członków SITIC do dyspozycji
- Konsultacje z ekspertami przed uruchomieniem strony internetowej
- Różne punkty wejścia na stronę internetową
- Dużo dostępnych treści
- Wykorzystanie Internetu jako kanału
- Rozpoczęcie działań na krótko przed datą uruchomienia strony internetowej
- Zespół projektowy (5/10 osób)
- Analiza grupy docelowej przed rozpoczęciem kampanii - przeprowadzono ją przy pomocy wywiadów, a nie ankiety. Przeprowadzono rozmowy z różnymi osobami w celu zgromadzenia informacji o ich potrzebach/wiedzy. W działanie to zaangażowana była firma zewnętrzna (podejście marketingowe).
- Zaangażowanie mediów – w pierwszym etapie projektu wykorzystano komunikaty prasowe i bannery reklamowe. Bannery przeznaczone były głównie dla mniejszych firm i konsumentów do umieszczenia na ich stronach internetowych – media nie były zaangażowane
- W drugim etapie dzięki większemu budżetowi rozpoczęto kampanię w sieci, umożliwiając wykorzystanie płatnych reklam itd.
- Pomiar poziomu kliknięć i surfowania po sieci
- Rozprowadzenie materiałów drukowanych (tj. broszur) w szkołach, bibliotekach itd.

Porażki

- Zespół nie był w pełni zaangażowany w projekt (jeśli chodzi o czas)
- Brak kompetencji – trudności pracowników biura informacyjnego ze zrozumieniem/aktualizowaniem informacji dotyczących MŚP. Aktualizowanie treści dla użytkowników prywatnych było łatwiejsze.
- SITIC nie zawsze był dostępny (jeśli chodzi o pracę nad projektem)
- Ocena poziomu wiedzy przed rozpoczęciem kampanii. Nie przeprowadzono jej z powodu braku środków oraz dlatego że uznano, iż wstępna analiza była wystarczająca, aby zobrazować sytuację
- Brak określenia kategorii w obrębie grup docelowych (np. młodzież)
- Dotarcie do młodzieży – używa ona odmiennego języka, ma odmiennie potrzeby
- Utrzymanie narzędzi opracowanych przez różne źródła: „Kontrola bezpieczeństwa” (zaporą sieciową) jest oparta na oprogramowaniu o otwartym kodzie źródłowym, zwanym Nessus; „Tester hasła dostępu” jest częściowo oparty na oprogramowaniu zwanym CrackLib
- Zaawansowane narzędzia niedostępne dla użytkowników

Wskazówki pod kątem przyszłych kampanii

- Należy jasno określić wartość środków przeznaczonych na projekt
- Należy ocenić poziom wiedzy przed rozpoczęciem kampanii
- Konieczne jest ograniczenie zakresu i liczby grup docelowych
- Należy skoncentrować się na konsumentach i większych zagrożeniach
- Należy skierować działania do ludzi młodych
- Potrzebne jest większe zaangażowanie mediów
- Konieczne jest opracowanie narzędzia, które będzie wykorzystywane przez użytkowników, lub zaoferowanie czegoś użytkownikowi (np. narzędzia do testowania laptopów). Najlepiej nie używać oprogramowania, które można ściągnąć z Internetu, gdyż wymaga ono dodatkowej konserwacji
- Potrzebna jest dynamiczna strona internetowa
- Bardziej szczegółowe określenie grup docelowych – kanały, poprzez które dociera się do starszych użytkowników Internetu są zazwyczaj inne
- Należy zaangażować ISP
- Potrzebne są dostępne środki na aktualizowanie materiałów
- Należy mieć plan działań podejmowanych po rozpoczęciu kampanii. Konieczne jest określenie ról i obowiązków w zakresie zarządzania kampanią i dostosowania jej, o ile istnieje taka potrzeba

SurfaLugnt (rok 2005 i początek roku 2006)

Sukcesy

- Wyznaczenie kierownika projektu (PM) – PM dostarcza pomysły, jest gotowy do działania i zajmuje się wieloma pojawiającymi się problemami. PM dowodzi kampanią dużo bardziej skutecznie
- Rada kierownicza spisała się dobrze pomimo wielu różnych zaangażowanych partnerów
- Kompetencje zaangażowanych stron: zaangażowano 12/15 partnerów. Każda z organizacji miała odpowiednie kompetencje, które mogła wykorzystać na cele kampanii
- Wykorzystanie istniejących materiałów – często istnieją dobre porady, testy i inne praktyczne informacje, które można i należy wykorzystać
- Rozpowszechnienie na poziomie lokalnym/regionalnym – jeśli naprawdę chce się zmienić postępowanie użytkowników przy pomocy ograniczonej ilości środków, kluczowym rozwiązaniem jest znalezienie lokalnych partnerów (również osób mających wpływ na opinię publiczną/ambasadorów) oraz zaangażowanie lokalnych sieci z myślą o grupach docelowych
- Strona internetowa przygotowana przez lokalne/regionalne obszary – strona taka jest bardzo ważnym narzędziem do przekazywania informacji o pomysłach, wydarzeniach, narzędziach itd. Jeśli użytkownik może dowiedzieć się, co się dzieje na jego obszarze, może być mu łatwiej zdecydować się na włączenie w jakieś reklamowane działanie/wydarzenie/dyskusję
- Nie opracowano nadmiernej ilości treści
- Użytkownikom zapewniono zrozumiałe, praktyczne porady. Grupy docelowe doceniły wyczerpujące informacje
- Najpierw stworzono stronę internetową, a następnie publicznie –prywatne partnerstwo
- Określono role i obowiązki
- Strona internetowa jako kanał – opłacalne narzędzie do pracy nad kampanią na poziomie krajowym przy ograniczonych środkach i bardzo dużych grupach docelowych

Porażki

- PM nie pracował w pełnym wymiarze godzin
- Zainteresowanie mediów było niewystarczające – jest ono bardzo ważne dla zainteresowanych stron kampanii
- Liczba ISP zaangażowanych w projekt nie była zgodna z oczekiwaniami
- Niewystarczająca liczba partnerów i ekspertów – na przykład, pojawiło się bardzo dużo pytań w związku z dokonywaniem płatności przez Internet, lecz zespół nie był w stanie odpowiedzieć na nie, gdyż nie posiadał odpowiedniej wiedzy z zakresu bankowości
- Brak zrozumienia grup docelowych – presja czasu nie pozwalała na zwrócenie się do grup docelowych we właściwy sposób. Sposób przekazywania informacji nie zawsze był odpowiedni (np. w przypadku MŚP)
- Jakość przygotowanych materiałów

- Kontrakt umożliwiał prowadzenie działań tylko przez jeden rok. W celu kontynuowania działań w 2006 roku, konieczny był nowy kontrakt

Zdobyte doświadczenia, które można wykorzystać w bieżącej kampanii

- Zrozumienie grup docelowych w celu wywierania większego wpływu
- Zmiana strategii działań z poprzedniego roku - z „dlaczego” na „jak sobie poradzić”
- Opracowanie lepszych materiałów – w tym roku przygotowano film dla szkół i prezentacje. Szkoły wykorzystywane są jako instytucje rozpowszechniające informacje, często dzięki zaangażowaniu rodziców
- Zwiększenie widoczności mediów – pakiet mediów obejmuje w tym roku wszystkie szwedzkie gazety
- Zdobycie profesjonalnego wsparcia w celu przyciągnięcia uwagi mediów
- Bardziej elastyczny kontrakt – nowy kontrakt podpisany przez firmy można przedłużyć bez konieczności nowych zadań (plan roczny jest przyjęty poprzez dokonanie płatności) Jeśli w przyszłości tylko kilka firm zaangażuje się w projekt, możliwe, że trzeba będzie z niego zrezygnować. Przewiduje się długą współpracę
- Nawiązanie stosunków z różnymi organizacjami rozpowszechniającymi informacje (np. stowarzyszenia sportowe, stowarzyszenia ludzi starszych itd.)
- Stworzenie grup roboczych (WG), które pomagają PM w opracowaniu pomysłów. Podejście to należy ulepszyć po dokonaniu pierwszej oceny działalności WG

Wskazówki pod kątem przyszłych kampanii

- Potrzebne są dostępne środki w celu aktualizacji materiałów
- Należy przygotować plan dotyczący działań po rozpoczęciu kampanii. Plan ten powinien określać role i obowiązki, sposób zarządzania kampanią i dostosowania jej, jeśli jest to konieczne

Inicjatywy w ramach kampanii

e-bezpieczeństwo - Sztokholm

W miarę jak administracja publiczna zwiększa zakres swoich usług i kontakt z obywatelami, potrzeba e-bezpieczeństwa jest coraz większa. Obywatele korzystający z nowych usług oczekują takiego samego bezpieczeństwa, poufności i wiarygodności jak wówczas, gdy korzystają z tradycyjnych usług, nie świadczonych drogą internetową. Aby obywatele zaakceptowali nowe usługi i zaczęli z nich korzystać, muszą mieć do nich zaufanie i dlatego e-bezpieczeństwo jest bardzo ważną kwestią dla wszystkich rządów i władz lokalnych.

Charakter współczesnej globalnej infrastruktury oznacza również, że wszystkie miasta stanowią część nowej cyfrowej gospodarki usług. Miasta powinny zrozumieć znaczenie e-bezpieczeństwa oraz to, że muszą stawać się coraz bardziej zależne od siebie nawzajem, aby móc zapewnić właściwe e-bezpieczeństwo.

Istnieje kilka inicjatyw poświęconych e-bezpieczeństwu, lecz większość z nich podejmowana jest w ramach programów poszerzających wiedzę, skierowanych do obywateli i firm. Wraz z rosnącą presją wywieraną na miasta, aby zapewniały usługi w sposób bezpieczny i poufny, zachodzi silna potrzeba, aby miasta współpracowały ze sobą w tworzeniu standardów i dzieleniu się najlepszymi praktykami w zakresie e-bezpieczeństwa.

SaferInternet - Youth panels a success story! (artykuł)²²

Streszczenie

Aby rozpowszechniać wiedzę o bezpieczniejszym korzystaniu z Internetu, szwedzki węzeł zdecydował się zorganizować kilka regionalnych seminariów: są one skierowane głównie do nauczycieli, ale obejmują również innych profesjonalistów pracujących z dziećmi i młodzieżą.

Jednym z najbardziej udanych i docenianych elementów tych seminariów jest grupa młodzieży opowiadająca o tym, jak młodzi ludzie korzystają z nowych mediów i jak je postrzegają.

Szczegóły

Mimo że dzieci i nauczyciele spotykają się prawie codziennie, nauczyciele są w większości przypadków całkowicie nieświadomi tego, jak ich uczniowie korzystają z nowych mediów, takich jak Internet i telefony komórkowe, w życiu społecznym. Dla nauczycieli Internet stanowi w większej mierze narzędzie gromadzenia informacji niż komunikowania się. W przypadku ludzi młodych sytuacja wygląda odwrotnie.

Na każdym regionalnym seminarium szwedzki węzeł upewnia się, że lokalny partner wybrał zespół młodych ludzi ze szkół w danym regionie. Zespół ten zazwyczaj składa się z sześciu do ośmiu dziewcząt i chłopców w wieku od 13 do 18 lat. Z pomocą profesjonalnego moderatora dzielą się oni z publicznością swoją wiedzą i doświadczeniami.

Młodzi ludzie proszeni są o opisanie, do jakich celów, na co dzień wykorzystują Internet: chatowanie, odwiedzanie różnych grup dyskusyjnych, odrabianie pracy domowej oraz granie w gry internetowe. Pytani są również o problemy takie jak zastraszanie, spoufalanie się w celu ewentualnego wykorzystania seksualnego (child grooming) itd., które oni lub ich znajomi napotykają, oraz o to, jak radzą sobie z tymi problemami. Poruszane są również takie zagadnienia jak edukacja w zakresie ICT w szkole i zaangażowanie rodziców.

²² <http://www.saferInternet.org/www/en/pub/insafe/news/articles/0706/sv1.htm> , 31 lipca 2006 r.

Z zasady wszyscy nastolatkomie należący do takiego zespołu bardzo chętnie rozmawiają i dumni są z tego, że są ekspertami dnia. Bardzo doceniają to, że są traktowani poważnie i wysłuchiwanie przez dorosłych. Punktem seminarium, który zazwyczaj oceniany jest najwyżej, jest właśnie wystąpienie zespołu młodych ludzi. Potwierdza to, że dorośli również uznają te wypowiedzi za bardzo cenne i są zainteresowani wypełnieniem luki w wiedzy pomiędzy pokoleniami.

SaferInternet - Swedish pupils and mobile phones (artykuł)²³

Streszczenie

Szwedzka ankieta zawiera informacje na temat użycia telefonów komórkowych przez dzieci i młodzież.

Szczegóły

Na początku wiosennego trymestru 2006 poproszono uczniów kilku klas o odpowiedź na internetowy kwestionariusz dotyczący użycia telefonów komórkowych. Były to klasy, z którymi skontaktowano się w ramach projektu "młody Internet" poświęconego bezpieczniejszemu użyciu Internetu i nowych technologii. Na kwestionariusz odpowiedziało 130 uczniów w wieku od 10 do 18 lat.

Kwestionariusz ten wykazał, że 97% uczniów uczniów ma swój własny telefon, a 80% używa go codziennie. Zgodnie z oczekiwaniami, najpopularniejszym zastosowaniem telefonu są rozmowy telefoniczne (90%) i wysyłanie/otrzymywanie SMS-ów (78%). Inne zastosowania telefonu wymienione w ankiecie to: gry (27%), zdjęcia (44%), MMS-y (21%) i e-maile (4%). Jeden uczeń na czterech otrzymał SMS-a lub zdjęcia, które zdenerwowały go, zasmuciły lub przestraszyły. Jednak tylko 3% spośród tych uczniów powiedziało o tym osobie dorosłej.

Inna część kwestionariusza była poświęcona zasadom dotyczącym korzystania z telefonów komórkowych w szkołach. Jeden uczeń na trzech nie wiedział, czy w szkole obowiązują takie zasady.

Chociaż telefony komórkowe stały się bardzo popularne, więcej niż jeden telefon na cztery nie ma aparatu fotograficznego i bardzo niewielu uczniów ma telefony z najnowszymi funkcjami takimi jak 3G.

²³ <http://www.saferInternet.org/ww/en/pub/insafe/news/articles/0706/sv2.htm> , 31 lipca 2006.

28. Wielka Brytania

Na podstawie odpowiedzi na kwestionariusz oraz uzupełniających informacji z przeprowadzonych rozmów, badań i dodatkowych materiałów dla Wielkiej Brytanii wyszczególniono następujące części:

[Obecna sytuacja](#)

[Rząd jako twórca prawnych, regulacyjnych i instytucjonalnych uregulowań służących poszerzaniu wiedzy](#)

[Władze państwowe jako użytkownik systemów informacyjnych](#)

[Władze lokalne jako użytkownik systemów informacyjnych](#)

[Rząd jako partner przedsiębiorstw i przemysłu](#)

[Rząd jako partner społeczeństwa](#)

[Statystyki i kluczowe wskaźniki wydajności \(KPI\)](#)

[Inicjatywy w ramach kampanii](#)

Obecna sytuacja

- „W 2004 roku dwie trzecie firm brytyjskich doświadczyło złośliwego incydentu w związku ze sprzętem elektronicznym – do czerwca 2005 roku rozsyłano po całym świecie ponad 5,7 miliona fałszywych e-maili dziennie, szukając informacji finansowych potrzebnych do popełnienia oszustwa”²⁴
- Według Ankiety dotyczącej naruszania bezpieczeństwa informacji (Information Security Breaches Survey 2006)²⁵ zleconej przez Ministerstwo Handlu i Przemysłu Wielkiej Brytanii:
 - Dwie trzecie firm brytyjskich doświadczyło w poprzednim roku incydentu związanego z bezpieczeństwem. Ponad połowa firm brytyjskich doświadczyła złośliwego incydentu
 - O jedną trzecią mniej firm niż w 2004 roku miało wirusy. Jednak liczba infekcji, jakie miały miejsce w każdej firmie, wzrosła i wirusy nadal stanowią 50% najgorszych incydentów związanych z bezpieczeństwem (pojedyncza główna przyczyna)
 - Pomimo dalszego wzrostu akceptowanych strategii użycia i ograniczenia dostępu do Internetu incydenty związane z niewłaściwym użyciem nadal są na poziomie z 2004 roku. Niewłaściwe użycie przez pracowników ma

²⁴ Symantec Research, Management Today, listopad 2005 r.

²⁵ [dti_info_security_2006.pdf](#)

największy wpływ na małe firmy – połowa z nich podawała to jako źródło najgorszego rodzaju incydentów

- o Pomimo dużej wagi, jaką przywiązuje się do bezpieczeństwa i wzrostu bezpieczeństwa oraz akceptowanych strategii użycia, w wielu firmach nie ma kultury związanej z wiedzą o bezpieczeństwie

Rząd jako twórca prawnych, regulacyjnych i instytucjonalnych uregulowań służących poszerzaniu wiedzy

Krajowa strategia poszerzania wiedzy

Brytyjską Rządową Strategię Bezpieczeństwa Informacji (Government Strategy for Information Assurance) ratyfikowano w czerwcu 2003 roku. Stworzył ją Centralny Gwarant Bezpieczeństwa Informacji (Central Sponsor for Information Assurance - CSIA) powołany spośród członków Kancelarii Gabinetu. Strategia ta poświęcona jest poszerzaniu wiedzy w zakresie partnerstw pomiędzy rządem, szerszym sektorem publicznym, przedsiębiorstwami i obywatelami w celu ochrony społecznego i ekonomicznego dobra narodu. Strategia ta obejmuje około 70 kluczowych działań, w tym pomoc dla społeczeństwa i porady dla małych przedsiębiorstw.

Jest ona wymierzona do kluczowych odbiorców takich jak władze państwowe, władze lokalne, przemysł i obywatele. Dotychczas wpływ strategii był znaczący dzięki programom takim jak CSIA Claims Tested Mark (www.cctmark.gov.uk), Senior Information Risk Owner Programme (SIRO), Information Assurance Governance Framework, projektem ostrzegającym takim jak ITsafe (www.itsafe.gov.uk) oraz programom poszerzającym wiedzę, np. kampanii Get Safe Online (www.getsafeonline.org)

Prawne, regulacyjne i instytucjonalne ustalenia w celu poszerzania wiedzy

W rządzie brytyjskim poszerzanie wiedzy w zakresie bezpieczeństwa informacji staje się coraz ważniejszą kwestią. CSIA współpracuje z różnymi partnerami w rządzie, m.in. z Ministerstwem Handlu i Przemysłu (DTI), Centrum Koordynacji Bezpieczeństwa Krajowej Infrastruktury (NISCC), Ministerstwem Spraw Wewnętrznych i Urzędem ds. Przestępczości Zorganizowanej (SOCA).

Dzięki komisjom takim jak Komisja Pomocy, która podlega Komisji ds. Bezpieczeństwa powołanej spośród członków Kancelarii Gabinetu, opracowywane są kampanie i fora poszerzania wiedzy w celu zapewnienia ogólnorządowego podejścia do poszerzania wiedzy w zakresie bezpieczeństwa informacji.

Pracując nad promowaniem dobrego zarządzania bezpieczeństwem informacji, DTI popiera używanie międzynarodowych norm bezpieczeństwa ISO 17799 i ISO 27001 (które są odpowiednikami dotychczasowych norm brytyjskich BS 7799 Część 1 i 2). Są to normy oparte na ryzyku, które w zamierzeniu mają być rozwiązaniami opartymi na zarządzaniu. Według DTI normy te są pomocne w biznesie. Opracowywanie norm

wciąż trwa: BS 7799 Część 3, dotyczącą zarządzania ryzykiem, wprowadzono wcześniej w 2006 roku. W ISO nadal trwają prace i oczekuje się, że wraz z upływem czasu na arenie norm międzynarodowych pojawi się „rodzina” norm dotyczących bezpieczeństwa informacji z serii ISO 27000. DTI jest poważnie zaangażowane na poziomie międzynarodowym, jeśli chodzi o normy bezpieczeństwa.

Zakres kompetencji DTI obejmuje przedsiębiorstwa. Kancelaria Gabinetu zajmuje wiodącą pozycję, jeśli chodzi o wdrażanie norm na poziomie władz państwowych i lokalnych.

Ogólne informacje na temat norm: W 1993 roku w odpowiedzi na zapotrzebowania przemysłu DTI powołało grupę roboczą ds. przemysłu składającą się z osób doświadczonych w dziedzinie zarządzania bezpieczeństwem informacji. Kodeks postępowania w zakresie zarządzania bezpieczeństwem informacji utworzono później tego samego roku i dał on podstawę dla Brytyjskiej Normy (British Standard) BS 7799 Część 1, po raz pierwszy opublikowanej w 1995 roku i poprawionej w 1999 roku.

W przemyśle potrzebny był również mechanizm, który umożliwiłby certyfikację w oparciu o BS 7799, która zapewniłaby niezależny i wiarygodny sposób wykazywania zgodności z normami. A zatem DTI zwróciło się do BSI (British Standards) o przygotowanie BS 7799 Część 2 - specyfikacji, w oparciu o którą firma oceniana jest pod kątem przestrzegania BS 7799 Część 1. BS 7799 Część 2 również stworzono w porozumieniu z brytyjskimi przedsiębiorstwami. Po raz pierwszy opublikowano tę część w 1998 roku, a poprawiono w 1999 roku, a następnie w 2002 roku.

W grudniu 2000 BS 7799 Część 1 uzyskała status normy międzynarodowej, stając się ISO/IEC 17799. Normę tę poprawiono w 2005 roku zgodnie ze zwykłymi procedurami ISO. Począwszy od kwietnia 2007 roku norma ta będzie na nowo oznakowana jako ISO/IEC 27002.

W 2005 roku BS 7799 Część 2 również stała się normą międzynarodową i obecnie jest oznaczona jako ISO/IEC 27001. Wiele firm może wyrazić chęć uzyskania niezależnej certyfikacji w oparciu o ISO/IEC 27001 za pośrednictwem zewnętrznych organizacji takich jak organy uwierzytelniające. Inne firmy mogą zdecydować się na korzystanie z ISO/IEC 17799 jako wytycznych dotyczących wdrażania ich własnego systemu zarządzania bezpieczeństwem informacji, niekoniecznie ubiegając się o certyfikację.

W wyniku wpływowej Ankiety dotyczącej naruszania bezpieczeństwa informacji przeprowadzonej dla DTI w 2006 roku przez PricewaterhouseCoopers (zobacz dalej) okazało się, że czynnikami motywującymi firmy i dostawców do przyjęcia norm bezpieczeństwa informacji są skuteczność i wydajność (a nie jakakolwiek chęć posiadania znaku jakości). 87% firm stosujących te normy stwierdziło, że ulepszyło ciągłość działania firmy, a 85% uznało, że zmniejszyło szkody wynikające z incydentów związanych z bezpieczeństwem. Nie jest to zjawisko typowe wyłącznie dla Zjednoczonego Królestwa. Przyjęcie normy pod koniec 2005 roku, gdy BS Część 2

stała się międzynarodową normą, doprowadziło do znacznego wzrostu, zwłaszcza na takich rynkach jak japoński.

Władze państwowe jako użytkownik systemów informacyjnych

Najnowsze programy i inicjatywy poszerzania wiedzy

Poszerzanie wiedzy władz państwowych odbywa się za pośrednictwem CSIA poprzez kluczowe programy rozwojowe.

W 2003 roku napisano i opublikowano dokument Protecting Our Information Systems, Working in partnership for a secure and resilient UK information infrastructure („Ochrona naszych systemów informacyjnych, praca w ramach partnerstwa na rzecz bezpiecznej i odpornej infrastruktury informacyjnej Zjednoczonego Królestwa”). Określa on, dlaczego systemy informacyjne muszą być chronione, wymienia zagrożenia dla systemów informacyjnych oraz wyjaśnia, dlaczego rząd zainteresowany jest ochroną wszystkich takich systemów. Dokument ten można ściągnąć ze strony:

http://www.cabinetoffice.gov.uk/csia/documents/pdf/CSIA_booklet.pdf

Opracowywane programy obejmują również sieć Senior Information Risk Owner – inicjatywę mającą na celu wyznaczenie osób na wyższych stanowiskach jako odpowiedzialnych za ryzyko informacyjne. W ramach programu szkoli się odpowiedzialnych za ryzyko informacyjne tak, by byli coraz bardziej świadomi znaczenia kluczowych zasad bezpieczeństwa informacji dotyczących poufności, integralności i dostępności oraz tego, jak należy je właściwie stosować.

Innym środkiem opracowanym i wdrażanym na poziomie władz państwowych jest dokument Information Assurance Governance Framework (Podstawy zarządzania bezpieczeństwem informacji). Został on opublikowany w sieci 22 listopada 2005 roku i wyjaśnia proces zarządzania bezpieczeństwem informacji oraz przedstawia wytyczne dotyczące wdrażania i najlepszej praktyki dla organizacji sektora publicznego.

Dokument ten można ściągnąć ze strony:

www.cabinetoffice.gov.uk/csia/ia_governance/content.asp

Przeglądu inicjatyw związanych z bezpieczeństwem informacji dokonał dla CSIA niezależny podmiot w listopadzie 2004 roku. Raport zatytułowany Information Assurance: A review of UK Government and Industry Initiatives („Bezpieczeństwo informacji: przegląd brytyjskich inicjatyw rządowych i przemysłowych”) zawiera informacje na temat inicjatyw, strategii i polityk, które wspierają ochronę systemów informacyjnych, opisując działania podejmowane przez organizacje sektora publicznego oraz prywatnego.

Kolejnym przedsięwzięciem w ramach strategii poszerzania wiedzy jest Information Assurance Technical Programme (IATP). Program ten jest inicjatywą ogólnorządową mającą na celu zbadanie wymogów poszczególnych ministerstw w zakresie

bezpieczeństwa informacji, jako że zapewnienie bezpieczeństwa informacji przez ministerstwa ma ścisły związek z przyszłym produktem, natomiast rozwój usług – z technologią informacyjną.

Ankieta dotycząca naruszania bezpieczeństwa informacji przeprowadzona przez DTI, choć skierowana do firm, jest powszechnie znana na poziomie władz państwowych i lokalnych i zawiera dużo informacji na temat pracy DTI z firmami. W 2006 roku podjęto próbę promowania wyników ankiety na bardziej lokalnym poziomie, np. wśród Organów ds. Rozwoju Regionalnego.

Administracja lokalna jako użytkownik systemów informacyjnych

Najnowsze programy i inicjatywy poszerzania wiedzy

Władze lokalne odniosły korzyść ze współpracy z władzami państwowymi w dziedzinie przyjęcia podstaw bezpieczeństwa informacji (www.cabinetoffice.gov.uk/csia/ia_governance/content.asp) w celu rozwiązania kluczowych problemów związanych z bezpieczeństwem informacji na poziomie władz lokalnych.

CSIA Claims Tested mark (www.cctmark.gov.uk) jest znakiem jakości w zakresie bezpieczeństwa IT dającym władzom lokalnym pewność, że produkty i usługi związane z bezpieczeństwem informacji, z których władze te korzystają, będą miały dokładnie takie działanie, jakiego władze te spodziewają się.

Pokazy CSIA poświęcone bezpieczeństwu informacji miały miejsce w Zjednoczonym Królestwie w 2005 i 2006 roku i okazały się bardzo skuteczne, jeśli chodzi o przekazanie kluczowych wiadomości dotyczących bezpieczeństwa informacji władzom lokalnym i szerszej sieci sektora publicznego. Sesje te umożliwiły debatę na tematy związane z zarządzaniem informacjami, normami bezpieczeństwa informacji, znakiem CSIA Claims Tested Mark i Instytutem dla Profesjonalistów w dziedzinie Bezpieczeństwa Informacji.

Inicjatywa WARPs (Warning Advice and Reporting Points), wspierana przez CSIA i wdrażana za pośrednictwem NISCC, obejmuje władze lokalne. W ramach inicjatyw WARP tworzone są portale wymiany informacji, do których dostęp mają wyłącznie zaufani członkowie konkretnej inicjatywy WARP. Dalsze informacje dostępne są pod następującym adresem: <http://www.niscc.gov.uk/niscc/warplnfo-en.html>. Inicjatywy WARP stanowią część strategii wymiany informacji NISCC, mającej na celu pomoc w zwalczaniu rosnącego ryzyka ataku elektronicznego na systemy informacyjne.

Brytyjska Grupa Użytkowników ISO 17799 powołana przez DTI liczy ponad 600 członków, głównie przedstawicieli przedsiębiorstw, ale również wielu przedstawicieli sektora publicznego. Grupa ta dowodzona jest przez komisję nadzorującą ds. przemysłu (DTI zapewnia sekretariat), systematycznie organizuje warsztaty dotyczące różnych aspektów bezpieczeństwa z naciskiem na serię norm ISO 17799/27000. Gospodarzem

ostatnich warsztatów regionalnych (maj 2006) był przedstawiciel sektora publicznego (Rada Miasta Leeds). Przewodnik dotyczący Grupy Użytkowników można ściągnąć ze strony internetowej DTI www.dti.gov.uk/sectors/infosec

DTI wspiera konferencję „Bezpieczeństwo informacji i ciągłość działania firmy w sektorze prywatnym”, piąte z kolei wydarzenie tego typu, które ma mieć miejsce w listopadzie 2006 roku. Zobacz: www.kable.co.uk

Administracja jako partner przedsiębiorstw i przemysłu

Małe i średnie przedsiębiorstwa (MŚP)

Imprezy objazdowe organizowane przez CSIA – Brytyjskie Izby Handlowe mają trwać od kwietnia 2006 do listopada 2006 roku. W imprezach tych kładziony jest nacisk na zagadnienia związane z bezpieczeństwem informacji oraz promowane są inicjatywy takie jak CCT Mark, Get Safe Online, ITSafe, WARPs, nadzór nad bezpieczeństwem informacji oraz programy SIRO dla małych i średnich przedsiębiorstw. Organizatorzy tych imprez docierają bezpośrednio do około 500 małych przedsiębiorstw, udzielając im porad i wskazówek na temat bezpieczeństwa informacji.

Inicjatywę Get Safe Online podjęto w październiku 2005 roku. Jest to inicjatywa krajowa obejmująca zarówno sektor publiczny jak i prywatny, mająca na celu poszerzenie wiedzy z zakresu bezpieczeństwa w Internecie zarówno w społeczeństwie jak i wśród mikroprzedsiębiorstw (np. mniej niż 10 pracowników lub brak pracowników ponoszących bezpośrednią odpowiedzialność za bezpieczeństwo IT). Inicjatywa Get Safe Online jest wspierana przez rząd Jej Królewskiej Mości, organy porządku publicznego i przemysł. Więcej informacji można znaleźć na stronie: www.getsafeonline.org

Plany związane z inicjatywą Get Safe Online zakładają obranie strategii kampanii koncentrującej się na małych i średnich przedsiębiorstwach, opartej na partnerstwie z organizacjami takimi jak Business Links i National Computing Centre.

WARPs (zobacz powyżej). Członkowie WARP zgadzają się na współpracę w ramach wspólnoty i wymianę informacji w celu zmniejszenia ryzyka zagrożenia ich systemów informacyjnych, a tym samym zmniejszenia ryzyka dla ich organizacji. Wspólnota ta mogłaby opierać się na konkretnym sektorze biznesu, położeniu geograficznym, normach technologicznych, grupowaniu ryzyka lub czymkolwiek, co ma sens w kontekście biznesu.

Począwszy od zobowiązania zawartego w Białym Dokumencie Rządu Zjednoczonego Królestwa, DTI stworzyło materiały, które są dostępne w Internecie i zawierają łatwe do zrozumienia wskazówki dotyczące bezpieczeństwa informacji dla mniejszych przedsiębiorstw. Materiały te uzupełniano i aktualizowano, są one dostępne pod adresem www.dti.gov.uk/sectors/infosec (poprawione strony będą dostępne od października 2006). Na stronie tej dostępnych jest wiele publikacji oraz innych pozycji. Stworzono również internetowe narzędzie kontroli stanu bezpieczeństwa oparte

na ówczesnej normie brytyjskiej BS 7799 (która stała się normą międzynarodową) – narzędzie to znajduje się na stronie www.securityhealthcheck.dti.gov.uk.

DTI pełni rolę Sekretariatu Brytyjskiej Grupy Użytkowników ISO 17799 – forum prowadzonego przez przedstawicieli przemysłu, mającego na celu promowanie i rozpowszechnianie wymiany dobrej praktyki i wiedzy specjalistycznej z zakresu dobrego zarządzania bezpieczeństwem informacji w oparciu o korzystanie z ISO 17799 i ISO 27001 (dotychczas Normy Brytyjskie BS 7799 Część 1 i 2). Grupa ta dowodzona jest przez Komisję Nadzorującą, składającą się głównie z przedstawicieli przemysłu. Korzyściami płynącymi z (darmowego) członkostwa w grupie są, między innymi, systematyczne warsztaty i biuletyny oraz możliwość nawiązywania kontaktów.

Dostawcy usług internetowych (ISP)

Get Safe Online ściśle współpracuje z brytyjskim Stowarzyszeniem ISP (ISPA). Przedstawiciel GSOL (Get Safe Online) wypowie się na Dorocznej Konferencji ISPA we wrześniu 2006 roku na temat tego, gdzie planuje się udostępnienie bezpłatnych, automatycznie dostarczanych treści („auto-content”) dotyczących ISP, opracowanych przez Get Safe Online i dostępnych dla wszystkich ISP. BT, jeden z największych brytyjskich dostawców usług internetowych, jest sponsorem Get Safe Online.

Media

Należy zwrócić uwagę na to, że w poniższym przykładzie wykorzystano media jako kanał dotarcia do innych grup docelowych i nie przedstawiono ich jako odrębną grupę docelową.

Inicjatywa Get Safe Online jest jak na razie najbardziej znaczącym długotrwałym przedsięwzięciem, jeśli chodzi o zainteresowanie mediów tematem bezpieczeństwa w Internecie. Kampania rozpoczęła się w zeszłym październiku i – jeśli chodzi o przyciągnięcie uwagi mediów – obecnie ma na swoim koncie następujące osiągnięcia:

- 208 relacji – 33 spośród nich były emitowane i drukowane na skalę krajową, pozostałe ukazały się w lokalnym/regionalnym radiu i gazetach
- Konkurs bezpłatnej krajowej gazety (Metro - rozprowadzane we wszystkich głównych konurbacjach Zjednoczonego Królestwa) – całkowity zasięg konkursu Metro: 18 milionów osób. Liczba uczestników konkursu Metro: 60 000 (dwa razy większa niż zwykle osiągnięty poziom 29 000 zgłoszeń)
- „Całkowita liczba uczestników konkursu Get Safe Online była najwyższa w historii konkursu Metro.” Anthony Worssam, Prezes Działu Sponsoringu i Promocji, Metro
- Steve Wright Show, Radio 2, „Internetowa strona tygodnia”
- Finalista europejskiej nagrody Sabre PR/Media Award

W tygodniu, w którym rozpoczęto kampanię, dotarła ona bezpośrednio do 175 000 osób – osobiście lub poprzez stronę internetową – co wiązało się z kosztem „pozyskania klienta” (cost per acquisition) równoważnym 60 pensom (Wielka Brytania).

Chociaż budżet przeznaczony na Get Safe Online, pochodzący z datków sponsorów, wynosi około 1 miliona funtów, nie wystarcza to, aby przeprowadzić krajową kampanię reklamową ATL (z wykorzystaniem tradycyjnych środków masowego przekazu). Jediną realną opcją jest kampania oparta na PR i reklamie internetowej.

Opracowywane są plany dotyczące kolejnego etapu działania rozpoczynającego się w październiku 2006 roku, w którym zostaną wykorzystane media krajowe, regionalne i lokalne.

Partnerstwo publiczno-prywatne

Skuteczne partnerstwo publiczno-prywatne (w dziedzinie poszerzania wiedzy i edukacji/szkolenia)

DTI współpracuje na zasadzie partnerstwa z różnymi organizacjami w celu promowania dobrej praktyki bezpieczeństwa informacji. Przykłady współpracy w minionym roku obejmują przewodnik opracowany wspólnie z Instytutem Dyrektorów – Institute of Directors (dostępny na stronie DTI www.dti.gov.uk/sectors/infosec), publikację i cykl warsztatów poświęcone bezpieczeństwu informacji w łańcuchu dostaw (inicjatywa DTI, CBI (Związku Pracodawców Brytyjskich) oraz różnych firm z sektora prywatnego). Zobacz: www.cbi.org.uk

DTI współpracowało z Izbą Handlową Środkowego Yorkshire (Mid Yorkshire Chamber of Commerce) w celu opracowania pakietu do e-nauki, który z założenia ma być zarówno łatwy, jak i atrakcyjny w użyciu. Zobacz: www.bobs-business.co.uk

Obecnie DTI współpracuje z Urzędem ds. Rozwoju Regionalnego (RDA) księstwa Yorkshire (Yorkshire Forward), z SOCA, lokalnymi oddziałami policji Yorkshire i lokalną organizacją charytatywną (People United Against Crime) w celu opracowania regionalnej strony internetowej poświęconej bezpieczeństwu informacji - „Yorkshire Safe”. Strona ta zostanie uruchomiona w październiku 2006 roku, a zatem wydarzenie to zbiegnie się z planowanymi imprezami promocyjnymi Get Safe Online. Nawiązano kontakt z innymi RDA i oczekuje się, że będą realizowane kolejne wspólne projekty.

DTI wsparło rozwój Instytutu Profesjonalistów ds. Bezpieczeństwa Informacji (IISP) www.instisp.org, który ma na celu podnieść kwalifikacje i pozycję profesjonalistów ds. bezpieczeństwa informacji. IISP powstał w lutym 2006 roku i w ciągu pierwszych trzech miesięcy jego istnienia złożono ponad 700 wniosków o członkostwo w Instytucie, z czego część pochodzi z zagranicy. Różne rządowe departamenty, w tym DTI, Kancelaria Gabinetu, CESG (Communications-Electronics Security Group – Grupa ds. Bezpieczeństwa Łączności i Elektroniki), NISCC zaangażowały się w prace

Instytutu. Obecnie DTI współpracuje z IISP nad opracowaniem członkowskiego portalu internetowego. Ukończenie projektu planowane jest przed lutym/marcem 2007 roku.

DTI współpracuje z sektorem przemysłowym w celu opracowania Ankiety dotyczącej naruszania bezpieczeństwa informacji, która ma być przeprowadzana, co dwa lata. Jest to największa i najbardziej wpływowa ankieta tego rodzaju i jest przeprowadzona na w pełni reprezentatywnej próbie. Ankietę 2006 zapoczątkowano w kwietniu 2006 roku; kopie raportu są dostępne na stronie internetowej ENISA lub na stronie www.security-survey.gov.uk. Ankietę 2006 przeprowadziła dla DTI firma PricewaterhouseCoopers. Przedsięwzięcie to sponsorowane było przez kilka największych firm zajmujących się bezpieczeństwem. Różne organizacje (w sumie 8) pełniły rolę niezależnych recenzentów.

DTI jest członkiem różnych organizacji związanych z bezpieczeństwem, np. Forum Bezpieczeństwa Informacji (Information Security Forum, ISF – które pełniło rolę jednego z niezależnych recenzentów Ankiety dotyczącej naruszania bezpieczeństwa informacji w 2006) czy Organu Doradczego ds. Bezpieczeństwa Informacji (Information Assurance Advisory Council - IAAC). DTI było, na przykład, gospodarzem posiedzeń IAAC, w tym Dorocznego Sympozjum IAAC.

CSIA jest fundatorem Get Safe Online, wspólnej inicjatywy sektora publicznego i prywatnego. Chociaż przygotowanie tej inicjatywy zajęło trochę czasu, obecnie w ramach Get Safe Online podejmowane są regularnie działania poszerzające wiedzę. Zaangażowanie znanych brytyjskich i międzynarodowych marek, takich jak BT, Dell, eBay, HSBC, Lloyds TSB i Microsoft zapewniło kilka kanałów o wyjątkowo dużym zasięgu, prowadzących do konsumentów internetowych.

Kilka przykładów zaangażowania firm w sponsoraowanie inicjatyw

Microsoft zapewnił reklamę internetową i artykuł wstępny w jednomiesięcznym okresie wdrażania inicjatywy, a inicjatywa GSOL przejęła stronę internetową firmy w dniu, w którym rozpoczęła się. Dzięki temu w październiku 2005 roku reklama pojawiła się na stronie ponad 60 milionów razy, co stanowiło wartość równą 200 tysiącom funtów. Oprócz działalności związanej z kampanią Microsoft podjął się umieszczenia na trwałe w portalu internetowym MSN ponad 400 kluczowych słów związanych z bezpieczeństwem.

Microsoft prowadził również promocyjny program regionalnych imprez objazdowych, w którym wykorzystano przyciągające uwagę, oznakowane marką komputery Mini i w ramach którego setki ochotników udzielały w centrach handlowych porad w zakresie bezpieczeństwa w Internecie.

Firma BT połączyła inicjatywę GSOL z wieloma różnymi kampaniami poświęconymi podobnym zagadnieniom, np. usłudze Clean Feed, która polega na blokowaniu stron pornograficznych w komputerach osobistych.

O GSOL było również głośno w wielu relacjach prasowych, radiowych oraz relacjach środków przekazu, które były poświęcone defraudacji tożsamości, bezpieczeństwu w Internecie i grom komputerowym. W ramach krajowych relacji prasowych pojawiły się obszernie artykuły, natomiast w styczniu rozprowadzono 3,25 miliona dodatków do gazety Mail on Sunday poświęconych bezpieczeństwu, z wizerunkiem Alice Beer z programu „Watchdog” na okładce. („Watchdog” to program poświęcony ochronie konsumenta, emitowany w BBC)

Dodatkowe stałe wsparcie stanowi strona internetowa BT (www.bt.com/security) i firmowa broszura Green Cross Code.

Firma HSBC ma swój udział w komentarzach ukazujących się w mediach, pełniąc rolę rzecznika GSOL oraz aktywnych mówców w czasie imprez – na przykład w czasie ostatniej imprezy GSOL Executive Briefing, która odbyła się w Admiralty House oraz w podcastach Guardian Unlimited. Firma HSBC podjęła również wiele internetowych działań promocyjnych, m. in. umieściła na stałe na stronie www.hsbc.co.uk wyróżniające się odsyłacze oraz rozpoczęła bezpośrednią internetową korespondencję bankową z klientami.

Firma LloydsTSB nie tylko wzięła udział w promocji internetowej, ale także włączyła GSOL do swojej internetowej ankiety poświęconej bezpieczeństwu w bankowości oraz wykorzystwała bankomatowe rachunki do rozpowszechnienia wiadomości o 4 milionach transakcji w listopadzie. Firma ta wykorzystuje również treści GSOL w swojej sekcji poświęconej bezpieczeństwu w Internecie.

Aktywny charakter sponsorowanego marketingu umożliwił znaczne rozszerzenie zasięgu GSOL na obszary, które byłyby niemożliwe do sfinansowania przy użyciu tradycyjnego modelu marketingu. Na kilku najbardziej popularnych brytyjskich stronach internetowych, takich jak www.ebay.co.uk i www.paypal.co.uk umieszczono sieć reklamową, która doskonale odpowiada wspólnemu celowi „panowania nad Internetem”.

Wartość tej przestrzeni reklamowej wynosi ponad 200 tysięcy funtów. Sieć jest doskonała dla celów GSOL – w momencie, w którym dokonywane są transakcje, wiadomość o bezpieczeństwie pojawia się w centralnym punkcie ekranu.

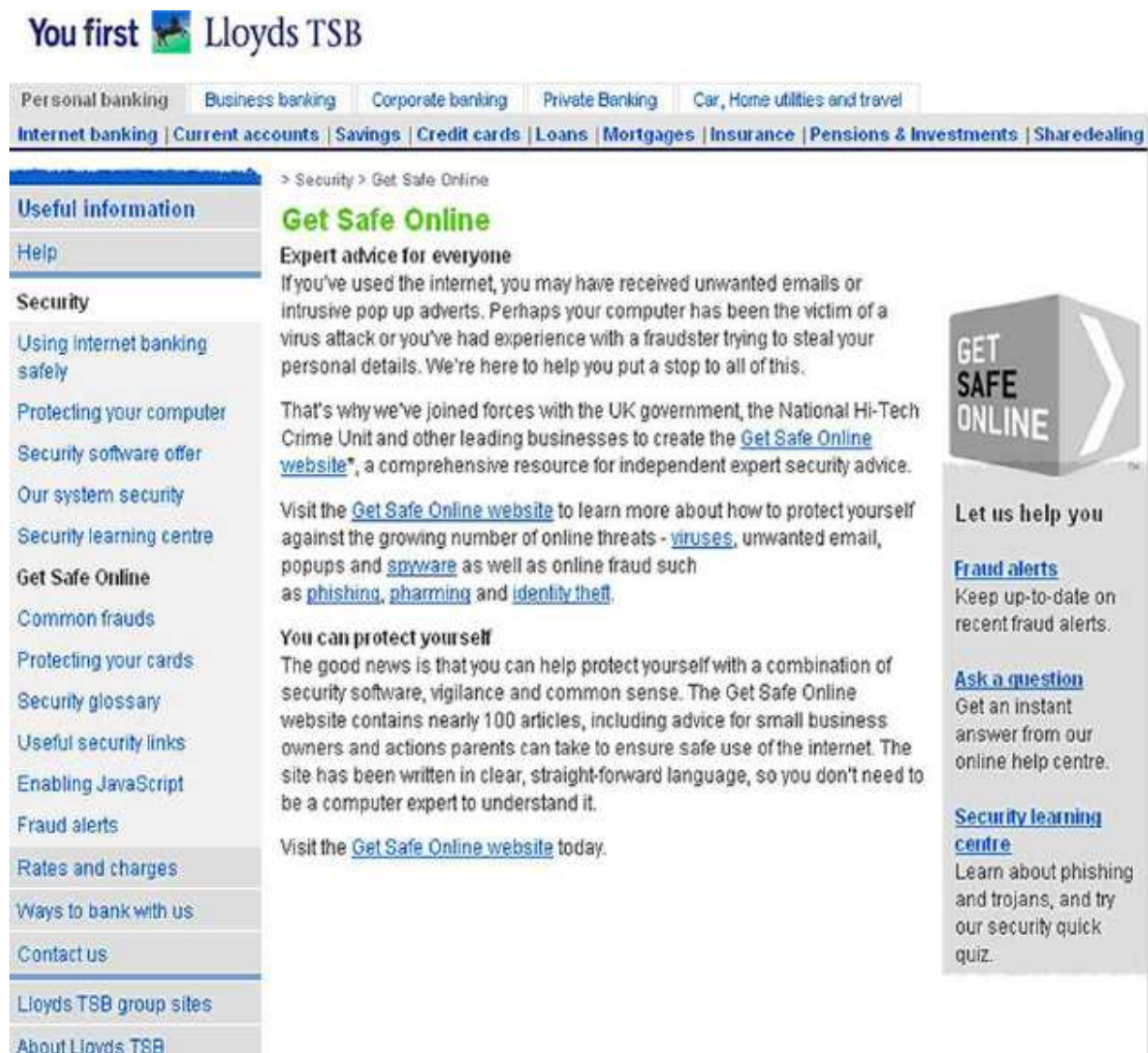
Wsparcie i koordynacja ze strony Kancelarii Gabinetu wzmocniły początkową organizację GSOL, a obecnie zapewniają kluczową strategię oraz podejmowanie rutynowych działań. Ministerialne poparcie i aproba ze strony rządu są składową oddziaływania inicjatywy GSOL i umożliwiły współpracę z wieloma największymi brytyjskimi organizacjami non-profit jak również z Directgov. Należą do nich Business Links, Citizens Advice i UK Online.


Nowy Urząd ds. Przestępczości Zorganizowanej – SOCA (który przejął funkcje Państwowej Jednostki ds. Przestępczości w zakresie Najnowszej Technologii

oraz różnych innych organizacji) był aktywnym zwolennikiem GSOL i przewodniczył Grupie Nadzorczej GSOL w okresie 2006-2007.

Wkład organizacji wspierających bardzo pomógł w rozpowszechnieniu wiadomości na zasadzie wzajemnego wsparcia, np. wspólnych publikacji prasowych z ABTA (Stowarzyszeniem Brytyjskich Biur Podróży) czy śniadań służbowych dla członków brytyjskich Izb Handlowych. GSOL będzie współpracować z organizacjami członkowskimi i konsumenckimi przez następnych 12 miesięcy w celu dostarczenia wiadomości swoim odbiorcom w sposób bardziej wydajny i skuteczny.

Przykład działalności sponsorów



You first  **Lloyds TSB**

Personal banking | Business banking | Corporate banking | Private Banking | Car, Home utilities and travel

Internet banking | Current accounts | Savings | Credit cards | Loans | Mortgages | Insurance | Pensions & Investments | Sharedealing

> Security > Get Safe Online

Get Safe Online

Expert advice for everyone

If you've used the internet, you may have received unwanted emails or intrusive pop up adverts. Perhaps your computer has been the victim of a virus attack or you've had experience with a fraudster trying to steal your personal details. We're here to help you put a stop to all of this.

That's why we've joined forces with the UK government, the National Hi-Tech Crime Unit and other leading businesses to create the [Get Safe Online website](#)*, a comprehensive resource for independent expert security advice.

Visit the [Get Safe Online website](#) to learn more about how to protect yourself against the growing number of online threats - [viruses](#), unwanted email, popups and [spyware](#) as well as online fraud such as [phishing](#), [pharming](#) and [identity theft](#).

You can protect yourself

The good news is that you can help protect yourself with a combination of security software, vigilance and common sense. The Get Safe Online website contains nearly 100 articles, including advice for small business owners and actions parents can take to ensure safe use of the internet. The site has been written in clear, straight-forward language, so you don't need to be a computer expert to understand it.

Visit the [Get Safe Online website](#) today.

GET SAFE ONLINE

Let us help you

[Fraud alerts](#)
Keep up-to-date on recent fraud alerts.

[Ask a question](#)
Get an instant answer from our online help centre.

[Security learning centre](#)
Learn about phishing and trojans, and try our security quick quiz.

Useful information

Help

Security

- [Using internet banking safely](#)
- [Protecting your computer](#)
- [Security software offer](#)
- [Our system security](#)
- [Security learning centre](#)
- Get Safe Online**
- [Common frauds](#)
- [Protecting your cards](#)
- [Security glossary](#)
- [Useful security links](#)
- [Enabling JavaScript](#)
- [Fraud alerts](#)
- [Rates and charges](#)
- [Ways to bank with us](#)
- [Contact us](#)
- [Lloyds TSB group sites](#)
- [About Lloyds TSB](#)

Rząd jako partner społeczeństwa

Najnowsze programy i inicjatywy poszerzania wiedzy

Zobacz części [Rząd jako twórca](#) i [Rząd jako partner \(przedsiębiorstw\)](#), aby uzyskać informacje na temat kampanii Get Safe Online. Kampania jest również skierowana do grupy Użytkowników Prywatnych.

Statystyki i i kluczowe wskaźniki wydajności (KPI)

Statystyki/KPI do oceny skuteczności inicjatywy poszerzania wiedzy

Użyto następujących statystyk do pomiaru skuteczności i wpływu marketingu, public relations i budowania marki kampanii Get Safe Online w okresie 2005-2006 i przewiduje się, że będą one nadal wykorzystywane w nowym roku finansowym zaczynającym się w lipcu 2006 roku.

- Jakościowe i ilościowe badania rynku poświęcone zmianie działania
- Możliwości analizy mediów drukowanych i radiowo-telewizyjnych
- Tendencje w ruchu na stronie internetowej z uwzględnieniem korzystania z treści na stronach zewnętrznych firm i organizacji
- Odsyłacze do GSOL na stronach internetowych zewnętrznych organizacji i firm
- Udział organizacji partnerskich w działaniach promocyjnych

Podsumowanie osiągnięć i wpływu

Okres wdrażania inicjatywy październik – grudzień 2005. Kontrolna grupa 500 respondentów – całkowita liczba uczestników - 1617.

33% respondentów wiedziało o kampanii lub logo w jednomiesięcznym okresie wdrażania inicjatywy

- 62% uznało, że konieczne jest zachowanie ostrożności w czasie korzystania z Internetu
- 52% uznało za swój obowiązek zachowanie bezpieczeństwa
- 52% miało świadomość potencjalnych zagrożeń
- 40% stwierdziło, że zachęcono ich do tego, by dowiedzieć się czegoś więcej

Świadomość zagrożeń takich jak keylogging i phishing wzrosła odpowiednio o 15 i 12 punktów. Zmiana zachowania respondentów była najbardziej widoczna w przypadku kopii bezpieczeństwa danych: 75% po kampanii w porównaniu z 53% przed kampanią.

- Po przeprowadzonej kampanii:
- zaistniały większe szanse, że respondenci zainstalują w swoich komputerach zaporę sieciową lub oprogramowanie antyspyware
- było dużo bardziej prawdopodobne, że respondenci będą tworzyć kopie bezpieczeństwa
- respondenci byli dużo bardziej skłonni do nieudostępniania danych osobowych
- pojawiły się dużo większe szanse, że respondenci będą regularnie używać i aktualizować narzędzia antywirusowe i antyspyware

Przeciwwstawne wskaźniki

19% respondentów poczuło się mniej pewnie, gdy uświadomili sobie potencjalne zagrożenia, podczas gdy 24% poczuło się bardziej pewnie dzięki poszerzonej wiedzy i upewnieniu się, że postępują właściwie.

Ruch na stronie internetowej i wyniki związane ze stroną internetową

W okresie wdrażania inicjatywy zarejestrowano 114 000 odwiedzin na stronie, a wszystkie kolejne działania z zakresu marketingu i public relations wykazują jasny i konsekwentny związek z pokoleniem web traffic (ruch w sieci). Przewiduje się, że liczba odwiedzających osiągnie około 500 tysięcy przed październikiem 2006 – znaczące osiągnięcie jak na rozpoczynającą się promocję niepowiązaną z produktem lub usługą w przeciągu dwunastu miesięcy.

Obecnie liczba odwiedzających w skali roku osiąga poziom 282 000 przed podjęciem jakiegokolwiek istotnego działania marketingowego. Planuje się, że liczba ta wzrośnie dziesięciokrotnie dzięki kolejnym ulepszeniom takim jak optymalizacja wyszukiwarki czy dodatkowa działalność promocyjna związana ze stronami sponsorów.

www.getsafeonline.org pojawia się na ponad 13 000 aktywnych stron internetowych, które odsyłają bezpośrednio do tej strony. Wynik ten jest bardzo korzystny w porównaniu z alternatywnymi stronami oferującymi informacje:

- 450 w przypadku www.banksafeonline.org
- 260 w przypadku www.besafeonline.org
- 92 w przypadku www.staysafeonline.org

Kampanie

Walijski program poszerzania wiedzy w zakresie e-przestępczości

Szczyt poświęcony e-przestępczości w Walii jest dowodem na zobowiązanie się Walijskiego Zgromadzenia Narodowego, czterech departamentów walijskich sił policyjnych, Walijskiego Urzędu ds. Rozwoju, Morgan Cole oraz Państwowej Jednostki ds. Przestępczości z wykorzystaniem Zaawansowanej Technologii (NHTCU) do rozpoczęcia programu obejmującego kształcenie, inwestycje i wsparcie, który

zachęci nowe pokolenie firm do budowania bezpiecznych i odpornych na przestępczość fundamentów gospodarczej przyszłości Walii.

Szczyt poświęcony e-przestępczości

Ponad 200 przedstawicieli różnych przedsiębiorstw i organizacji uczestniczyło w Szczycie 2006. Na szczycie tym przedstawiono manifest oraz projekt trzyletniego Planu Działania dotyczącego ochrony organizacji przed przestępczością w Internecie, a także opisano praktyczne kroki, jakie należy podjąć, aby zapewnić sukces tego planu wśród odpowiedzialnych organów.

Uczestnicy otrzymali aktualne instrukcje i informacje od wyższych rangą przedstawicieli firmy Microsoft, NHTCU, Morgan Cole i HSBC dotyczące skali i charakteru tego bardzo realnego zagrożenia dla przedsiębiorstw.

Jeszcze ważniejsze jest to, że delegaci dowiedzieli się, jakie propozycje zawarte są w manifestie, jeśli chodzi o sposób wspierania i ochrony Walii przed cyberprzestępcstwami poprzez profesjonalne porady, poszerzanie wiedzy, wymianę informacji, zaostrzone procedury i nadzór.

Aby uzyskać więcej informacji o szczycie, zobacz:

http://www.wda.co.uk/index.cfm/technology_and_innovation/mtp/partner_programme/ecrime/en8118

Aby zdobyć kopię manifestu, zobacz http://www.wda.co.uk/resources/E-Crime_Wales_Manifesto_Final2.pdf

Aby zdobyć kopię Planu Działania, zobacz [e-crime wales action plan final2.pdf](#)

SaferInternet - Internet Safety Zone (artykuł)²⁶

Streszczenie

InternetSafetyZone.com to portal one-stop-shop zawierający holistyczne porady dotyczące bezpieczeństwa w Internecie dla rodziców, nauczycieli i dzieci. Opracowywano go przez ponad rok na Wydziale Badań Cyberprzestrzeni, University of Central Lancashire (UCLAN) – brytyjskim węźle UE i partnerze koordynującym w projekcie ISCA.

Szczegóły

²⁶ <http://www.saferInternet.org/www/en/pub/insafe/news/articles/0706/uk1.htm> , 1 sierpnia 2006.

Portal Internet Safety Zone (ISZ) oferuje obszerne informacje na różne tematy, np.: zasady działania Internetu, e-mail, chat, natychmiastowe przesyłanie komunikatów i sieć społeczna (social networking). Zagadnienia te omówione są od strony technicznej (na przykład, jak powstaje, jak jest przekazywany i otrzymywany e-mail), ale również z perspektywy bezpieczeństwa w Internecie (np. jakie są potencjalne zagrożenia dla dzieci korzystających z chatroomów?). Użytkownicy mogą przeglądać zarówno bardziej ogólne jak i bardziej szczegółowe informacje.

Ponadto ISZ ma na celu zapewnienie holistycznego podejścia do bezpieczeństwa w Internecie poprzez omawianie zagadnień z zakresu tzw. „cyberwellness” (dobrego samopoczucia przy korzystaniu w Internetu). W portalu szczegółowo omówiono zagadnienia takie jak rasizm, prawa człowieka, samookaleczenie, samobójstwo i zaburzenia odżywiania. Zachęca się dzieci do wyrobienia w sobie krytycznego spojrzenia na korzystanie z Internetu i uświadomienia sobie, że nie wszystko, co widzą w Internecie, jest „prawdą”.

Treść portalu ISZ została zgromadzona i napisana w ramach współpracy wielu organizacji, w celu opracowania najlepszej praktyki. Rzeczywiście wiele organizacji takich jak AOL, BBC, Becta, Childnet, Internet Watch Foundation (IWF), Microsoft, NSPCC, O2, Vodafone, policja i Virtual Global Taskforce (VGT) pomogły w udzielaniu porad i wskazówek zarówno dla rodziców jak i dzieci korzystających z internetowych i komórkowych technologii informacyjnych.

Twórcy ISZ wysłuchali również krytycznych komentarzy skierowanych pod adresem wielu portali w węzle UE, stwarzając odpowiednie warunki do zgłaszania problemów związanych z bezpieczeństwem w Internecie. Ze strony głównej użytkownicy mogą za pomocą jednego kliknięcia przejść do stron zawierających odpowiednie informacje i odsyłacze do organizacji, w których można zawiadamiać o problemach. Przykładem jest ikona „report abuse icon” związana z problemem wykorzystywania dzieci przez Internet, która przenosi użytkowników na stronę zawierającą jasne informacje o tym, że mogą oni zgłosić problem wykorzystywania dzieci do IWF oraz o tym, jak mogą to zrobić.

Ponadto ISZ oferuje pojedynczym osobom lub całym grupom przekazywanie informacji bezpośrednio na ich komputery osobiste, gdy udostępniane są nowe treści. Przy każdym zagadnieniu znajduje się odsyłacz RSS, który umożliwia indywidualnemu użytkownikowi lub organizacji korzystanie z treści w sposób otwarty i elastyczny: pojedyncze osoby mogą otrzymywać aktualizacje bezpośrednio w swojej skrzynce elektronicznej/ czytniku RSS, natomiast organizacje mogą wyświetlać najnowsze informacje na swoich własnych stronach internetowych/portałach poprzez przyłączenie „okna” RSS do swojej strony internetowej.

Jest to kluczowy aspekt ISZ – umożliwienie innym organizacjom rozpowszechnianie porad dotyczących bezpieczeństwa w Internecie w szybki i prosty sposób wśród tych, którzy na co dzień mogą nie mieć styczności z tym zagadnieniem. Ponadto umożliwia to



Poradnik dla użytkowników: Jak poszerzyć wiedzę o bezpieczeństwie informacji

portalowi ISZ, a poprzez ISZ – kwestii bezpieczeństwa dziecka w Internecie, dotarcie do znacznie większej rzeszy odbiorców.

Zobacz <http://www.Internetsafetyzone.co.uk>, aby odwiedzić Internet Safety Zone

Dobre praktyki w grupach docelowych

Użytkownik prywatny

Obecna sytuacja

Użytkownik prywatny bardzo często stanowi grupę docelową większości inicjatyw poszerzających wiedzę na temat bezpieczeństwa informacji, podejmowanych w państwach członkowskich. Głównymi odbiorcami są zazwyczaj ludzie młodzi i dorośli; do starszych użytkowników inicjatywy kierowane są rzadziej. Do przekazywania wiadomości dotyczących bezpieczeństwa wykorzystywane są różne kanały komunikacyjne, wśród których najbardziej popularne to portale, imprezy publiczne, komiksy i media (np. telewizja).

Dobre praktyki w poszczególnych krajach

Austria

Obecnie główną grupą docelową Inicjatywy SaferInternet.at, mającej na celu zwiększenie bezpieczeństwa w związku z korzystaniem przez małoletnich z Internetu i telefonów komórkowych, są rodzice. W celu uzyskania dalszych informacji, kliknij poniższy odsyłacz, aby przejść do szczegółów o [Austrii](#) w części *Dobre praktyki w poszczególnych krajach*.

Belgia

W Belgii, gdy dzieci osiągają wiek 12 lat, otrzymują elektroniczną kartę identyfikacyjną z komiksem opowiadającym o bezpieczeństwie w Internecie. Dostają również czytnik kart elektronicznych, który umożliwia im bezpieczne chatowanie na pewnych, wcześniej określonych stronach. W celu uzyskania dalszych informacji, kliknij poniższy odsyłacz, aby przejść do szczegółów o [Belgii](#) w części *Dobre praktyki w poszczególnych krajach*.

Na fikcyjnej stronie internetowej operatora telefonii komórkowej znajduje się propozycja bezpłatnej subskrypcji na usługi takie jak telefony komórkowe, SMS i e-mail. Jest ona skierowana głównie do młodzieży; aby się zarejestrować, surfer musi wprowadzić dane osobowe. Strona wyświetla wiadomość, że operator ten nie istnieje i przenosi surfersa na inną stronę zawierającą szczegóły dotyczące bezpieczeństwa informacji. W celu uzyskania dalszych informacji, kliknij poniższy odsyłacz, aby przejść do szczegółów o Belgii w części *Dobre praktyki w poszczególnych krajach*.

Dania

Doroczna kampania Net-safe now! ma na celu poszerzanie wiedzy z zakresu bezpieczeństwa IT i promowanie bezpieczniejszego zachowania w Internecie. Kampania skierowana jest do różnych grup, prowadzona jest na zasadzie współpracy

wielu partnerów i wykorzystuje się w niej różne kanały do przekazywania wiadomości. W celu uzyskania dalszych informacji, kliknij poniższy odsyłacz, aby przejść do szczegółów o [Danii](#) w części *Dobre praktyki w poszczególnych krajach*.

Aby uzyskać więcej informacji na temat inicjatyw poszerzania wiedzy takich jak „Youth Ring”, która jest owocem współpracy pomiędzy ośrodkami i klubami młodzieżowymi, kliknij następujący odsyłacz, aby przejść do szczegółów zawartych w części *Dobre praktyki w poszczególnych krajach* poświęconej Danii.

Finlandia

W Finlandii dostarczono do ponad 1 miliona domów Poradnik na temat bezpiecznego korzystania z Internetu (Joka Kodin Tietoturvaopas). Uzupełniającym elementem inicjatywy była strona internetowa. W celu uzyskania dalszych informacji, kliknij poniższy odsyłacz, aby przejść do szczegółów o [Finlandii](#) w części *Dobre praktyki w poszczególnych krajach*.

Innymi inicjatywami poszerzania wiedzy podejmowanymi w Finlandii są: podręcznik *Hiiripiiri* (rozprowadzany wśród dzieci szkolnych w ramach programu nauczania, z dostępną certyfikacją), Dzień Bezpiecznego Internetu, komiksy dla dzieci i współpraca z dostawcami treści. W celu uzyskania dalszych informacji, kliknij poniższy odsyłacz, aby przejść do szczegółów o [Finlandii](#) w części *Dobre praktyki w poszczególnych krajach*.

Francja

W ramach inicjatywy mającej na celu poszerzanie wiedzy wśród młodzieży francuska Rada Ministrów wraz z przedsiębiorcami i społeczeństwem, z uwzględnieniem ISP, rozpoczęła kampanię wykorzystującą wiele kanałów komunikacyjnych, w tym krótkie filmy w telewizji. W celu uzyskania dalszych informacji, kliknij poniższy odsyłacz, aby przejść do szczegółów o [Francji](#) w części *Dobre praktyki w poszczególnych krajach*.

Niemcy

Rząd Federalny kieruje inicjatywy poszerzania wiedzy do ludzi na wszystkich poziomach. Wykorzystywane są różne materiały i narzędzia w celu informowania i wspierania użytkowników-amatorów. Użytkownicy prywatni mogą również złożyć wnioski o usługi ostrzegawcze. W celu uzyskania dalszych informacji, kliknij poniższy odsyłacz, aby przejść do szczegółów o [Niemczech](#) w części *Dobre praktyki w poszczególnych krajach*.

Grecja

W ramach węzła Insafe, inicjatywa SafeNetHome przewidziana jest jako demaskatorska kampania poszerzania wiedzy wśród różnych grup docelowych, lecz zwłaszcza wśród

dzieci i młodzieży. W celu uzyskania dalszych informacji, kliknij poniższy odsyłacz, aby przejść do szczegółów o [Grecji](#) w części *Dobre praktyki w poszczególnych krajach*.

Węgry

Dotychczas Rząd i stowarzyszenia obywatelskie podejmowały różne inicjatywy oparte na współpracy i mające na celu poszerzanie wiedzy z zakresu ochrony użytkowników prywatnych i społeczeństwa (z uwzględnieniem MŚP). W celu uzyskania dalszych informacji, kliknij poniższy odsyłacz, aby przejść do szczegółów o [Węgrzech](#) w części *Dobre praktyki w poszczególnych krajach*.

Islandia

Projekt SAFT, skierowany głównie do młodzieży, ale w pewnym stopniu również do rodziców jako kanału służącego do komunikacji z młodymi ludźmi, podjął na kilku frontach pracę mającą na celu poszerzanie wiedzy. Użyto wiele różnych kanałów, w tym broszury, ankiety, animowane reklamy, artykuły w gazetach, blogatony i konferencje. W kampaniach wykorzystano różne środki przekazu i poruszono takie kwestie jak bezpieczeństwo telefonów komórkowych, gry komputerowe, a także bezpieczne i etyczne korzystanie z Internetu. W celu uzyskania dalszych informacji, kliknij poniższy odsyłacz, aby przejść do szczegółów o [Islandii](#) w części *Dobre praktyki w poszczególnych krajach*.

Włochy

Projekt, skierowany głównie do osób dorosłych, ma na celu wypełnienie luki pomiędzy poziomem wiedzy obywateli a nowymi technologiami, którą odnotowano w ramach innych trwających projektów. Projekt będzie miał formę kursu edukacyjnego, ogólnie dostępnego z sieciowych portali organizacji instytucjonalnych. Istnieją ponadto plany poszerzania wiedzy wśród pracowników MŚP poprzez seminaria, naukę przez Internet oraz media, na przykład telewizję. W celu uzyskania dalszych informacji, kliknij poniższy odsyłacz, aby przejść do szczegółów o [Włoszech](#) w części *Dobre praktyki w poszczególnych krajach*.

Litwa

Na Litwie zaplanowano lub przeprowadzono już szereg inicjatyw mających na celu poszerzenie wiedzy całego społeczeństwa. W inicjatywach tych wykorzystano fora dyskusyjne, artykuły, broszury, a także inne narzędzia. W celu uzyskania dalszych informacji, kliknij poniższy odsyłacz, aby przejść do szczegółów o [Litwie](#) w części *Dobre praktyki w poszczególnych krajach*.

Luksemburg

Podjęto i nadal podejmuje się szereg inicjatyw mających na celu poszerzenie wiedzy wśród obywateli. Konkretnie wiadomości przekazywane są tej grupie docelowej poprzez różne kanały informacyjne, np. tzw. flash movies, portale internetowe czy też imprezy objazdowe (road shows). W celu uzyskania dalszych informacji, kliknij poniższy odsyłacz, aby przejść do szczegółów o [Luksemburgu](#) w części *Dobre praktyki w poszczególnych krajach*.

Malta

Podjęto szereg inicjatyw skierowanych do dzieci, rodziców i osób starszych. Miały one zazwyczaj postać ankiet, kursów i publikacji. W celu uzyskania dalszych informacji, kliknij poniższy odsyłacz, aby przejść do szczegółów o [Malcie](#) w części *Dobre praktyki w poszczególnych krajach*.

Holandia

Podjęto szereg inicjatyw skierowanych do użytkowników prywatnych. Wykorzystano w nich następujące kanały: targi, strony internetowe, wydarzenia polegające na wymianie doświadczeń, materiały, np. broszury, i imprezy publiczne. W celu uzyskania dalszych informacji, kliknij poniższy odsyłacz, aby przejść do szczegółów o [Holandii](#) w części *Dobre praktyki w poszczególnych krajach*.

Norwegia

W Norwegii podjęto publiczno-prywatną inicjatywę obejmującą dostawców usług internetowych, mającą na celu stworzenie strony internetowej przeznaczonej dla ogółu społeczeństwa. Na stronie tej znajdują się informacje, porady oraz wskazówki dotyczące bezpiecznego korzystania z Internetu. Zawartość strony jest usystematyzowana według tematów i kategorii. W celu uzyskania dalszych informacji, kliknij poniższy odsyłacz, aby przejść do szczegółów o [Norwegii](#) w części *Dobre praktyki w poszczególnych krajach*.

Polska

Pod nadzorem ministerstwa oraz przy współpracy z innymi organami, wdrożono szereg projektów skierowanych do użytkowników prywatnych i MŚP. Główne kanały komunikacyjne, jakie wykorzystano w działaniach, to strony internetowe, infolinie oraz imprezy publiczne. Do współpracy w zakresie niektórych kwestii związanych z bezpieczeństwem IT zaproszono również dostawców usług internetowych. W celu uzyskania dalszych informacji, kliknij poniższy odsyłacz, aby przejść do szczegółów o [Polsce](#) w części *Dobre praktyki w poszczególnych krajach*.

Portugalia

Podjęto szereg inicjatyw mających na celu poszerzenie wiedzy, skierowanych do użytkowników prywatnych, MŚP oraz władz lokalnych. Inicjatywy te obejmowały

głównie szkolenie i imprezy publiczne oraz opierały się na współpracy. W celu uzyskania dalszych informacji, kliknij poniższy odsyłacz, aby przejść do szczegółów o [Portugalii](#) w części *Dobre praktyki w poszczególnych krajach*.

Słowenia

Najważniejsze inicjatywy koncentrowały się na poszerzaniu wiedzy wśród użytkowników prywatnych (zwłaszcza młodych). Wykorzystano w nich różne kanały, np. strony internetowe, sesje szkoleniowe, imprezy publiczne i infolinie. W celu uzyskania dalszych informacji, kliknij poniższy odsyłacz, aby przejść do szczegółów o [Słowenii](#) w części *Dobre praktyki w poszczególnych krajach*.

Szwecja

W Szwecji miały lub mają miejsce różne inicjatywy mające na celu poszerzenie wiedzy, skierowane do użytkowników prywatnych, MŚP oraz władz lokalnych. Przykładem takich inicjatyw jest projekt realizowany przez Państwowy Urząd Pocztowy i Telekomunikacyjny, w którym - oprócz innych kanałów – wykorzystuje się interaktywne strony internetowe oraz publikacje. Ponadto, warto wspomnieć o projekcie SurfaLugnt, utworzonym przy współpracy z sektorem IT i właściwymi organami. Inna inicjatywa, podjęta przez Sztokholm, obejmowała nakręcenie filmu dla pracowników sektora publicznego dotyczącego roli, jaką ci pracownicy odgrywają w społeczeństwie. Film ten zawierał również wskazówki dotyczące bezpieczeństwa. W celu uzyskania dalszych informacji, kliknij poniższy odsyłacz, aby przejść do szczegółów o Szwecji w części *Dobre praktyki w poszczególnych krajach*.

Prowadzone są również regionalne seminaria mające na celu rozpowszechnianie wiedzy o bezpiecznym korzystaniu z Internetu. Seminaria te skierowane są głównie do nauczycieli, ale obejmują też inne zawody opierające się na pracy z dziećmi. Jedno z bardziej owocnych działań polega na tworzeniu zespołów młodzieżowych, które dzielą się informacjami o tym, jak młodzi ludzie korzystają z mediów i jak je postrzegają. W celu uzyskania dalszych informacji, kliknij poniższy odsyłacz, aby przejść do szczegółów o [Szwecji](#) w części *Dobre praktyki w poszczególnych krajach*.

Wielka Brytania

W Wielkiej Brytanii podjęto kilka inicjatyw mających na celu poszerzenie wiedzy, skierowanych do użytkowników prywatnych, MŚP oraz władz lokalnych. Do przekazywania informacji wykorzystano następujące kanały: strony internetowe, imprezy publiczne, ogólnokrajowe media (takie jak telewizja i radio) oraz imprezy objazdowe dla sektora publicznego. Programy rozwojowe, takie jak CSIA, również mają na celu poszerzanie wiedzy na poziomie władz państwowych i lokalnych. W celu uzyskania dalszych informacji, kliknij poniższy odsyłacz, aby przejść do szczegółów o [Wielkiej Brytanii](#) w części *Dobre praktyki w poszczególnych krajach*.

InternetSafetyZone.com to portal one-stop-shop służący do udzielania obywatelom porad o charakterze holistycznym, dotyczących bezpieczeństwa w Internecie. Treść tego portalu gromadzona jest i tworzona wspólnie z wieloma organizacjami. Surfowanie na tej stronie nie przysparza trudności, a ponadto zawiera ona łatwą w obsłudze funkcję zgłaszania incydentów. W celu uzyskania dalszych informacji, kliknij poniższy odsyłacz, aby przejść do szczegółów o [Wielkiej Brytanii](#) w części *Dobre praktyki w poszczególnych krajach*.

Dobre praktyki w innych organizacjach

FORTH

Przez ostatnich kilka lat firma EKATO (<http://www.ekato.gr>) prowadziła grecki projekt na skalę krajową mający na celu poszerzanie wiedzy z zakresu bezpieczeństwa w Internecie. Zdjęcie ekranu przedstawiającego stworzony portal można zobaczyć poniżej. Aby uzyskać więcej informacji, zobacz www.saferInternet.gr



Krajowy miesiąc poszerzania wiedzy o cyberbezpieczeństwie (NCSAM) 2005 w Stanach Zjednoczonych

Drugi rok z rzędu sektor publiczny i prywatny połączył siły, aby zorganizować Krajowy miesiąc poświęcony wiedzy o cyberbezpieczeństwie, krajową inicjatywę opartą na współpracy i mającą na celu kształcenie użytkowników Internetu w każdym wieku w zakresie bezpiecznych praktyk internetowych. NCSA (National Cyber Security Alliance) z przyjemnością informuje, że inicjatywa ta odniosła w 2005 roku duży sukces. Szacuje się, że w październiku w ramach tej inicjatywy dzięki relacjom środków przekazu oraz państwowym i lokalnym imprezom komunikaty NCSA dotarły do ponad 70 milionów konsumentów. W wyniku tych działań z udziałem mediów ruch na stronie internetowej NCSA zwiększył się o ponad 300% na przełomie września i października, osiągając wynik 114,992 wizyt na stronie w październiku – przewidywana liczba 100 000 odwiedzin na stronie w skali miesiąca została przekoczona o 14%, a jednocześnie była to rekordowa liczba odwiedzin w skali miesiąca na stronie staysafeonline.org.

Powyższe wyniki obrazują, w jakim stopniu zrealizowano cele przyjęte na tamten miesiąc, głównie, jeśli chodzi o:

- Poszerzenie wiedzy na temat bezpieczeństwa w Internecie i National Cyber Security Alliance wśród wyznaczonych kluczowych odbiorców – użytkowników prywatnych, MŚP i środowiska edukacyjnego.
- Promowanie bezpiecznych praktyk w zakresie korzystania z Internetu wśród kluczowych odbiorców, a także w innych grupach.

Aby osiągnąć wyżej wspomniane cele, NCSA i partnerzy rozpoczęli wieloaspektową kampanię edukacyjną dla konsumentów, która obejmowała następujące elementy:

- Kampanię z wykorzystaniem relacji środków przekazu informujących o Krajowym miesiącu poszerzania wiedzy o cyberbezpieczeństwie. W kampanii tej położono nacisk na relacje telewizyjne jako sposób na stworzenie „efektu domino” medialnego rozmachu, który miał objąć w październiku wszystkich docelowych odbiorców.
- Ogłoszenie telewizyjne wspomagające relacje mediów i zapewniające NCSA dodatkowy kanał przekazywania wiedzy.
- Wielorakie imprezy na poziomie krajowym i lokalnym, które umożliwiły oddolnie zainicjowane forum, na którym można było wyjaśniać zagadnienia związane z bezpieczeństwem w Internecie i pouczać ludzi o bezpiecznym zachowaniu w Internecie
- Kulminacją wszystkich działań było wezwanie do odwiedzenia strony www.staysafeonline.org w celu uzyskania dalszych informacji, w tym wskazówek dotyczących zwiększenia w maksymalnym stopniu bezpieczeństwa w Internecie. Aby zagwarantować pozytywne wrażenia konsumentów, zmieniono projekt strony internetowej tak, by była łatwiejsza w użyciu, bardziej atrakcyjna wizualnie

oraz by zawierała wyczerpujące informacje i odsyłacze do dodatkowych stron poza NCSA.

Osiągnięcia Krajowego miesiąca poszerzania wiedzy o cyberbezpieczeństwie były naprawdę imponujące i są zdecydowanie lepsze od wyników osiągniętych w roku inauguracyjnym 2004. Niemniej jednak jest wiele sposobów, dzięki którym możemy odnieść jeszcze większy sukces w 2006 roku. Wstępne zalecenia są następujące:

- *Zapewnienie zatwierdzenia wszystkich stron zainteresowanych i oddolnie organizowanych imprez odpowiednio wcześniej.* Mimo że plan dotyczący NCSAM przedłożono w lipcu, na trzy tygodnie przed początkiem października wciąż trwały dyskusje i podejmowano decyzje dotyczące rzeczników, strategii działania itd. Każdy kolejny etap narad wymagał wielu uczestników oraz poświęcenia cennego czasu, co ostatecznie opóźniło tournée mediów satelitarnych, kluczowego elementu NCSAM. Ponadto wiele lokalnych imprez rynkowych/oddolnych wciąż było finalizowanych (lub w niektórych przypadkach – odwoływanych) w połowie września, co powodowało niejasność w związku z zakresem i poziomem zasobów PR, które miały być przeznaczone na te działania. Ostatecznie wszystko powiodło się, ale mamy nadzieję, że w przyszłym roku wszystkie strony zainteresowane wezmą udział w procesie planowania i zatwierdzania, aby zatwierdzony plan był gotowy do realizacji przed połową sierpnia i aby w końcowym etapie dokonywane były niewielkie korekty strategii.
- *Stworzenie bardziej atrakcyjnego przesłania.* Największe wyzwanie, jakie stoi przed NCSA jest takie, aby problem bezpieczeństwa w Internecie był często omawiany w mediach, a wynik końcowy jest zazwyczaj taki, że różne jednostki udzielają różnych wskazówek odnośnie używania oprogramowania antywirusowego, zapór sieciowych, itd. Chociaż tegoroczna kampania skupiająca się na kradzieży tożsamości osiągnęła dobre wyniki, uważamy, że można było osiągnąć więcej i zapewnić relację mediów o świeżym i nowym śmiałym podejściu. Sądzymy, że konkretna kampania może nigdy nie doprowadzić do zgody pomiędzy stronami zainteresowanymi NCSA, ale mamy nadzieję, że w przyszłym roku zrealizujemy kampanię, w ramach, której zostanie podjęte większe ryzyko i będzie promowane stanowisko charakterystyczne tylko dla NCSA.
- *Zapewnienie koniecznych narzędzi medialnych i/lub szybkie reagowanie na możliwości, jakie dają media.* Chociaż NCSAM jest szlachetną sprawą, w rzeczywistości jest to impreza poświęcona przekazywaniu wiadomości; nie jest natomiast wiadomością sama w sobie lub o sobie. Dlatego też ważne jest, aby w czasie trwania NCSAM przekazywać nowe informacje w postaci studium lub sponsorować program, o którym warto przekazywać informacje.

Zobacz [us national cyber security awareness month 2005 summary 2.pdf](#) w części *Pliki Źródłowe*, aby uzyskać więcej informacji o tej kampanii w Stanach Zjednoczonych.

MŚP

Obecna sytuacja

Działania skierowane do grupy docelowej MŚP dotyczą najczęściej inicjatyw związanych z poszerzaniem wiedzy na terenie państw członkowskich, chociaż wydaje się, że to użytkownicy prywatni są w tym przypadku traktowani priorytetowo. Główną grupą odbiorców w MŚP są raczej pracownicy szeregowi, jednakże informacje mogą być również wykorzystywane przez inne kategorie pracowników MŚP. Wykorzystywane są popularne kanały dotarcia do odbiorców, w tym szkolenia, seminaria oraz zasoby online.

Wyniki ankiety przeprowadzonej przez firmę Trend Micro, lidera w dziedzinie programów antywirusowych i bezpieczeństwa zawartości, wskazują, że niektórzy użytkownicy końcowi działający w otoczeniu gospodarczym, częściej byli skłonni do podejmowania ryzykownych działań w sieci, gdy korzystali z komputera w pracy, niż w domu.²⁷

- Studium, przeprowadzone w lipcu 2005 r., objęło ponad 1.200 firmowych użytkowników Internetu ze Stanów Zjednoczonych, Niemiec i Japonii, którzy udzieli odpowiedzi na pytania zawarte w ankiecie online. Spośród wielu wniosków, nasuwających się po przeprowadzeniu ankiety, najważniejsze są prawdopodobnie te, które dotyczą współzależności pomiędzy obecnością działu IT, a przekonaniem użytkowników końcowych, że komputery są zabezpieczone przed niepożądanym działaniem wirusów, robaków, oprogramowania typu spyware, spamu, phishingu i pharmingu (skutkiem tego rodzaju przekonania było często podejmowanie ryzykownych działań, które mogą mieć potencjalnie negatywny wpływ na realizację zadań IT w zakresie ochrony komputerów przed coraz mniej przewidywalnymi zagrożeniami)
- 39% firmowych użytkowników Internetu stwierdziło, że IT jest w stanie ochronić ich przed takimi zagrożeniami jak oprogramowanie typu spyware i phishing. Przekonanie to spowodowało, że respondenci podejmowali bardziej ryzykowne działania w sieci. Spośród tych respondentów, którzy podejmowali bardziej ryzykowne działania w sieci, 63 % przyznało, że są znacznie bardziej spokojni, klikając na podejrzane linki, czy też odwiedzając podejrzane strony internetowe, wiedząc, że dział IT zainstalował w ich komputerach oprogramowanie ochronne. 40 % respondentów, którzy przyznali się do podejmowania bardziej ryzykownych działań w sieci stwierdziło, że czyni tak dlatego, iż w przypadku pojawienia się jakichkolwiek problemów mogą liczyć na wsparcie ze strony działu IT.

Dobre praktyki w poszczególnych krajach

Austria

²⁷ <http://www.trendmicro.com/en/about/news/pr/archive/2005/pr091305.htm>

Inicjatywa IT-Safe skierowana jest przede wszystkim do małych przedsiębiorstw, w szczególności do MPŚ, zatrudniających maksymalnie 25 pracowników. W ramach inicjatywy prowadzone są specjalne działania doradcze, których poziom jest uzależniony od wiedzy beneficjentów i struktury informatycznej przedsiębiorstw. Wydano ponadto specjalny podręcznik dla przedsiębiorstw, a także udostępniono oprogramowanie, opracowane przez firmy prowadzące działalność w zakresie bezpieczeństwa danych. W celu uzyskania dalszych informacji kliknij poniższy odsyłacz, aby przejść do szczegółów o [Austrii](#) w części *Dobre praktyki w poszczególnych krajach*

Czechy

Czeskie ministerstwo oraz firma Microsoft podjęły wspólne działania mające na celu promocję bezpieczeństwa informacji wśród MŚP. W celu uzyskania dalszych informacji kliknij poniższy odsyłacz, aby przejść do szczegółów o [Czechach](#) w części *Dobre praktyki w poszczególnych krajach*

Dania

Coroczna kampania pod hasłem „Net-safe now!” miała na celu poszerzenie wiedzy na temat bezpieczeństwa IT i bezpiecznego poruszania się po Internecie. Kampania, skierowana do wielu grup, została przeprowadzona we współpracy z licznymi partnerami, a w trakcie jej realizacji wykorzystano różnorodne kanały informacyjne. W celu uzyskania dalszych informacji kliknij poniższy odsyłacz, aby przejść do szczegółów o [Danii](#) w części *Dobre praktyki w poszczególnych krajach*

Finlandia

W ramach Krajowego Dnia Bezpieczeństwa Informacji 2006, uruchomiono usługę online skierowaną do MŚP, w której przedstawiono w kompleksowy sposób problem bezpieczeństwa informacji. Usługa ta ma charakter przewodnika i jest w szczególności skierowana zarówno do pracodawców, jak i pracowników. W celu uzyskania dalszych informacji kliknij poniższy odsyłacz, aby przejść do szczegółów o [Finlandii](#) w części *Dobre praktyki w poszczególnych krajach*

Niemcy

Rząd Federalny podjął działania skierowane do wszystkich grup społecznych. Ich celem jest poszerzanie wiedzy na temat bezpieczeństwa informacji. W ramach ww. inicjatywy stworzone zostały specjalne portale internetowe dla profesjonalistów oraz podręczniki i wytyczne z zakresu bezpieczeństwa. Rząd Federalny zobowiązał się ponadto do rozpowszechniania innych informacji dotyczących bezpieczeństwa. Utworzono również liczne partnerstwa publiczno-prywatne, zrzeszające różnego rodzaju organizacje. W celu uzyskania dalszych informacji kliknij poniższy odsyłacz, aby przejść do szczegółów o [Niemczech](#) w części *Dobre praktyki w poszczególnych krajach*.

Węgry

Rząd Węgier oraz środowiska społeczne podjęły współpracę w zakresie poszerzania wiedzy na temat ochrony użytkowników prywatnych, a także pozostałej części społeczeństwa (także MŚP). W celu uzyskania dalszych informacji kliknij poniższy odsyłacz, aby przejść do szczegółów o [Węgrzech](#) w części *Dobre praktyki w poszczególnych krajach*.

Irlandia

Inicjatywy w zakresie poszerzania wiedzy podjęła prywatna organizacja VigiTrust, specjalizująca się w przeprowadzaniu szkoleń dla podmiotów sektora publicznego i prywatnego. Szczegółowe informacje znajdują się w częściach *Dobre praktyki w grupach docelowych*, *Dobre praktyki w innych organizacjach* – Władze lokalne.

Włochy

Projekt, skierowany pierwotnie do osób dorosłych, miał na celu wypełnienie luki, jaka powstała pomiędzy poziomem umiejętności i kompetencji obywateli, a obecnym stanem wiedzy z zakresu nowych technologii. Istnienie ww. luki potwierdziły wyniki innych wdrożonych już projektów. Projekt będzie miał formę kursu edukacyjnego, ogólnie dostępnego za pośrednictwem portali sieciowych należących do organizacji instytucjonalnych. Istnieją ponadto plany dotyczące poszerzenia wiedzy wśród pracowników MŚP. Inicjatywy tego rodzaju byłyby realizowane poprzez organizację seminariów, wdrażanie opartych na sieci programów typu e-learning oraz wykorzystanie mediów masowych, na przykład telewizji. W celu uzyskania dalszych informacji kliknij poniższy odsyłacz, aby przejść do szczegółów o [Włoszech](#) w części *Dobre praktyki w poszczególnych krajach*.

Litwa

Zaplanowano, względnie zainicjowano, szereg inicjatyw mających na celu poszerzenie wiedzy całego społeczeństwa. Działania te obejmują wykorzystanie forów dyskusyjnych, tworzenie artykułów i broszur, a także zastosowanie innych narzędzi. W celu uzyskania dalszych informacji kliknij poniższy odsyłacz, aby przejść do szczegółów o [Litwie](#) w części *Dobre praktyki w poszczególnych krajach*.

Luksemburg

Podjęto i kontynuowano szereg inicjatyw mających na celu poszerzenie wiedzy wśród MŚP. Do grup docelowych skierowano specjalnie dostosowane komunikaty, wykorzystując przy tym różne kanały informacyjne, takie jak na przykład tzw. flash movies, portale internetowe czy też tzw. *road show*. W celu uzyskania dalszych informacji kliknij poniższy odsyłacz, aby przejść do szczegółów o [Luksemburgu](#) w części *Dobre praktyki w poszczególnych krajach*.

Malta

Stworzono różnego rodzaju kursy szkoleniowe na temat sposobów wykorzystania przez przedsiębiorstwa ICT. Materiał zaprezentowany podczas kursów odnosił się również do kwestii związanych z poszerzaniem wiedzy. W celu uzyskania dalszych informacji kliknij poniższy odsyłacz, aby przejść do szczegółów o [Malcie](#) w części *Dobre praktyki w poszczególnych krajach*.

Holandia

Podjęto inicjatywy mające na celu poszerzanie wiedzy. Przeprowadzono szereg badań ankietowych oraz wdrożono szereg programów szkoleniowych. W celu uzyskania dalszych informacji kliknij poniższy odsyłacz, aby przejść do szczegółów o [Holandii](#) w części *Dobre praktyki w poszczególnych krajach*.

Norwegia

Inicjatywa publiczno-prywatna, obejmująca dostawców usług internetowych, miała na celu stworzenie strony internetowej przeznaczonej dla MŚP. Na stronie znajdują się informacje, porady oraz wskazówki dotyczące bezpiecznego korzystania z Internetu. Zawartość strony jest usystematyzowana według określonych tematów i kategorii. W celu uzyskania dalszych informacji kliknij poniższy odsyłacz, aby przejść do szczegółów o [Norwegii](#) w części *Dobre praktyki w poszczególnych krajach*.

Polska

Pod nadzorem ministerstwa oraz we współpracy z innymi organami wdrożono szereg projektów skierowanych do użytkowników prywatnych oraz do MŚP. Główne kanały informacji, jakie wykorzystano w działaniach, to przede wszystkim strony internetowe, infolinie oraz imprezy publiczne. Do współpracy w zakresie niektórych kwestii związanych z bezpieczeństwem IT zaproszono ponadto dostawców usług internetowych. W celu uzyskania dalszych informacji kliknij poniższy odsyłacz, aby przejść do szczegółów o [Polsce](#) w części *Dobre praktyki w poszczególnych krajach*.

Szwecja

W Szwecji podjęto szereg różnorodnych inicjatyw mających na celu poszerzenie wiedzy. Niektóre z nich trwają nadal. Są one skierowane w pierwszym rzędzie do użytkowników prywatnych, MŚP oraz do władz lokalnych. Przykładem może być projekt uruchomiony przez Państwowy Urząd Poczty i Telekomunikacyjny. Projekt ten zakłada stworzenie interaktywnych stron internetowych, a także tworzenie materiałów informacyjnych i rozpowszechnianie ich za pośrednictwem różnych kanałów. Warto również wspomnieć o projekcie SurfaLugnt, utworzonym we współpracy z sektorem IT i właściwymi władzami. Inna inicjatywa, podjęta przez miasto Sztokholm, dotyczyła stworzenia filmu dla pracowników sektora publicznego dotyczącego roli, jaką ww. pracownicy odgrywają

w społeczeństwie. W filmie znalazły się również wskazówki dotyczące bezpieczeństwa. W celu uzyskania dalszych informacji kliknij poniższy odsyłacz, aby przejść do szczegółów o [Szwecji](#) w części *Dobre praktyki w poszczególnych krajach*.

Wielka Brytania

Podjęto szereg inicjatyw mających na celu poszerzenie wiedzy, skierowanych do użytkowników prywatnych, MŚP oraz do władz lokalnych. W realizacji projektu wykorzystano takie kanały informacyjne jak: strony internetowe, imprezy publiczne, media krajowe (radio i telewizja), a także tzw. *road show*, przeznaczone dla podmiotów z sektora publicznego. Również programy rozwoju, takie jak CSIA mają na celu poszerzenie wiedzy władz państwowych oraz lokalnych. W celu uzyskania dalszych informacji kliknij poniższy odsyłacz, aby przejść do szczegółów o [Wielkiej Brytanii](#) w części *Dobre praktyki w poszczególnych krajach*.

Podczas walijskiego szczytu, którego tematem przewodnim było zapobieganie przestępstwom elektronicznym, Zgromadzenie Narodowe (Welsh Assembly Government) oraz inne organizacje, zobowiązały się do wdrożenia programu kształcenia, inwestycji oraz wsparcia, których celem będzie zachęcenie MŚP do budowania bezpiecznych i odpornych na działalność przestępczą struktur. W celu uzyskania dalszych informacji kliknij poniższy odsyłacz, aby przejść do szczegółów o [Wielkiej Brytanii](#) w części *Dobre praktyki w poszczególnych krajach*.

Dobre praktyki w innych organizacjach

FORTH

Forum e-Biznesu (<http://www.ebusinessforum.gr/>) podejmuje działania związane z upowszechnianiem informacji w zakresie okołobiznesowych programów dotyczących bezpieczeństwa sieci i informacji. Chodzi tu w szczególności o takie elementy jak: płatność elektroniczna, podpis elektroniczny oraz elektroniczne metody uwierzytelniania.

Go-online.gr (<http://www.go-online.gr>) dostarcza MŚP oraz podmiotom indywidualnym informacji na temat bezpieczeństwa sieci i prywatności.

Krajowe Centrum Dokumentacji (<http://www.ekt.gr>) regularnie organizuje wydarzenia mające na celu informowanie społeczności naukowej i zawodowej w Grecji na temat możliwości finansowania i współpracy w kontekście wdrażania programów unijnych.

Partnerstwa prywatno-publiczne

MD5 (<http://www.md5sa.com>) oraz ENCODE (<http://www.encode.gr>) organizują regularnie imprezy mające na celu poszerzenie wiedzy na temat bezpieczeństwa.

Statystyki i kluczowe wskaźniki wydajności (KPI)

Safeline (<http://www.safeline.gr>), to pierwsza w Grecji infolinia na temat bezpiecznego dostępu do Internetu, dostarczająca regularnych ocen aktywności na podstawie wskaźników wydajności używanych przez infolinię w całej Europie. Do wskaźników wydajności należą m.in. takie elementy jak: dostępność, przejrzystość, stosunki z organami ścigania oraz współpraca z innymi operatorami infolinii. Na prośbę osoby zainteresowanej możliwe jest udostępnienie pełnej listy wskaźników wydajności.



Istotną kwestią jest opracowanie wspólnych wskaźników. Po opracowaniu tego rodzaju statystyk należy przedstawić je państwom członkowskim z zaleceniem, aby były stosowane przy podejmowaniu podobnych działań w przyszłości. Ma to na celu umożliwienie oceny przyszłych kampanii oraz porównanie wyników osiągniętych w różnych państwach członkowskich.

SAP

Skuteczne inicjatyw poszerzania wiedzy

Mcert został utworzony przez stowarzyszenie BITKOM, Ministerstwo Spraw Wewnętrznych, Urząd Federalnego ds. Bezpieczeństwa Informacji oraz szereg innych uprawnionych podmiotów działających w sektorze w formie partnerstwa publiczno-prywatnego. W oparciu o takie elementy jak obiektywność i niezależność producentów, Mcert dostarcza informacji na temat bezpieczeństwa IT, skierowanych w pierwszym rzędzie do małych i średnich przedsiębiorstw. Dostarczając wiarygodną i niezawodną wiedzę, Mcert udziela wsparcia MŚP w rozwiązywaniu problemów związanych z bezpieczeństwem. Klienci mają możliwość skorzystania z security advisories oraz zaleceń opracowanych dla podmiotów świadczących usługi. Aby uzyskać więcej informacji zobacz: <http://www.mcert.de/>

Bürger-CERT dostarcza społeczeństwu informacji i praktycznych porad w zakresie aktualnych kwestii związanych z bezpieczeństwem. Zainicjowany w marcu 2006r. projekt jest usługą całkowicie obiektywną oraz bezpłatną. Celem projektu Bürger-CERT

jest poszerzenie wiedzy całego społeczeństwa na temat wszechobecnego zagrożenia związanego z korzystaniem z Internetu oraz elektronicznych systemów komunikacji. Użytkownicy mają możliwość zarejestrowania się w serwisie w celu otrzymywania pocztą elektroniczną właściwych informacji. Projekt Bürger-CERT stanowi wspólne przedsięwzięcie Federalnego Ministerstwa Spraw Wewnętrznych i Niemieckiego Stowarzyszenia Mcert ds. Bezpieczeństwa IT. Aby uzyskać więcej informacji zobacz: <http://www.buerger-cert.de/>

Inicjatywa *Deutschland sicher im Netz* (DsiN)

W ramach projektu „*Mittelstand sicher im Internet*”, którego inicjatorem jest Federalny Minister Gospodarki i Pracy oraz Federalne Ministerstwo Spraw Wewnętrznych, na stronie internetowej projektu prezentowane są informacje przeznaczone dla małych i średnich przedsiębiorstw. Ich celem jest poszerzenie wiedzy, ukazanie istniejącego ryzyka oraz przedstawienie prostych i skutecznych sposobów rozwiązywania problemów związanych z bezpieczeństwem. Inicjatywa przyczynia się do zachowania ścisłej współpracy pomiędzy różnymi podmiotami działającymi w sektorze takimi jak na przykład: Bitkom e.V., Bundesverband der Deutschen Industrie e.V. (BDI), Niemiecki Związek Izb Przemysłowych i Handlowych (DIHK), Mcert, TeleTrusT Deutschland e.V. oraz inne stowarzyszenia i organizacje. Aby uzyskać więcej informacji zobacz: <http://www.mittelstand-sicher-im-Internet.de/>

Przedsiębiorstwa takie jak eBay oraz T-Online powołały wraz SAP i Microsoft wspólną inicjatywę, wspieraną przez Federalne Ministerstwo Gospodarki i Pracy. Łącznie 14 partnerów porozumienia zobowiązało się do zwiększenia bezpieczeństwa w zakresie opracowania elektronicznych procesów biznesowych, poprawy wiarygodności w procesie wdrażania i posługiwania się oprogramowaniem oraz do lepszej ochrony danych. Uczestnicy projektu będą wspierać działania podejmowane w ramach inicjatywy poprzez organizowanie kampanii informacyjnych, opracowywanie wytycznych oraz narzędzi programowych, tak aby zwiększyć bezpieczeństwo i zaufanie zarówno po stronie przedsiębiorstw, jak i konsumentów. Rezultaty projektu zostały poddane analizie w maju 2006 r. Aby uzyskać więcej informacji zobacz: <https://www.sicherim-netz.de>

Inicjatywa opiera się na siedmiu zobowiązaniach do działania:

- Microsoft oraz Computer Associates zobowiązały się do opracowania i upowszechnienia kontroli bezpieczeństwa, pozwalającej na zidentyfikowanie luk w systemie.
- eBay zobowiązał się do udostępnienia pakietu informacyjnego, na podstawie którego użytkownicy uzyskają możliwość zapoznania się z wymogami prawnymi oraz zagrożeniami dotyczącymi prowadzenia bezpiecznego handlu w Internecie.
- Microsoft, niemiecka organizacja pomocy dzieciom *Deutsches Kinderhilfswerk*, oraz grupa wolontariuszy działających z ramienia dostawców usług multimedialnych, zobowiązały się do stworzenia portalu internetowego

przeznaczanego dla dzieci w wieku 8-13 lat, który byłby pomocny w treningu umiejętności medialnych.

- SAP, Mcert oraz Microsoft dostarczą małym i średnim przedsiębiorstwom pakiet informacyjny dotyczący bezpieczeństwa.
- Teletrust oraz niemieckie wydawnictwo *Deutsche Sparkassenverlag* zobowiązały się do dostarczenia małym i średnim przedsiębiorstwom, a także pośrednikom (*System resellers*) informacji, programów szkoleniowych oraz świadectw potwierdzających stosowanie technik szyfrowania.
- SAP oraz Microsoft zobowiązały się do realizacji programu bezpiecznego rozwoju, a także do dostarczenia szkołom wyższym odpowiednich informacji, które umożliwią studentom zapoznanie się z zagrożeniami związanymi z bezpieczeństwem oraz sposobami ich unikania w procesie opracowywania oprogramowania komputerowego.
- Firma T-Online zapewni bezpłatną usługę „barometr bezpieczeństwa”, umożliwiającą każdemu użytkownikowi określenie ryzyka związanego z bezpieczeństwem transakcji zawieranych drogą elektroniczną.

Definicja MŚP

ENISA przyjęła typową definicję MŚP, jednak w odniesieniu do średnich przedsiębiorstw bardziej trafna byłaby definicja określająca liczbę pracowników na poziomie od 250 do 5000.

Główne problemy związane z grupą docelową

MŚP na co dzień korzystają z Internetu oraz transakcji zawieranych drogą elektroniczną. Nie dysponują jednak zasobami finansowymi i personalnymi w takim zakresie, aby poradzić sobie z wszystkimi aspektami dotyczącymi bezpieczeństwa komunikacji elektronicznej. Podmioty te muszą dbać o swoje interesy. Właściciele przedsiębiorstw oraz menadżerowie rzadko są świadomi odpowiedzialności prawnej związanej z bezpieczeństwem IT. Specjaliści ITC potrzebują wsparcia w zakresie kwestii związanych z bezpieczeństwem, a pracownicy muszą mieć świadomość istniejących zagrożeń i niebezpieczeństw.

Charakterystyka odbiorców docelowych

Grupa odbiorców składa się głównie ze specjalistów ICT, o niskim poziomie wiedzy na temat kwestii związanych z bezpieczeństwem. Niektóre inicjatywy są również skierowane do pracowników, dyrektorów lub menedżerów, którzy nie posiadają żadnej wiedzy na ten temat / nie są świadomi istnienia tych kwestii, lub ich wiedza jest bardzo niska.

Wykorzystane kanały informacyjne

Głównym kanałem informacyjnym wykorzystanym w ramach podjętych działań był Internet. Ponadto, przy realizacji niektórych inicjatyw mających na celu poszerzenie wiedzy, wykorzystano materiały na płytach CD-ROM oraz podjęto się organizacji wydarzeń o zasięgu lokalnym.

W przypadku inicjatywy DsiN najważniejszym elementem było wydarzenie rozpoczynające kampanię. Wykorzystano następujące kanały informacyjne: strony internetowe, konferencje prasowe, płyty CD-ROM, wydawnictwa książkowe, audycje radiowe, przekazy telewizyjne oraz imprezy typu *truck tour*.

Wykorzystanie osób rozpowszechniających wiedzę

W przypadku inicjatywy DsiN do rozpowszechnienia informacji wykorzystano programy uniwersyteckie. Za pomocą sieci uniwersyteckiej, obsługiwanej przez SAP i Microsoft, udało się dotrzeć do 60.000 studentów, informując ich o spotkaniach mających na celu rozszerzenie wiedzy na temat bezpiecznego programowania.

Ramy czasowe

Inicjatywy trwają nie krócej niż przez okres jednego roku.

Zdobyte doświadczenie

Inicjatywa DsiN była doskonałym przykładem działania w ramach partnerstwa prywatno-publicznego. Ponieważ główną siłą napędową inicjatywy stanowiły podmioty działające w sektorze, to działania te stanowiły znakomite połączenie rzeczywistej pomocy dla grup docelowych z elementami kształtowania wizerunku/PR uczestników. Chociaż budżet przedsięwzięcia był bardzo wysoki, a zainteresowanie mediów inicjatywą DsiN duże, to poziom wiedzy wśród grup docelowych w dalszym ciągu należy uznać za niewystarczający. W odniesieniu do inicjatyw dotyczących bezpieczeństwa IT obowiązują takie same zasady, jak w przypadku innych kampanii marketingowych: Jedną z podstawowych zasad głosi, że chcąc osiągnąć „rozpoznawalność marki” na poziomie 80%, należy dysponować wystarczająco wysokim budżetem i utrzymywać stały zasięg kampanii.

Statystyki / wskaźniki KPI

Przykładem statystyk/wskaźników KPI wykorzystanych w inicjatywie „Deutschland sicher im Netz” są:

- statystyki stron internetowych
- Liczba osób biorących udział w danym wydarzeniu

- Liczba szkoleń przeprowadzonych przez uprawnionych partnerów inicjatywy „Deutschland sicher im Netz”
- Liczba uczestników inicjatywy DsiN oraz imprez typu *trade show* (Systems, Cebit)

Ocena inicjatywy jest kontynuowana. Można w tym przypadku zauważyć pewne podobieństwa do kampanii towarzyszących wprowadzaniu produktu na rynek, czy też do kampanii mających na celu poprawę wizerunku. Każdy element kampanii na rzecz poszerzania wiedzy musi podlegać ocenie i kontroli, tak aby można było określić, które działania pomagają osiągnąć cel kampanii, a które należy przerwać z uwagi na fakt, że nie są skuteczne.

Swiss Re

Swiss Re jest największą na świecie spółką reasekuracyjną i największym na świecie reasekuratorem ubezpieczeń na życie oraz ubezpieczeń chorobowych. Spółka posiada 70 oddziałów w ok. 30 krajach świata, zatrudniając 10.000 pracowników.

Projekt: Wyzwania i problemy

Spółka Swiss Re przeprowadziła niedawno kampanię na rzecz poszerzania wiedzy, dostrzegając powagę kwestii bezpieczeństwa, a także znaczny wzrost ryzyka oraz zagrożeń związanych z bezpieczeństwem IT. Po wdrożeniu zaawansowanych technicznie środków ochronnych, kierownictwo spółki dostrzegło, że infrastruktura oraz wszelkie podejmowane wysiłki mogą okazać się bezużyteczne, jeżeli pracownicy nie będą świadomi zagrożeń związanych z bezpieczeństwem IT i nie będą postępować w odpowiedni sposób. Tego rodzaju „czynniki ludzkie” stanowi w organizacji krytyczny element bezpieczeństwa informacji. Poszerzanie wiedzy na temat istniejących zagrożeń jest uznawane za jeden z elementów strategii w zakresie bezpieczeństwa, realizowanej przez przedsiębiorstwa.

Utworzono zespół zajmujący się projektem. Do udziału w pracach zespołu zaproszono pracowników różnych działów (np. działu prawnego, grup biznesowych itp.). Przeprowadzono również szereg badań wstępnych. Obejmowały one między innymi analizę grupy odbiorców, analizę uprzedzeń kulturowych w grupie odbiorców, analizę w zakresie postrzegania kwestii bezpieczeństwa IT, rozmowy z kierownictwem oraz analizę technik poszerzania wiedzy. Jako część analizy:

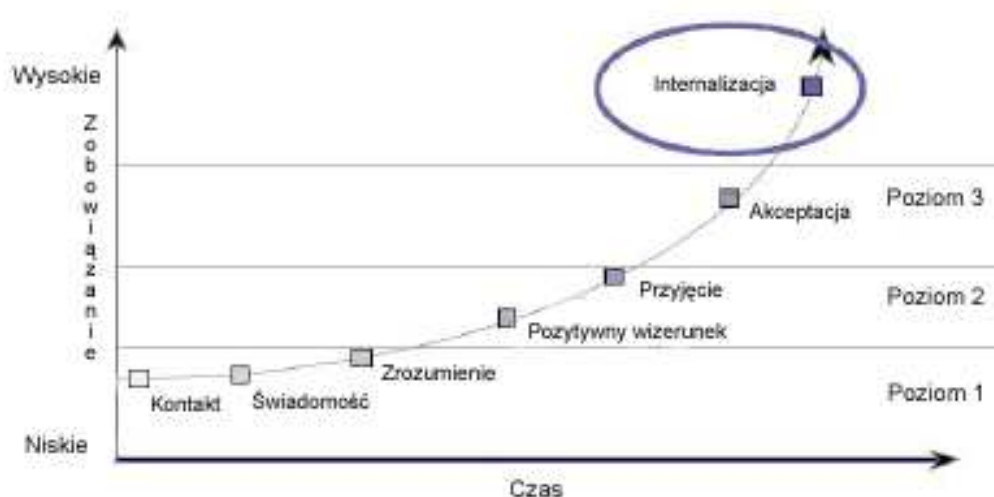
- określono 3 grupy docelowe: kadrę kierowniczą, użytkowników końcowych oraz personel IT
- określono 2 typy pracowników: indywidualiści (chętnie biorą na siebie odpowiedzialność) oraz hierarchiści (niechętnie podejmują ryzyko)
- Analizy wykazały, że sama informacja nie stanowi wystarczającego bodźca do zmiany zachowania w oczekiwanym kierunku
- Dla powodzenia inicjatywy poszerzania wiedzy decydujący był element wsparcia ze strony kadry kierowniczej wyższego szczebla

Zwrócono uwagę na szereg elementów, które mają duże znaczenie w trakcie prowadzenia kampanii na rzecz poszerzania wiedzy. Inicjatywy powinny:

- uwzględniać w odpowiedni sposób różnice kulturowe i językowe
- maksymalnie wykorzystywać istniejące kanały informacyjne
- unikać nadmiaru informacji
- obejmować zakresem szerokie grupy odbiorców, a jednocześnie być zaadresowane do indywidualnych odbiorców

Strategia: dwa poziomy realizacji zadań

Celem kampanii na rzecz poszerzania wiedzy było wywołanie trwałej zmiany postaw wśród pracowników (internalizacja):



Kampania została przeprowadzona na dwóch poziomach: z jednej strony przeprowadzono kampanię skierowaną do szerokiej grupy odbiorców, na którą składały się ogólne działania mające na celu poszerzanie wiedzy, z drugiej strony wdrożono kampanię, skierowaną do określonych grup użytkowników. Na obu poziomach przyjęto podejście odgórne. W obu kampaniach użyto różnych metod oraz środków:



Dwa obszary aktywnych działań :

KAMPAANIA SKIEROWANA DO SZEROKIEJ GRUPY ODBIORCÓW

Ogólne działania w zakresie poszerzania wiedzy

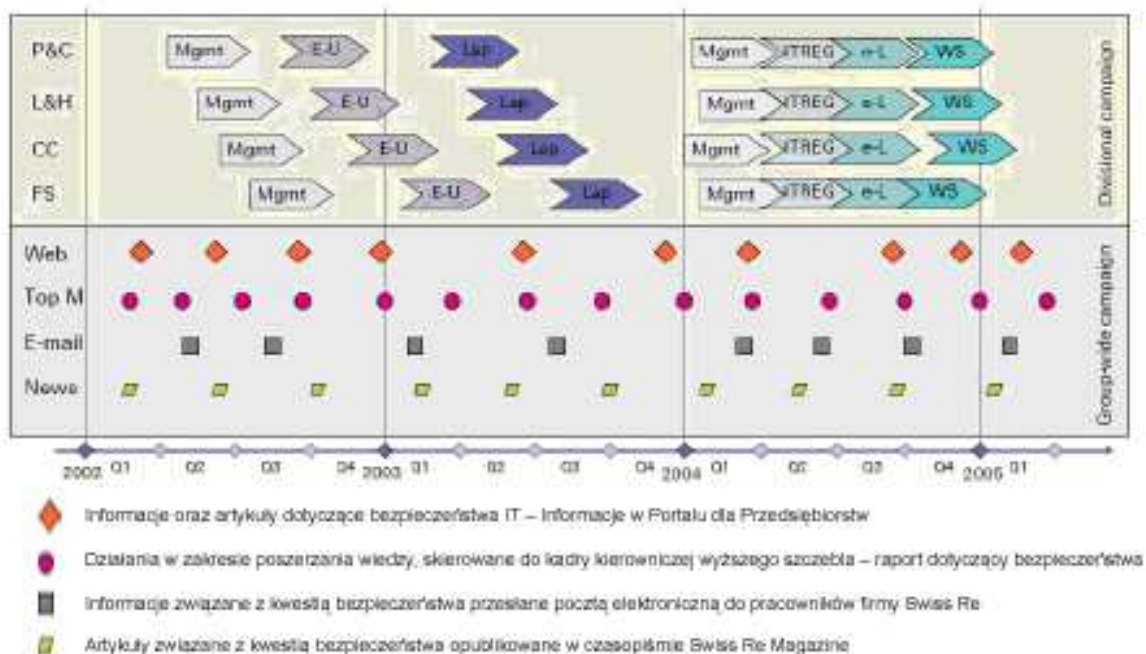
- Artykuły w czasopiśmie *Swiss Re Magazine*
- Broszura BIS
- Strona w sieci intranet
- Kwestionariusz internetowy BIS
- Informacje dla szerokich grup odbiorców, przesyłane pocztą elektroniczną
- itd.

KAMPAANIA DLA PRACOWNIKÓW POSZCZEGÓLNYCH DZIAŁÓW PRZEDSIĘBIORSTWA

skierowana do określonych grup

- Informacje dotyczące zarządzania
- Szkolenia dla użytkowników końcowych
- Szkolenia z wykorzystaniem laptopów
- Szkolenia dla pracowników IT
- Narzędzia z zakresu e-learning
- itd.]

Opracowano wysokiej jakości plan inicjalizowania kampanii, zawierający szczegółowy opis głównych działań podejmowanych w ramach kampanii wśród pracowników określonych działów obejmującej szeroką grupę odbiorców (w której wykorzystano różnego rodzaju środki).



Dotarcie do użytkowników: rozpoczęcie kampanii

Rozpoczęcie kampanii zbiegło się w czasie z podjęciem szeregu działań:

- Kadrze kierowniczej wyższego szczebla spółki Swiss Re wyświetlono film. W filmie tym zwrócono szczególną uwagę na istotne zagrożenia, takie jak na przykład używanie prostych haseł i przesyłanie poufnych informacji za pomocą faksu.
- Tydzień później, w czasopiśmie wydawanym przez spółkę, ukazały się artykuły na temat bezpieczeństwa informacji handlowych. Poszczególne egzemplarze pisma zostały obłożone w papierową obwolutę, w której umieszczono krótkie wskazówki dotyczące bezpieczeństwa informacji. Pracownicy byli w ten sposób zmuszeni do zapoznania się z tymi hasłami, jeszcze przed otwarciem danego egzemplarza pisma. Ponadto, na wewnętrznej stronie obwoluty umieszczono hasło. Jego wprowadzenie na nowej stronie internetowej poświęconej bezpieczeństwu IT, wiązało się z możliwością wygrania nagród.
- Uruchomiono także nowy portal internetowy poświęcony kwestiom związanym z bezpieczeństwem. Umożliwiło to zajęcie się zagadnieniami związanymi z klientami.

Sesje szkoleniowe typu „zajęciowego”

Przed rozpoczęciem sesji szkoleniowych typu „zajęciowego” przygotowano materiały szkoleniowe. Materiały te obejmowały: slajdy, podręczniki, przewodniki dla prowadzących szkolenie, materiały drukowane (takie jak na przykład fiszki) oraz zestawy narzędzi i materiałów szkoleniowych dla osób prowadzących zajęcia. Materiały zostały opracowane w języku angielskim, a następnie przetłumaczone na 4 inne języki: niemiecki, francuski, włoski oraz hiszpański. Zrealizowano również moduły szkoleniowe, które miały na celu uzyskanie informacji zwrotnych od uczestników szkolenia oraz warsztaty, których celem był przegląd i powtórzenie dotychczas przekazanych wiadomości. Zorganizowano ponadto szkolenia typu „Train the Trainer” adresowane do osób prowadzących szkolenia. Sesje te były prowadzone przez wykwalifikowanych trenerów i obejmowały zagadnienia dotyczące sposobów przeprowadzania warsztatów i motywowania uczestników szkoleń. W celu przetestowania struktury oraz formy planowanych szkoleń, przeprowadzono w dwóch firmach szkolenia pilotażowe. Jako część szkoleń typu klasowego:

- przedstawiono w trakcie sesji trzy zagadnienia: zagrożenia związane z korzystaniem z poczty elektronicznej, zagrożenia związane z korzystaniem z Internetu oraz zagrożenia związane z używaniem haseł.
- zorganizowano interaktywne warsztaty umożliwiające przeprowadzenie dyskusji, przeprowadzono analizę studiów przypadku, zaprezentowano materiały wideo oraz zorganizowano sesje poświęcone zagadnieniom teoretycznym, podczas których udzielano odpowiedzi na najczęstsze pytania (Q&A)
- Obowiązkowe były sesje dla użytkowników końcowych i użytkowników laptopów
- Przeprowadzono ponad 700 sesji szkoleniowych
- Uczestnicy szkolenia zostali poproszeni o wypełnienie formularza z informacjami zwrotnymi, który miał być pomocny w stworzeniu zestawienia typu „przed” i „po”.

W kwestionariuszu z informacjami zwrotnymi zamieszczono dziewięć różnych pytań dotyczących zmiany postaw wobec określonych problemów

- Na pamiątkę odbytej sesji szkoleniowej każdy jej uczestnik otrzymał materiały promocyjne w formie różnego rodzaju gadżetów.

Sesje szkoleniowe wykorzystujące e-learning

W drugiej fazie projektu wykorzystano technikę szkolenia na odległość zwaną e-learning. Sesje z wykorzystaniem techniki e-learning umożliwiły każdemu pracownikowi odbycie szkoleń w indywidualnym tempie, niezależnie od lokalizacji. Zebrano ponadto dane dotyczące uczestników, które udostępniono następnie pracownikom Działu Zasobów Ludzkich. W przypadku szkoleń typu e-learning nie było potrzeby wynajmowania sal, ani zatrudniania instruktorów.

Szkolenie pracowników IT

Oprócz ogólnych działań mających na celu poszerzenie wiedzy, przeprowadzono również szkolenia dla personelu IT. Dotyczyły one w szczególności przepisów dotyczących bezpieczeństwa IT oraz ich stosowania w codziennej pracy. Celem szkolenia było ograniczenie / zmniejszenie ryzyka operacyjnego. Treść i forma szkolenia były uzależnione od poziomu wiedzy, doświadczenia, profilu zawodowego, lokalizacji oraz działu przedsiębiorstwa, w którym pracuje personel IT. Udostępniono również laboratorium elektroniczne.

Pomiary i materiały pomocnicze

W celu oceny wyników kampanii oraz zgromadzenia istotnych informacji zwrotnych wykorzystano szereg różnego rodzaju metod:

- Formularz zawierający informacje zwrotne: 30% respondentów przyznało, że nie rozumie dokładnie kwestii związanych z bezpieczeństwem, a 89% respondentów stwierdziło, że miało zamiar zmienić swoje postępowanie po zakończeniu szkolenia.
- Broszury – przekazywane i promowane przez kadrę kierowniczą wyższego szczebla; broszury zostały rozdane wszystkim pracownikom. Broszury (dostępne w 5 różnych językach) zostały rozesłane na dwa tygodnie przed opracowaniem kwestionariusza internetowego.
- Kwestionariusz internetowy – miał za zadanie zachęcić pracowników do udzielenia poprawnych odpowiedzi na zamieszczone pytania (kwestionariusz zawierał również odwołania do materiałów pomocniczych, takich jak na przykład broszury). W celu dalszego poszerzania wiedzy, przesłano drogą elektroniczną wiadomości dotyczące kampanii. Spotkały się one z dobrym przyjęciem. Planuje się coroczne dokonywanie oceny kwestionariusza internetowego, którego pytania ulegną zmianie

- Informacje na temat bezpieczeństwa zamieszczane w Intranecie - usługi typu pull, takie jak Intranet wpływają na liczbę pracowników odwiedzających portal poświęcony kwestiom bezpieczeństwa IT, ale większy wpływ wywierają usługi typu push, takie jak poczta elektroniczna.

Zdobyte doświadczenia

- Najważniejsi są ludzie
- Niezbędne jest wsparcie ze strony kadry kierowniczej wyższego szczebla (przyjęcie strategii odgórnej)
- Pomiary efektów są trudne, ale niezwykle istotne (stworzenie zestawienia typu „przed” i „po”)
- Bardzo duże znaczenie ma zaangażowanie przedstawicieli grup docelowych w opracowanie programów szkoleniowych (pozwala to wykorzystać wiedzę ekspertów w danej dziedzinie oraz umożliwia dostosowanie szkolenia do potrzeb danej grupy docelowej)
- Konieczne jest uwzględnienie różnic kulturowych i językowych (ważne komunikaty muszą być przekazywane w rodzimym języku odbiorców).
- Bardzo czasochłonnym przedsięwzięciem jest opracowanie i koordynacja kampanii skierowanej do szerokiego grona odbiorców
- W celu zapewnienia trwałości efektów kampanii konieczne jest podejmowanie na bieżąco następujących działań:
 - ogłaszanie artykułów w prasie firmowej
 - stałe aktualizowanie i dbałość o atrakcyjność wewnętrznej sieci Intranet
 - opracowywanie dla kadry kierowniczej wyższego szczebla comiesięcznych sprawozdań pt. „Ryzyko dotyczące bezpieczeństwa IT i informacja o incydentach”.
 - przeprowadzanie corocznej oceny w zakresie efektów działań mających na celu poszerzanie wiedzy oraz oceny wiedzy podstawowej
- Skuteczna kampania na rzecz poszerzania wiedzy może przyczynić się do zmian kulturowych
- Nie można zapominać o pracownikach, którzy niedawno dołączyli do firmy.
- Nie można zapominać o nowych zagrożeniach
- Należy sprawić, aby poszczególne elementy kampanii mogły stać się także prywatną sprawą odbiorców
- Należy przygotować różne moduły szkoleniowe i materiały na różnym poziomie
- Sesje szkoleniowe typu klasowego przynoszą lepsze efekty niż e-learning
- Metody prowadzenia szkoleń powinny być każdorazowo sprawdzane i w miarę potrzeby korygowane

Więcej informacji na temat kampanii spółki Swiss Re zobacz: [thehumanfactor-isf2004040903_v2.pdf](#) w części *Pliki Źródłowe*

Media

Obecna sytuacja

Środki masowego przekazu w dalszym ciągu stanowią główny kanał informacyjny, za pomocą którego inicjatywy na rzecz poszerzania wiedzy trafiają do pozostałych grup docelowych. Wprawdzie więcej państw członkowskich wykorzystuje media do przekazywania komunikatów w ramach kampanii, lecz zrobiono dotychczas niewiele w kwestii edukacji pracowników mediów masowych w zakresie problematyki bezpieczeństwa.

Dobre praktyki w poszczególnych krajach

Należy zwrócić uwagę na wskazany przez państwa członkowskie przykład wykorzystania mediów jako kanału dotarcia do innych grup docelowych; nie przedstawiono szczegółowych informacji dotyczących dotarcia do grupy docelowej „Media”.

Dobre praktyki w innych organizacjach

Reuters

To przedsiębiorstwo prasowo-medialne posiada około 16 000 pracowników w 220 miastach w 94 krajach na całym świecie – w tym 196 agencji wydawniczych. Każdego dnia wiadomości Reuters ogląda ponad miliard osób. Reuters stara się poszerzać wiedzę na temat bezpieczeństwa w taki sam sposób, jak robią to małe i średnie przedsiębiorstwa. Szkolenie zapewnione pracownikom przez przedsiębiorstwo jest skierowane do konkretnego grona odbiorców w oparciu o ich umiejętności i funkcje pracownicze (a tym samym ich potrzeby).

Spółka wykorzystuje dokument „Grupowa praktyka bezpieczeństwa” – ponieważ główni klienci Reutersa to duże instytucje finansowe, silny rozwój i gwarantowanie bezpieczeństwa to zasadnicze kwestie dla tego przedsiębiorstwa. Z tego powodu został przyjęty program intensywnego szerzenia wiedzy na temat bezpieczeństwa w związku z tworzeniem oprogramowania. Architekci, projektanci, programiści i pracownicy ds. gwarancji jakości - to do nich głównie kierowany jest projekt.

Firma wykorzystuje różne kanały przy rozpowszechnianiu komunikatów wśród docelowych odbiorców. Można wyróżnić wśród nich:

- różne formy szkolenia: ukierunkowane briefingi, briefingi w czasie lunchu/śniadania, zajęcia/warsztaty, nauka przez Internet;
- marketing i promocję: plakaty i broszury, imprezy związane z bezpieczeństwem/zagrożeniem, gry/quizy/zawody, podarunki i prezenty reklamowe;

- udzielanie pomocy/informacji; źródła on - line (intranet/extranet), e-maile i ostrzeżenia oraz krótkie informacje i biuletyny informacyjne;
- opinie: opinie on-line i sondaże pracowników.

Zauważono, że najbardziej skutecznymi kanałami umożliwiającymi poszerzanie wiedzy są szkolenia w ramach zajęć lub warsztatów. Nauka przez Internet i źródła on-line są umiarkowanie skuteczne przy dostarczaniu wiadomości, podczas gdy krótkie informacje i biuletyny informacyjne wydają się najmniej efektywne.

ISP

Obecna sytuacja

Współpraca między sektorem publicznym, prywatnym i ISP jest coraz intensywniejsza w obrębie państw członkowskich. Więcej dzieje się w zakresie dostarczania społeczeństwu informacji o bezpieczeństwie, choć można jeszcze wiele zrobić, jeśli chodzi o szkolenia pracowników ISP.

Dobre praktyki w poszczególnych krajach

Francja

Jako część inicjatywy szerzenia wiedzy wśród młodzieży francuskiej ministerstwo wraz z partnerami biznesowymi, społecznymi, w tym z ISP, przeprowadziło kampanię za pośrednictwem wielu kanałów, wraz z dystrybucją oprogramowania do kontroli rodzicielskiej. W celu uzyskania dalszych informacji, kliknij poniższy odsyłacz, aby przejść do szczegółów o Francji w części *Dobre praktyki w poszczególnych krajach*.

Włochy

Jako część prawa chroniącego małoletnich rozpoczęto inicjatywę skupiającą się na bezpiecznych narzędziach do surfowania i systemach filtrowania. Wysiłki ISP w kierunku zgodności z dyrektywą i inicjatywami były niewielkie. W celu uzyskania dalszych informacji, kliknij poniższy odsyłacz, aby przejść do szczegółów o [Włoszech](#) w części *Dobre praktyki w poszczególnych krajach*.

Luksemburg

Po inicjatywie badającej routery ADSL sprzedane w kraju stworzono podstawową rzecz, taką jak bezpieczna konfiguracja routerów. Stanowi to podstawę bliskiej współpracy z ISP. W celu uzyskania dalszych informacji, kliknij poniższy odsyłacz, aby przejść do szczegółów o [Luksemburgu](#) w części *Dobre praktyki w poszczególnych krajach*.

Malta

Rozpoczęto wspólny program z ISP mający na celu szerzenie wiedzy wśród dzieci. Celem jest zaznajomienie dzieci na wczesnym etapie życia z internetowymi zagrożeniami. W celu uzyskania dalszych informacji, kliknij poniższy odsyłacz, aby przejść do szczegółów o [Malcie](#) w części *Dobre praktyki w poszczególnych krajach*.

Norwegia

Inicjatywa publiczno-prywatna, obejmująca ISP zaowocowała stworzeniem strony internetowej przeznaczonej dla ogółu społeczeństwa i MŚP. Na stronie internetowej

znajdują się informacje, porady i wskazówki dotyczące bezpiecznego korzystania z Internetu. Zawartość strony została podzielona na tematy i kategorie. W celu uzyskania dalszych informacji, kliknij poniższy odsyłacz, aby przejść do szczegółów o [Norwegii](#) w części *Dobre praktyki w poszczególnych krajach*.

Polska

ISP współpracowali przy rozwiązaniach niektórych problemów bezpieczeństwa IT, które dotyczą ogółu społeczeństwa. W celu uzyskania dalszych informacji, kliknij poniższy odsyłacz, aby przejść do szczegółów o [Polsce](#) w części *Dobre praktyki w poszczególnych krajach*.

Portugalia

Organizacje pozarządowe współpracowały z ISP przy próbach rozwiązania niektórych problemów bezpieczeństwa IT, z którymi ma do czynienia ogół społeczeństwa. Organizowano spotkania i fora. W celu uzyskania dalszych informacji, kliknij poniższy odsyłacz, aby przejść do szczegółów o [Portugalii](#) w części *Dobre praktyki w poszczególnych krajach*.

Dobre praktyki w innych organizacjach

FORTH

Przez ostatnie cztery lata FORTHnet (jeden z największych greckich ISP) przy współpracy z SAFENET, IME i FORTH zarządzał SAFELINE (<http://www.safeline.gr>), grecką linią interwencyjną w ramach walki z cyberprzestępczością. SAFELINE została wsparta częściowo przez Komisję Europejską, rząd grecki i wyżej wymienione organizację partnerskie. Linia SAFELINE była zawsze aktywna w promowaniu bezpieczniejszego korzystania z Internetu skupiając się na tym, jak pomóc dzieciom i młodzieży w zdobyciu bezpiecznego i owocnego doświadczenia w korzystaniu z niego. Aby upowszechnić swoją działalność SAFELINE organizuje imprezy, mobilizuje przedstawicieli branżowych w Grecji i współpracuje ze szkołami o odpowiedniej organizacji. Patrz niżej: screenshot portalu.



Władze lokalne

Obecna sytuacja

Coraz więcej państw członkowskich zaczyna w szczególny sposób ukierunkowywać się na władze lokalne w ramach działań na rzecz szerzenia wiedzy. Kraje zorientowały się, że pracownicy sektora państwowego muszą zostać poinformowani o kwestiach i protokołach bezpieczeństwa informacji, ponieważ obywatele i podmioty gospodarcze oczekują od administracji szybkich, skutecznych i bezproblemowych usług. Do chwili obecnej większość inicjatyw z zakresu poszerzania wiedzy została przeprowadzona w ramach seminariów, sesji szkoleniowych, publikacji i poprzez wykorzystanie informacji on-line. W obrębie państw członkowskich rozpoczęto programy, które wymagają współpracy między różnymi ministerstwami lub organami administracji.

Dobre praktyki w poszczególnych krajach

Niemcy

Rząd Federalny podjął działania skierowane do wszystkich grup społecznych, których celem jest poszerzanie wiedzy. Pracownicy administracyjni byli również objęci tymi działaniami, na przykład poprzez wykorzystanie podręczników. W celu uzyskania dalszych informacji, kliknij poniższy odsyłacz, aby przejść do szczegółów o [Niemczech](#) w części *Dobre praktyki w poszczególnych krajach*.

Węgry

Powstało kilka programów i inicjatyw skierowanych do obywateli, ale także urzędników państwowych, by poprawić skuteczność korzystania z portali. W celu uzyskania dalszych informacji, kliknij poniższy odsyłacz, aby przejść do szczegółów o [Węgrzech](#) w części *Dobre praktyki w poszczególnych krajach*.

Irlandia

Prywatna organizacja VigiTrust specjalizuje się w prowadzeniu szkoleń mających na celu poszerzania wiedzy na temat bezpieczeństwa dla podmiotów sektora publicznego i prywatnego. Szczegóły w części *Dobre praktyki w innych organizacjach* we fragmencie poświęconym [władzom lokalnym](#).?????? irlandia

Włochy

Inicjatywa szerzenia wiedzy w administracji publicznej, skierowana do najwyższego kierownictwa, głównych menadżerów ds. bezpieczeństwa ICT i ich pracowników jest obecnie w toku. Wykorzystano różne kanały, łącznie z seminariami i nauczaniem przez Internet. Pracownicy posiadają również możliwość w miejscu pracy, dobrowolnie, oglądania specjalne nakręconych filmów. W celu uzyskania dalszych informacji, kliknij

poniższy odsyłacz, aby przejść do szczegółów o [Włoszech](#) w części *Dobre praktyki w poszczególnych krajach*.

Litwa

W ramach inicjatyw rządowych przeszkolono ponad 200 osób pracujących w państwowych instytucjach. Program szerzenia wiedzy na temat bezpieczeństwa IT jest dostępny na CD - ROMie lub na stronie internetowej. Wykorzystano również lub planuje się wykorzystać materiały na seminaria i do nauczania na odległość dla urzędników i pracowników. W celu uzyskania dalszych informacji, kliknij poniższy odsyłacz, aby przejść do szczegółów o [Litwie](#) w części *Dobre praktyki w poszczególnych krajach*.

Luksemburg

Zainicjowano projekt w pełni skupiający się na bezpieczeństwie w ministerstwach i organach administracji. W czasie tego projektu przeprowadzana jest analiza ryzyka w ministerstwie i sporządzana jest strategia bezpieczeństwa informacji. W ramach projektu pracownicy rządowi otrzymują materiały przygotowane specjalnie dla nich, poszerzające wiedzę za pośrednictwem ulotek, plakatów, Intranetu i specjalnych kursów. W celu uzyskania dalszych informacji, kliknij poniższy odsyłacz, aby przejść do szczegółów o [Luksemburgu](#) w części *Dobre praktyki w poszczególnych krajach*.

Holandia

Wiele inicjatyw takich jak ICTU i eGEM ma na celu szerzenie wiedzy na temat bezpieczeństwa. Grupą docelową są władze lokalne. W celu uzyskania dalszych informacji, kliknij poniższy odsyłacz, aby przejść do szczegółów o Holandii w części *Dobre praktyki w poszczególnych krajach*.

Portugalia

Zrealizowano lub realizuje się nadal szereg inicjatyw mających na celu poszerzenie wiedzy, skierowanych do użytkowników prywatnych, ISP i władz lokalnych. Przeprowadzano je głównie poprzez szkolenia, imprezy publiczne lub współpracę z różnymi podmiotami. W celu uzyskania dalszych informacji, kliknij poniższy odsyłacz, aby przejść do szczegółów o [Portugalii](#) w części *Dobre praktyki w poszczególnych krajach*.

Szwecja

Szwecja zrealizowała lub realizuje nadal różne inicjatywy mające na celu poszerzenie wiedzy, skierowane do użytkowników prywatnych, MŚP, ISP i władz lokalnych. Niektóre przykłady zawierają projekt uruchomiony przez Państwowy Urząd Pocztowy i Telekomunikacyjny, który korzysta z interaktywnych stron internetowych i publikacji

za pośrednictwem innych kanałów, a także projekt SurfaLugnt, który został opracowany przy współpracy z przemysłem IT i właściwymi organami. Inna inicjatywa, podjęta przez Sztokholm, obejmowała nakręcenie filmu dla pracowników sektora publicznego dotyczącego ich funkcji. Film ten zawierał również wskazówki dotyczące bezpieczeństwa.

W celu uzyskania dalszych informacji, kliknij poniższy odsyłacz, aby przejść do szczegółów o [Szwecji](#) w części *Dobre praktyki w poszczególnych krajach*.

Wielka Brytania

W Wielkiej Brytanii podjęto kilka inicjatyw mających na celu poszerzenie wiedzy, skierowanych do użytkowników prywatnych, MŚP oraz władz lokalnych. Do przekazywania informacji wykorzystano następujące kanały: strony internetowe, imprezy publiczne, ogólnokrajowe media (takie jak telewizja i radio) oraz imprezy objazdowe dla sektora publicznego. Programy rozwojowe, takie jak CSIA, również mają na celu poszerzanie wiedzy na poziomie władz państwowych i lokalnych. W celu uzyskania dalszych informacji, kliknij poniższy odsyłacz, aby przejść do szczegółów o [Wielkiej Brytanii](#) w części *Dobre praktyki w poszczególnych krajach*.

Dobre praktyki w innych organizacjach

VigiTrust

VigiTrust nie jest partnerem rządu irlandzkiego, jeśli chodzi o programy i inicjatywy szerzenia wiedzy, współpracuje jednak z kilkoma podmiotami sektora publicznego (departamentami rządowymi, władzami lokalnymi i innymi organizacjami) przy organizacji szkoleń poszerzających wiedzę na temat bezpieczeństwa. Ma na celu zwiększenie poziomu wiedzy na temat bezpieczeństwa wśród wszystkich osób, które oczekują takiego szkolenia. Zainteresowani mogą wybrać publiczne warsztaty, gdzie będą szkoleni wraz z prywatnymi podmiotami lub warsztaty, które można dostosować do wymogów poszczególnych organizacji rządowych i przeprowadzać je w urzędach.

Opis docelowych odbiorców

Personel techniczny IT, dyrektorzy IT, a także dyrektorzy lub dyrektorzy naczelni w departamentach rządowych biorą udział w szkoleniach, chcąc wiedzieć więcej na temat prawnych, handlowych, funkcjonalnych i technicznych aspektów bezpieczeństwa przedsiębiorstwa. By szerzyć wiedzę, VigiTrust zwraca raczej uwagę na rynkowe aspekty bezpieczeństwa, nie skupiając się na jego czysto technicznym aspekcie. Pięć filarów bezpieczeństwa to: bezpieczeństwo fizyczne, bezpieczeństwo ludzi, bezpieczeństwo danych, bezpieczeństwo IT i wyjście z kryzysu/ciągłość działalności.

Poziom wiedzy

Jest on zróżnicowany, od niskiego po wysoki, niemniej wiedza większości zainteresowanych przed uczestnictwem w warsztatach znajduje się między średnim a niskim poziomem.

Główne zagadnienia

Wydaje się, że zainteresowani skupiają się na zagadnieniach funkcjonalnych, takich jak DR i BC i na rozwiązywaniu problemów związanych z oprogramowaniem antywirusowym. Bardzo niewielu jest świadomych swojego zakresu odpowiedzialności na mocy Ustawy o ochronie danych i innych przepisów o zasadniczym znaczeniu.

Tam, gdzie odbyły się warsztaty dostosowane do danej instytucji, zaobserwowano, że większość zainteresowanych różnie rozumiała wymogi bezpieczeństwa i środki zapobiegawcze w swoim biurze administracji rządowej. Większość z nich nie posiada jasnych strategii, a istniejące strategie nie są upowszechniane lub nie realizuje się ich w skuteczny sposób. Dlatego wydaje się, że w Irlandii sektor publiczny stoi wobec takich samych problemów i prezentuje taki sam ogólny poziom wiedzy pod względem wymogów prawnych, jeśli chodzi o bezpieczeństwo.

Na poziomie technicznym organizacje rządowe są zazwyczaj bardziej zaawansowane niż ich odpowiedniki w sektorze prywatnym o podobnym wymiarze organizacyjnym. Coraz częściej posiadają narzędzia do filtrowania maili i stron internetowych, a także nieustannie obserwują pojawiające się zagrożenia, takie jak korzystanie z pamięci USB i zarządzanie zagrożeniami z pulpitu.

Wartość dodana dla zainteresowanych – w jaki sposób warsztaty zwiększają poziom wiedzy o bezpieczeństwie. Zazwyczaj zainteresowani przeprowadzają analizę SWOT swojego środowiska sprawdzając, jak bezpieczeństwo można analizować pod względem mocnych stron (*strengths*), słabych stron (*weaknesses*), szans (*opportunities*) i zagrożeń (*threats*) prawdopodobnych lub istniejących w otoczeniu. Dlatego opierają się na własnej wiedzy o poziomie bezpieczeństwa w biurze w porównaniu do najlepszej praktyki. Następnie są informowani, w jaki sposób zhierarchizować działania i jak je podzielić na te, których można dokonać wewnątrz organizacji za pośrednictwem zatrudnionych pracowników i na te, które należy rzeczywiście zlecić zewnętrznym ekspertom od bezpieczeństwa.

Pozytywny rezultat uzyskiwany za sprawą klientów rządowych to fakt, że wykorzystują oni wiedzę zdobytą na warsztatach jako podstawę do planu dalszego upowszechniania koncepcji poszerzania wiedzy na temat bezpieczeństwa w obrębie ich działu. Bardzo często organ tworzy plan, w jaki sposób zwiększyć poziom bezpieczeństwa na podstawie wniosków wyciągniętych w trakcie warsztatów.

Statystyki i kluczowe wskaźniki wydajności (KPI)

Statystyki oficjalnie nie są stosowane. Rząd irlandzki stara się podnieść ogólny poziom wiedzy, zachęcając do uczestniczenia w dniu pod hasłem „Makeitsecure” („Zapewnij bezpieczeństwo”), który obchodzony jest zazwyczaj w listopadzie (zob. www.makitsecure.ie). Efektywność tej kampanii można zmierzyć na podstawie uwagi, jaką przypisują jej zarówno media, jak i ogół społeczeństwa, a także na podstawie reakcji na stronach internetowych. Istnieje kilka organizacji zajmujących się bezpieczeństwem w Irlandii, które obsługują seminaria na temat bezpieczeństwa informacji, jednak większość skupia się na produkcji i jest ukierunkowana na działalność rynkową. *Global Security Week* nie promuje jakiegokolwiek indywidualnego produktu czy usługi. Zob. www.globalsecurityweek.com

Koncepcja stosowania analizy SWOT odnośnie do bezpieczeństwa przedsiębiorstw jest dobrym początkiem do stworzenia podstaw wiedzy przedsiębiorstwa na temat kluczowych zagadnień bezpieczeństwa w ramach pięciu filarów bezpieczeństwa. Poprzez porównanie wyników pierwszej analizy SWOT z wynikami drugiej analizy przeprowadzonej po uzgodnionym okresie (np. sześciu miesięcy), można określić efektywność programu zwiększania wiedzy przyglądając się następującym kwestiom:

- Czy zmierzono się z wszystkimi kluczowymi zagrożeniami?
- Czy wykorzystano kluczowe szanse wykorzystania bezpieczeństwa jako motoru działalności rynkowej, jako czynnika wzmacniającego kulturę przedsiębiorstwa i narzędzia zwiększania produktywności?
- Czy zidentyfikowane w pierwszej analizie SWOT mocne strony istnieją nadal i czy istnieją jakieś inne mocne strony po drugiej analizie?
- Czy wyzbyto się wszystkich słabych stron lub zmniejszono ich zakres?
- Czy wszyscy pracownicy są świadomi zmian?
- Czy wszyscy pracownicy posiadają większą wiedzę na temat bezpieczeństwa?

Jako przykład wyników analizy SWOT można podać następujące kwestie (lista ta nie jest wyczerpująca):

Mocne strony

Najlepsze w swoim rodzaju, techniczne rozwiązania zostały już zastosowane. Pracownicy IT posiadają wiedzę na temat podstawowych zagadnień. Niektóre strategie zostały już zrealizowane. Wykwalifikowany personel techniczny zapewniający zatwierdzanie bezpieczeństwa. Zarząd wspiera zespół IT, zobowiązując się finansowo wobec niego.

Szanse

Dostarczono już dodatkowych zasobów IT, gwarantując w ten sposób pozostałym pracownikom czas na intensywniejsze skupienie się na sprawach związanych z bezpieczeństwem.

Istnieje szansa wykorzystania bezpieczeństwa do zwiększenia produktywności, dostępności systemu i zmniejszenia ewentualnej odpowiedzialności. Projekt ten wzmocni również ducha zespołu.

Aspekty prawne bezpieczeństwa przedsiębiorstwa mogą być wykorzystane do zaangażowania wyższego kierownictwa.

Jest wyznaczany nowy dyrektor naczelny - nowa praktyka pracy może zostać wprowadzona w celu zwiększenia bezpieczeństwa, które może zająć ważniejsze miejsce w strategii działania firmy.

Słabe strony

Brak ogólnej wiedzy na temat zagrożeń dla bezpieczeństwa przedsiębiorstwa lub brak wiążących decyzji o walce z nimi. Przedsiębiorstwo X nie optymalizuje inwestycji w system IT ani w istniejące elementy zabezpieczające. Podobnie w przypadku procedur i strategii. Codzienne skupienie się na zagadnieniach bezpieczeństwa w przeciwieństwie do długoterminowej strategii wyeliminowania problemów lub aktywnego z nimi zmagania. Brak odpowiedzialności – brak oficjalnego kierownika ds. bezpieczeństwa. Brak spójnej polityki w ramach różnych części grupy. Brak niektórych strategii, konieczność aktualizacji lub przebudowy innych.

Zagrożenia

Brak zrozumienia, zaangażowania i uwagi kierownictwa pod względem ogólnych zagrożeń naruszenia bezpieczeństwa przedsiębiorstwa.

Hakerzy – nigdy nie przeprowadzano tzw. *penetration testing* (symulacja ataku na komputer [przyp. tłum.]) na systemach Rehab. DR? – Brak planu.

Zachowanie ludzi - użytkownicy w ogóle nieprzeszkoleni.

Zaufanie do bezpieczeństwa strony trzeciej w przypadku Intranetu i stron internetowych; im bliżej centra danych, tym większe zaufanie.

Inne sposoby mierzenia efektywności to obserwacja liczby incydentów naruszenia bezpieczeństwa przed rozpoczęciem programu szerzenia wiedzy i po rozpoczęciu. Dla przykładu, ile odnotowano przypadków zainfekowania wirusem, ile wykryto przypadków nadużycia internetowego (przeglądanie stron niezwiązanych z pracą i/lub niedozwolonych stron), ilu pracowników przeszło podstawowe szkolenie dzięki programowi i czy pracownicy ci są bardziej produktywni niż ci, którzy nie przeszli szkolenia?

Wytyczne dotyczące dobrych praktyk

Zalecenia

Ogólne

Nr	Wytyczna	Szczegóły
1	Odpowiednie zaplanowanie i realizacja inicjatywy	Ocena wymogów i wyraźne określenie celów kampanii. Korzystanie z planów i etapów w celu ułatwienia realizacji zadań i działań. Opracowanie Planu Przekazywania Informacji. Cała inicjatywa mająca na celu poszerzanie wiedzy powinna mieć charakter dynamiczny a nie statyczny, np. powinna zmienić cele poprzedniej inicjatywy na rzecz poszerzania wiedzy.
2	Wykorzystanie podmiotów upowszechniających informacje	Media należy wykorzystywać w charakterze ośrodków rozpowszechniających wiedzę, czyli podmiotów służących upowszechnianiu informacji dotyczących kampanii; media są w stanie maksymalnie zwiększyć zasięg kampanii na rzecz poszerzania wiedzy poprzez przekazywanie informacji. Inne sposoby korzystania z efektu powielania wiedzy to szkolenia trenerów, kształcenie nauczycieli i praca z ISP.
3	Wykorzystanie partnerstw prywatno-publicznych	Partnerstwo prywatno-publiczne może być bardzo skuteczne w przypadku przekazywania informacji na temat kampanii, szczególnie wtedy, gdy każda z organizacji może zrównoważyć siły i zasoby. W sytuacji gdy program został już opracowany, duże znaczenie ma Kodeks postępowania oraz takie elementy, jak wytyczne dotyczące projektów.
4	Wykorzystywanie różnych kanałów	Duże znaczenie ma wykorzystywanie różnych kanałów w celu przekazania wiadomości na temat poszerzania wiedzy, w tym wszystkich środków przekazu dostępnych on-line i off-line.
5	Wiadomości powinny być konkretne lub zrozumiałe	Treść przekazywanych wiadomości w postaci tematów lub sposobów wykorzystania może pomóc w zrozumieniu. Różne grupy docelowe mogą charakteryzować się różnym poziomem zrozumienia lub oczekiwań; przekazywana wiadomość powinna odpowiadać zainteresowaniom, potrzebom i poziomom wiedzy grup docelowych.
6	Sprawienie aby wiadomość była zauważalna lub interaktywna	Skuteczna kampania na rzecz poszerzania wiedzy promująca bezpieczeństwo musi być widoczna i zrozumiała dla wszystkich. Jednym ze sposobów jest rozwianie mitów i niewłaściwych założeń lub wskazanie grupom docelowym popełnianych przez nie

		błędów. Innym sposobem jest spowodowanie, aby doświadczenie miało bardziej interaktywny charakter, np. sprawdzanie skuteczności hasła przy użyciu usług internetowych.
7	Stosowanie prostej terminologii	Stosowane terminy i definicje powinny być zrozumiałe dla grup docelowych.
8	Stosowanie statystyk i kluczowych wskaźników wydajności (KPI)	„Jeśli potrafisz coś zmierzyć, możesz tym zarządzać”; potrzeba opracowania statystyk do zmierzenia skuteczności kampanii (a także do ustalenia punktu odniesienia). Umożliwia określenie zdobytych doświadczeń, które mogą przyczynić się do zwiększenia skuteczności bieżących i przyszłych inicjatyw.
9	Monitorowanie inicjatyw na rzecz poszerzania wiedzy	Prowadzenie częstych badań i przygotowywanie raportów podczas lub po kampanii może pomóc w odpowiednim dostosowaniu kanałów przekazu, przekazywaniu wiadomości i ogólnej skuteczności inicjatywy. Ważne może być także przekazanie informacji na temat odniesionych sukcesów, szczególnie do mediów.

Użytkownik prywatny

Nr	Wytyczna	Szczegóły
1	Wykorzystywanie nauczycieli w charakterze podmiotów upowszechniających informacje	Nauczyciele i media mogą zostać wykorzystani jako podmioty upowszechniające informacje w przypadku każdej kampanii; są oni w stanie maksymalnie zwiększyć zasięg kampanii na rzecz poszerzania wiedzy poprzez przekazywanie informacji dzieciom.
2	Zwiększanie skuteczności za pomocą certyfikacji	Pewne rodzaje programów certyfikacji, w ramach których prowadzone są działania na rzecz poszerzania wiedzy, mogą w większym stopniu zainteresować dzieci.
3	Wykorzystywanie zrozumiałych i możliwych do określenia tematów	Szczególnie w przypadku młodych osób wykorzystywanie łatwych i powszechnych tematów i marek może pomóc w zrozumieniu.
4	Opracowanie wiadomości	Należy określić potrzeby i zainteresowania młodzieży, w przeciwnym razie kampania nie będzie dla nich interesująca i nie odniesie sukcesu.
5	Kreatywność i umiejętność przyciągnięcia uwagi	Aby zwrócić uwagę młodzieży na kampanię konieczna jest inwencja i pomysłowość. Przydatne w tym celu może być wykorzystanie takich kanałów przekazu jak komiksy i filmy animowane. Dzieci także mogą przyczynić się do poszerzania wiedzy dorosłych na temat niektórych zagadnień.

6	Opracowywanie modułowych lub możliwych do ponownego wykorzystania materiałów	Informacje lub pakiety edukacyjne mają tę zaletę, że mogą być wykorzystywane przez młodzież i nauczycieli w szkole, a w domu przez rodziców. Zestawy edukacyjne są skuteczne, ponieważ docierają do wszystkich domowników.
7	Wykorzystywanie specjalnych kanałów przekazu	Placówki służby zdrowia i instytucje ubezpieczeń społecznych są skutecznym kanałem dotarcia do starszych użytkowników.
8	Powrót do podstaw	Wiadomości mające na celu poszerzanie wiedzy przekazywane starszym pokoleniom powinny dotyczyć podstawowych informacji, ponieważ osoby starsze nie dorastały w dobie technologii ICT.

MŚP

Nr	Wytyczna	Szczegóły
1	Wykorzystywanie skutecznych kanałów przekazu	Przy natłoku informacji, jakie są dostępne on-line, i przy braku czasu wykorzystywanie kanałów przekazu, takich jak broszury, ulotki i zestawienia, jest bardzo skutecznym sposobem przyciągnięcia uwagi a zatem też i poszerzenia wiedzy.
2	Wykorzystywanie specjalnych kanałów przekazu	Wykorzystywanie organizacji handlowych, warsztatów, seminariów i inicjatyw partnerskich jest skuteczną metodą dotarcia do podmiotów zarządzających i właścicieli przedsiębiorstw. Specjalistyczne kanały, takie jak strony internetowe lub magazyny branżowe mogą być skuteczną metodą dotarcia do pracowników sektora IT ze względu na znaczenie ich codziennej pracy. Agencje, takie jak lokalne izby handlowe, sieci MŚP, związki handlowe i magazyny branżowe, są skutecznymi kanałami dotarcia do podmiotów na stanowiskach kierowniczych.
3	Wsparcie ze strony innych organizacji	Współpraca z innymi instytucjami rządowymi lub agencjami powoduje, że kampanie skierowane do MŚP są bardziej prestiżowe.
4	Opracowanie wiadomości	O ile jest to możliwe, wiadomości i kanały ich przekazywania powinny być dostosowane do rodzaju MŚP, jak również odpowiadać ich funkcjom.
5	Poszerzanie wiedzy nie ma jednorazowego charakteru	W związku z tym, że żyjemy w świecie ciągłych zmian, nieprzerwana realizacja programów i szkoleń na temat bezpieczeństwa ma ogromne znaczenie dla poszerzania wiedzy dotyczącej zagrożeń, na jakie narażone jest bezpieczeństwo informacji.
6	Wykorzystywanie	Skuteczne poszerzanie wiedzy pracowników można

kanalów przekazu w miejscu pracy

osiągnąć poprzez pomyślną realizację polityki bezpieczeństwa informacji. W ramach tej polityki przewidziane są podręczniki dla pracowników, umowy i pisemne potwierdzenie zatrudnienia, prowadzenie szkoleń i kursów.

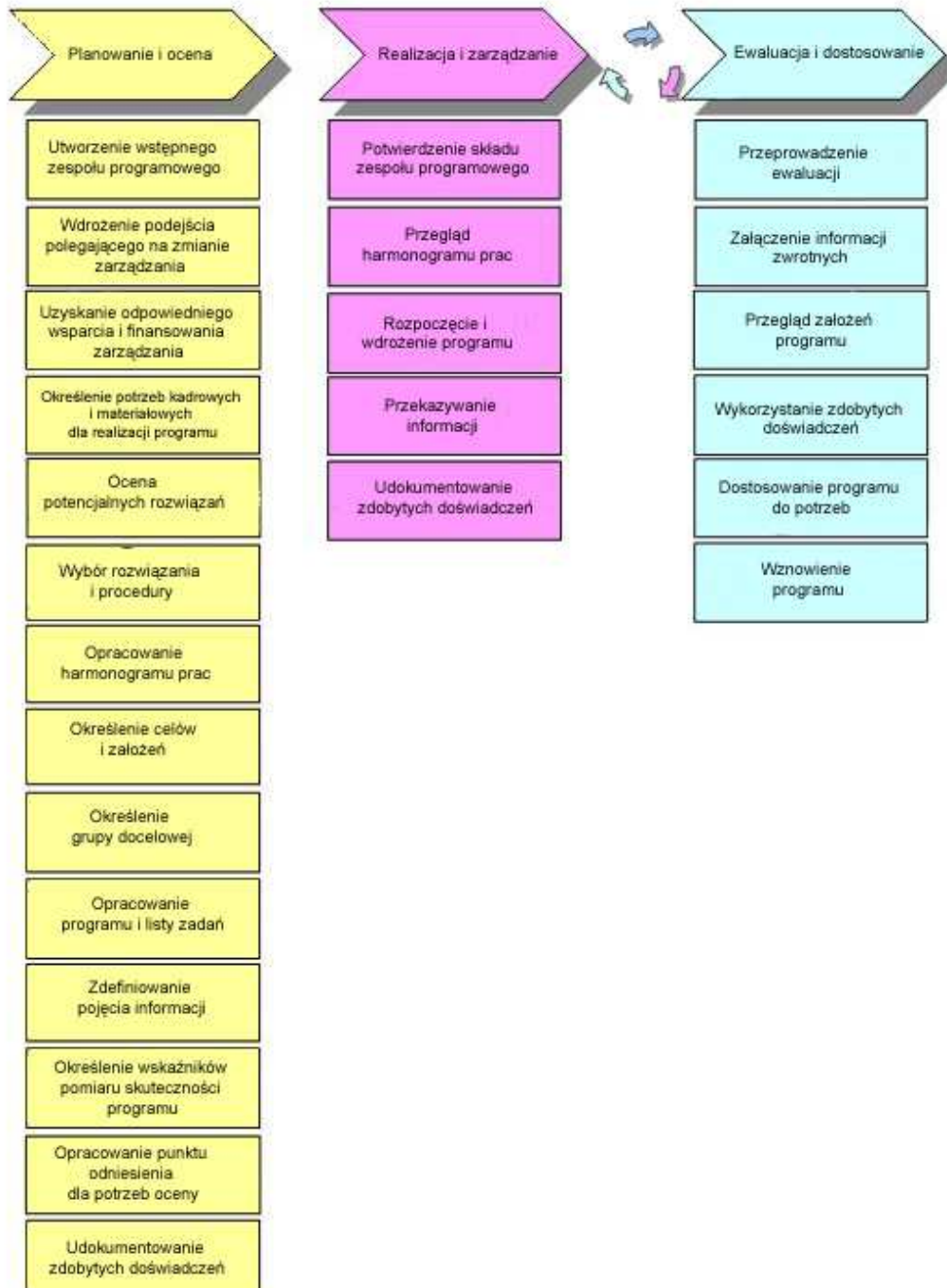
Media

Nr	Wytyczna	Szczegóły
1	Zrozumienie znaczenia, jakie mają media dla społeczeństwa	Przydatne mogłoby być przesłanie wiadomości zawierającej informację o odpowiedzialności społecznej, polegającej na dokładnym przekazywaniu informacji, jaka spoczywa na mediach, jak również o tym, że informacje przez nie przekazywane powinny być wysokiej jakości. Zagrożenia bezpieczeństwa informacji z założenia są w stanie zniszczyć zaufanie, integralność i dostępność informacji, a zatem mają kluczowe znaczenie dla nich.
2	Tworzenie sieci i partnerstw	Budowanie zaufania i dobrych relacji z mediami może pomóc w uzyskaniu możliwości relacjonowania przez nie działań, których celem jest poszerzanie wiedzy.
3	Opracowywanie wiadomości	Konferencje prasowe lub pakiety informacyjne dla mediów mogą pomóc w skoncentrowaniu wysiłków na przedstawianiu zagadnień dotyczących bezpieczeństwa informacji.
4	Wykorzystywanie specjalnych kanałów przekazu	Oprócz informacji dla prasy i innych podobnych materiałów, takich jak artykuły lub zestawienia, zamieszczenie informacji on-line lub gromadzenie informacji przeznaczonych dla grupy docelowej, jaką są media może ułatwić im poszerzenie wiedzy najpierw w ich własnym środowisku, a następnie w poszerzaniu wiedzy wśród społeczeństwa. Sesje szkoleniowe i warsztaty dla dziennikarzy są kolejnym działaniem, dzięki któremu możliwe jest przekazanie wiadomości na temat poszerzania wiedzy.
5	Utrzymanie zainteresowania	Oferowanie regularnych aktualizacji dotyczących aktualnych zagadnień lub bezpośrednie kontaktowanie się z agencjami prasowymi może być skutecznym sposobem na utrzymaniu zainteresowania i zaangażowania mediów.

Listy kontrolne

Przy planowaniu, realizowaniu i wprowadzaniu w życie wszelkich rodzajów inicjatyw na rzecz poszerzania wiedzy, zadania i działania mogą zostać podzielone na trzy główne etapy.

Zgodnie z dokumentem ENISA zatytułowanym [„Poradnik dla użytkowników: jak poszerzyć wiedzę o bezpieczeństwie informacji”](#) podział na etapy i składniki jest następujący:



Podział każdego etapu na zadania i działania umożliwia opracowanie pozycji listy kontrolnej. Państwa członkowskie powinny potraktować to w charakterze wskazówek do podjęcia głównych kroków przy prowadzeniu wszelkich programów mających na celu poszerzanie wiedzy na temat bezpieczeństwa informacji.

I. Planowanie i ocena

Nr	Pozycja listy kontrolnej
1	Utworzenie wstępnego zespołu programowego: należy utworzyć zespół programowy przeznaczony głównie do pierwszego etapu, mając jednakże na uwadze przejście zespołu do kolejnych etapów (aby zachować ciągłość). Należy zapewnić wyraźny podział ról i obowiązków.
2	Wdrożenie podejścia polegającego na zmianie zarządzania: Należy przyjąć i wdrożyć metodologię zmiany zarządzania aby zapewnić wypełnienie założeń kampanii i zmianę w zakresie wiedzy i zachowania grupy docelowej
3	Uzyskanie odpowiedniego wsparcia i finansowania zarządzania: należy pozyskać akceptację i wsparcie osób zainteresowanych / wyższej kadry kierowniczej. Należy poszukać partnerstw publiczno-prywatnych, jeśli jest to możliwe. Analiza kosztów i korzyści może być pomocna w określeniu potrzeb finansowych, a ustalenie korzyści wynikających z programu może pomóc w uzyskaniu akceptacji i finansowania
4	Określenie potrzeb kadrowych i materiałowych dla realizacji programu: należy upewnić się, czy zespół programowy i pracownicy mają odpowiednie umiejętności i doświadczenie w dziedzinach IT, HR, łączności, a także w szkoleniu i rozwoju. W celu ustalenia możliwych rozwiązań należy wykorzystać wiedzę państw członkowskich i innych źródeł informacji, takich jak Internet.
5	Ocena potencjalnych rozwiązań: przy ocenie potencjalnych rozwiązań należy wziąć pod uwagę partnerstwa publiczno-prywatne, a także czy dany program poszerzania wiedzy może zostać zaplanowany i wykonany wewnątrz organizacji czy konieczne jest skorzystanie z obsługi zewnętrznej
6	Wybór rozwiązania i procedury: po dokonaniu starannej oceny należy wybrać najlepsze rozwiązania i organizacje w celu wdrożenia programu poszerzania wiedzy
7	Opracowanie harmonogramu prac: należy rozpocząć tworzenie harmonogramu prac i zawrzeć główne działania, do których konieczne jest określenie potrzebnych zasobów, ram czasowych i etapów realizacji prac
8	Określenie celów i założeń: aby skutecznie zaplanować, zorganizować i ocenić program poszerzania wiedzy konieczne jest określenie celów i założeń programu
9	Określenie grup docelowych: bardzo istotne jest ustalenie i określenie konkretnej grupy, do której skierowana jest inicjatywa poszerzania wiedzy. Wszystkie grupy docelowe posiadają niepowtarzalne cele i potrzeby, a także funkcjonują w różnych środowiskach
10	Opracowanie programu i listy zadań: Konieczne jest skupienie działań na zaprojektowaniu programu, a także na dalszym rozwijaniu i realizacji planu. Należy również określić i opracować kluczowe wiadomości
11	Zdefiniowanie pojęcia informacji: skuteczny i sprawnie wdrożony plan przekazywania informacji ma decydujące znaczenie dla powodzenia programu poszerzającego wiedzę. Należy opracować strategię identyfikującą organy/organizacje, które mogą posłużyć jako kanały pośrednie bądź jako partnerzy. Treść wiadomości powinna być w dalszym stopniu rozwijana i sprawdzana,

- konieczne jest także ustalenie odpowiednich kanałów przekazywania informacji
- 12 Określenie wskaźników pomiaru powodzenia programu:** w celu oceny skuteczności programu poszerzającego wiedzę konieczne jest wyraźne ustalenie i opracowanie statystyk i kluczowych wskaźników wydajności
 - 13 Opracowanie linii odniesienia do ewaluacji:** poza określeniem statystyk i kluczowych wskaźników wydajności konieczne jest ustalenie aktualnej sytuacji dotyczącej grupy docelowej/ W ten sposób można ocenić skuteczność programu poszerzania wiedzy na podstawie zmian w sytuacji
 - 14 Udokumentowanie zdobytych doświadczeń:** w ustalanie doświadczeń zdobytych poprzez działania wykonane podczas pierwszego etapu należy włączyć kierownictwo programu i zespoły

II. Realizacja i zarządzanie

Nr	Pozycja listy kontrolnej
1	Potwierdzenie składu zespołu programowego: przed rozpoczęciem programu należy potwierdzić skład zespołu, który będzie odpowiadał zarówno za realizację, jak i za uzyskanie wyników. W trakcie realizacji inicjatywy i zarządzania nią każdy członek zespołu odpowiedzialnego za poszerzanie wiedzy powinien pełnić określoną rolę i obowiązki.
2	Przegląd harmonogramu prac: konieczne jest zaktualizowanie potrzeb harmonogramu prac i określenie etapów realizacji programu. Należy to wykonać przed rozpoczęciem programu, ponieważ zespół odpowiedzialny za poszerzanie wiedzy musi być świadom celów i założeń, a także wymogów budżetowych i ograniczeń projektu i stosować się do nich
3	Rozpoczęcie i wdrożenie programu: na tym etapie programu wszystkie protokoły i ustalenia powinny być już gotowe do wprowadzenia. Zespół odpowiedzialny za poszerzanie wiedzy i wszyscy partnerzy powinni wykonać wszelkie zadania dotyczące realizacji lub działania określone i przypisane im w harmonogramie prac
4	Przekazywanie informacji: należy wdrożyć plan przekazywania informacji i przekazać odpowiednie wiadomości właściwym grupom docelowym za pośrednictwem zamierzonych kanałów. Ważne jest, aby spróbować zebrać informacje zwrotne, ponieważ jest to związane ze statystykami i kluczowymi wskaźnikami wydajności, a także z ustalaniem zdobytych doświadczeń
5	Udokumentowanie zdobytych doświadczeń: należy ponownie wdrożyć procedury podobne do tych, które zostały wykorzystane pod koniec pierwszego etapu do udokumentowania zdobytych doświadczeń. Warto porównać rozwój programu z perspektywy zdobytych doświadczeń

III. Ewaluacja i dostosowanie

Nr	Pozycja listy kontrolnej
1	Przeprowadzenie ewaluacji: Konieczne jest zgromadzenie danych w celu ustalenia skuteczności programu i dokonania ilościowego i jakościowego pomiaru efektywności poszerzania wiedzy w zakresie bezpieczeństwa informacji, a więc i zmniejszenia liczby incydentów naruszenia bezpieczeństwa. Jednym ze sposobów przeprowadzenia ewaluacji jest zastosowanie ankiet kontrolnych i wieloaspektowych badań
2	Załączenie informacji zwrotnych: informacje zwrotne uzyskane przy przekazywaniu informacji programowych, powinny zostać przeanalizowane pod kątem ulepszenia przyszłych planów. Informacje te powinny zostać połączone z wynikami uzyskanymi ze statystyk ewaluacji.
3	Przegląd założeń programu: w dużym stopniu skuteczność programu poszerzania wiedzy może zostać ustalona poprzez odniesienie wyników do początkowych założeń. Jeżeli program wciąż trwa, może być konieczne ponowne rozważenie założeń w kontekście skuteczności
4	Wykorzystanie zdobytych doświadczeń: doświadczenia zdobyte w trakcie poprzednich etapów w połączeniu z informacjami zwrotnymi opartymi na planie przekazywania informacji mogą zostać wykorzystane do zwiększenia skuteczności trwających lub przyszłych programów. Ważne jest, aby wyciągać wnioski zarówno z działań skutecznych, jak i mniej udanych
5	Dostosowanie programu do potrzeb: jeżeli program wciąż trwa lub ma być ponownie realizowany, to dzięki wiedzy i rozumieniu wynikającym ze zdobytych do tej pory doświadczeń można program dostosować, aby zwiększyć jego skuteczność. Modyfikacje należy wprowadzać w taki sposób, aby zachować cele i założenia programu
6	Wznowienie programu: podczas wznowiania zmodyfikowanego programu należy powtórzyć zadania określone w etapie II. Należy położyć większy nacisk na działania zwiększające skuteczność programu poszerzania wiedzy

Więcej informacji na temat wszystkich etapów i związanych z nimi pozycjach listy kontrolnej można znaleźć w poradniku dla użytkowników [ENISA User Guide](#).

Statystyki / wskaźniki KPI

Definicje

Statystyki – System parametrów lub metod ilościowej oceny proces poddawanych pomiarowi oraz procesy potrzebne do przeprowadzenia takiego pomiaru.

Statystyki mogą być rozwijane i zmieniane na podstawie wiedzy nabywanej z czasem. Niektóre statystyki są autonomiczne, a inne są współzależne. Mogą one być dalej dzielone lub szczegółowo opisywane przy pomocy kluczowych wskaźników wydajności.

Kluczowe wskaźniki wydajności (KPI) – wymierne statystyki używane do oceny założeń w celu odzwierciedlenia wydajności organizacji. Wskaźniki KPI różnią się w zależności od charakteru organizacji. Należy wziąć pod uwagę różne warstwy i wymiary.

Wskaźniki KPI mogą być zarówno wskaźnikami ilościowymi, jak i jakościowymi, jednakże najbardziej użyteczne i powszechne są wskaźniki ilościowe. Zalicza się do nich między innymi wskaźniki liczbowe takie jak liczba obywateli, do których skierowana jest dana inicjatywa, ilość incydentów naruszenia bezpieczeństwa w ubiegłym roku w porównaniu z ubiegłymi latami i liczba odwiedzin w przypadku strony internetowej.

Aby ułatwić określenie planowanego poziomu i pomiaru wydajności (w tym wykorzystania statystyk i wskaźników KPI), można zastosować kilka instrumentów zarządzania strategicznego, takich jak Balanced Scorecard (Zrównoważona Karta Wyników) bądź Six Sigma.

Ewaluacja skuteczności

Wiele publicznych i prywatnych organizacji, które rozpoczęły inicjatywy poszerzające wiedzę w państwach członkowskich, nie zastosowało statystyk ani określonych wskaźników KPI, które mogą być wykorzystane do ilościowego określenia wartości programu poszerzania wiedzy. Ewaluacja przeprowadzonych kampanii jest bardzo istotna ze względu na zebranie zgromadzonych doświadczeń i wykorzystanie ich przy przyszłych inicjatywach. W ten sposób można nie tylko zwiększyć skuteczność przyszłych programów, ale również organizacja będzie mogła prześledzić czy programy poszerzania wiedzy poprawiają bezpieczeństwo informacji w przypadku przedsiębiorstw i obywateli.

Zajmowanie się grupami docelowymi

Warto zauważyć, że tej samej statystyki dotyczącej ewaluacji nie można powszechnie stosować w odniesieniu do wszystkich grup docelowych, gdyż cele i potrzeby, a także sytuacja użytkownika, bardzo się różnią między różnymi grupami.

Przy próbie określenia statystyk służących do ewaluacji kampanii skierowanych do użytkowników prywatnych i do MŚP (są to grupy docelowe, do których kierowana jest większość inicjatyw poszerzania wiedzy w dziedzinie bezpieczeństwa informacji) należy wziąć pod uwagę kilka zasadniczych kwestii:

- Programy poszerzania wiedzy skierowane do MŚP powinny skupiać się na potrzebie opracowania i wdrożenia strategii bezpieczeństwa informacji, jak również proponować środki stosowania się do strategii obowiązującej wewnątrz organizacji. Dotyczy to również organizacji w sektorze publicznym
- Władze publiczne nie zawsze są w stanie opracować strategię dotyczące bezpieczeństwa informacji dla użytkowników prywatnych. Dlatego też należy skupić się na opracowaniu „zalecanych wskazówek” lub „najlepszych praktyk” w odniesieniu do bezpieczeństwa informacji i propagować je w społeczeństwie.

Aby lepiej zrozumieć rozmaite zewnętrzne wpływy na grupy docelowe można posłużyć się narzędziami stosowanymi głównie w przedsiębiorczości, np. analizą PESTEL (analiza polityczna, środowiskowa, społeczna, technologiczna, ekologiczna i prawna).

Ustalenie głównych czynników decydujących o skuteczności

Przy próbie ustalenia statystyk i wskaźników KPI odpowiednich dla grupy docelowej bardzo ważne jest określenie głównych czynników decydujących o skuteczności w odniesieniu do danej grupy. Powinny to być kluczowe kryteria zwiększające szanse na pozytywny wpływ behawioralny na grupę docelową poprzez wykonany program poszerzania wiedzy. Na przykład:

Użytkownicy prywatni:

„Linie odniesienia” obecnego statusu należy ustalić przed wdrożeniem (lub zmodyfikowaniem) programu poszerzania wiedzy

Skierowane do użytkowników prywatnych programy poszerzania wiedzy w dziedzinie bezpieczeństwa nie będą skuteczne, jeżeli nie dotrą do docelowej grupy odbiorców. W celu rozpowszechnienia informacji należy wykorzystywać organizacje pozarządowe, instytucje, banki, ISP, biblioteki, lokalne przedsiębiorstwa handlowe, domy kultury, programy kształcenia dla osób dorosłych, szkoły i organizacje skupiające rodziców i nauczycieli.

Rozgłos ma podstawowe znaczenie w kampanii na rzecz poszerzania wiedzy, ponieważ zwiększa wpływ ponosząc liczbę osób, do których dociera wiadomość.

MŚP

„Linie odniesienia” obecnego statusu należy ustalić przed wdrożeniem (lub zmodyfikowaniem) programu poszerzania wiedzy

Programy poszerzania wiedzy w dziedzinie bezpieczeństwa informacji skierowane do MŚP nie będą skuteczne, jeżeli będą sprzeczne z kulturą organizacyjną lub nie będą wspierane przez kadrę kierowniczą wyższego szczebla.

Jednakże budowanie stałego wsparcia dla programów skierowanych dla MŚP wymaga przedstawienia skuteczności działań mających na celu poszerzanie wiedzy.

Ustalanie linii odniesienia do ewaluacji

Aby móc zastosować statystyki i wskaźniki KPI do pomiaru skuteczności lub wpływu programu poszerzania wiedzy, należy ustalić linię odniesienia obecnego statusu otoczenia. Jeśli uprzednio oceni się sytuację grupy docelowej, możliwe jest dostrzeżenie korzyści wynikających z programu poszerzania wiedzy.

Ankiety i wieloaspektowe badania to jedne ze sposobów ewaluacji skuteczności programów. Jeżeli stosuje się np. taką metodę zbierania danych należy zauważyć, że podobne ankiety i badania powinny być ponownie użyte w przyszłych etapach inicjatywy po przeprowadzeniu kampanii. Umożliwi to porównanie ewaluacji po zakończeniu inicjatywy z linią odniesienia.

Zagwarantowanie dokładnego pomiaru

Przy próbie zastosowania statystyk i wskaźników KPI do oceny skuteczności kampanii, należy powziąć kilka zasadniczych kroków, gwarantujących dokładny pomiar wartości programu poszerzania wiedzy.

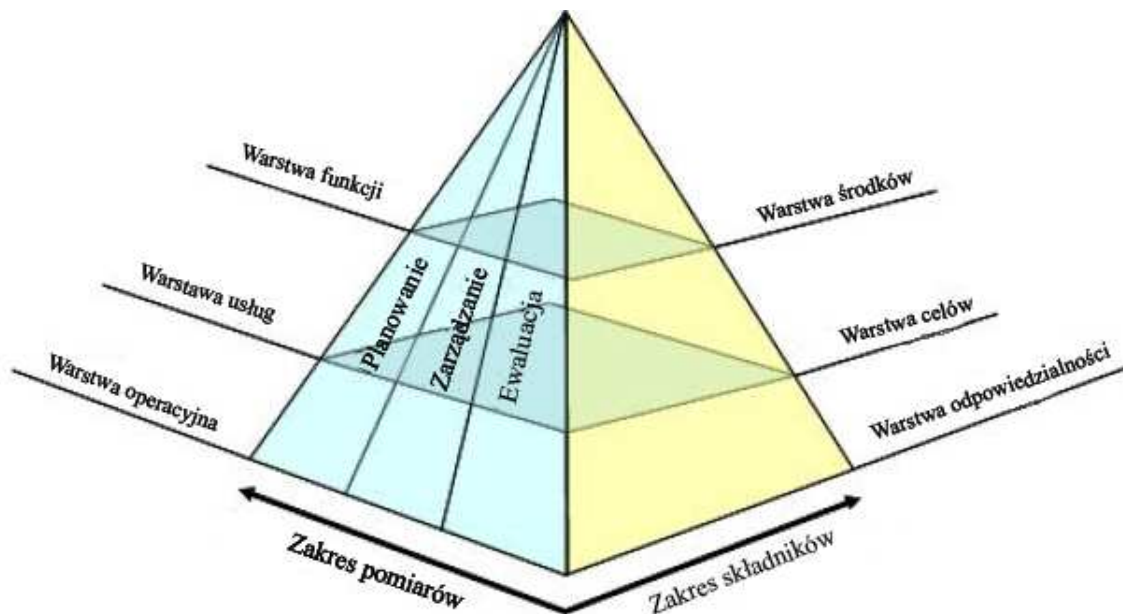
1. Należy określić procesy, zadania i działania konieczne do przeprowadzenia kampanii poszerzania wiedzy
2. Należy ustalić statystyki i wskaźniki KPI do pomiaru wiedzy w dziedzinie bezpieczeństwa
3. Należy odwzorować wskaźniki KPI dla odpowiednich procesów i działań

1.1. Określenie procesów, zadań i działań

Na początku każdej inicjatywy poszerzania wiedzy, poza pozycjami opisanymi szczegółowo w części [Listy kontrolne](#) należy wyraźnie określić zadania i działania specyficzne dla procesów i kampanii. Zazwyczaj każdy proces wymaga własnych wskaźników i kryteriów wydajności. Dlatego też niektóre procesy i działania będą odwzorowane względem statystyk / wskaźników KPI, co umożliwi monitorowanie i zgłaszanie konkretnych postępów i wyników.

2. Określenie statystyki i wskaźników KPI

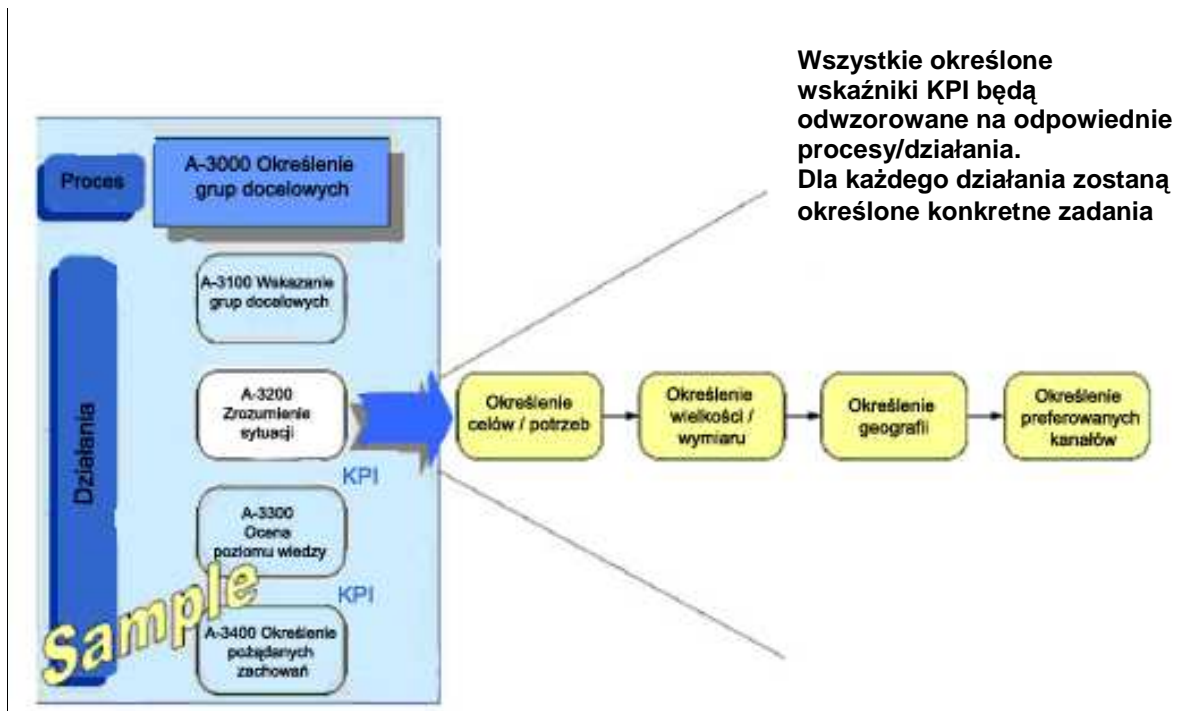
Przy tworzeniu statystyk i wskaźników KPI należy wziąć pod uwagę różne warstwy i wymiary.



Przykłady wskaźników KPI, które można wykorzystać przy próbie pomiaru skuteczności instytucji poszerzania wiedzy, można znaleźć w dokumencie [sample kpis.pdf](#). Dokument ten zawiera listę przykładowych wskaźników KPI, zebranych z wielu źródeł.

3. Odzworowanie wskaźników KPI na procesy

Po ustaleniu procesów, zadań/działań i statystyk/wskaźników KPI możliwe jest odzworowanie różnych czynników łącznie. Proces ten zapewnia właściwą obserwację i pomiar każdego istotnego posunięcia. Przykład:



Mierzenie skuteczności

Poziom wiedzy o bezpieczeństwie można mierzyć stosując i dostosowując statystyki proponowane przez firmę Gartner. Przy mierzeniu skuteczności każdego programu poszerzania wiedzy można zastosować cztery kategorie:

- *Ulepszenie procesu:* Kategoria ta dotyczy opracowania, rozpowszechnienia i rozmieszczenia zalecanych wskazówek w zakresie bezpieczeństwa, a także szkolenia w dziedzinie poszerzania wiedzy. Przykładowe statystyki ewaluacji uwzględniają następujące kwestie:
 - Dla użytkowników prywatnych – jaki odsetek badanych osób wie o istnieniu zalecanych wskazówek dotyczących bezpieczeństwa? Ile osób widziało je lub przeczytało?
 - Dla MŚP – jaki odsetek pracowników MŚP wie o istnieniu strategii bezpieczeństwa? Ile osób zapoznało się z nią?

- *Odporność na ataki:* Kategoria ta dotyczy rozpoznawania wydarzenia związanego z bezpieczeństwem informacji i odporności na atak. Przykładowe statystyki ewaluacji uwzględniają następujące kwestie:
 - Dla użytkowników prywatnych – jaki odsetek użytkowników nie ujawnił swojego hasła dostępu podczas testu?
 - Dla MŚP – jaki odsetek administratorów IT lub pracowników pomocy technicznej nie potrafił zapobiec niedozwolonej próbie zmiany hasła?
- *Wydajność i skuteczność:* Kategoria ta skupia się na wydajności i skuteczności w odniesieniu do incydentów naruszenia bezpieczeństwa. Przykładowe statystyki ewaluacji uwzględniają następującą kwestię:
 - Dla użytkowników prywatnych/MŚP – jaki odsetek incydentów naruszenia bezpieczeństwa, z którymi zetknęły się konkretne osoby, wynikał głównie z postępowania człowieka?
- *Wewnętrzna ochrona:* Kategoria ta dotyczy tego, jak dobrze dana osoba chroniona jest przed potencjalnymi zagrożeniami. Przykładowe statystyki ewaluacji uwzględniają następującą kwestię:
- Dla użytkowników prywatnych/MŚP – jaki odsetek systemów danych osób miał zainstalowane pirackie oprogramowanie?

Gromadzenie danych

Przy gromadzeniu danych do pomiaru wydajności inicjatyw poszerzania wiedzy zalecane jest zbieranie zarówno informacji ilościowych, jak i jakościowych. Dane powinny być gromadzone w sposób ciągły (ponieważ mierzenie wydajności i monitorowanie skuteczności inicjatywy powinno być przeprowadzane w trakcie realizacji i po niej) i najlepiej poprzez zautomatyzowane procesy.

Do metod gromadzenia danych zalicza się m.in. kwestionariusze, statystyki odwiedzania stron internetowych, ogólne obserwacje, statystyki centrów danych, grupy dyskusyjne, dane z punktów informacji telefonicznej/punktów kontaktowych, liczba zgłoszeń do obsługi IT, wycinki prasowe, biuletyny, komunikaty prasowe, liczba rejestracji na usługi sieciowe i liczba przeszkolonych osób.

Więcej szczegółowych informacji na temat stosowania statystyk i wskaźników KPI w przypadku inicjatyw poszerzanie wiedzy można znaleźć w części *Określenie wskaźników pomiaru powodzenia programu* Poradnika ENISA dla użytkowników [enisa a users guide how to raise is awareness.pdf](#).

Plan działań

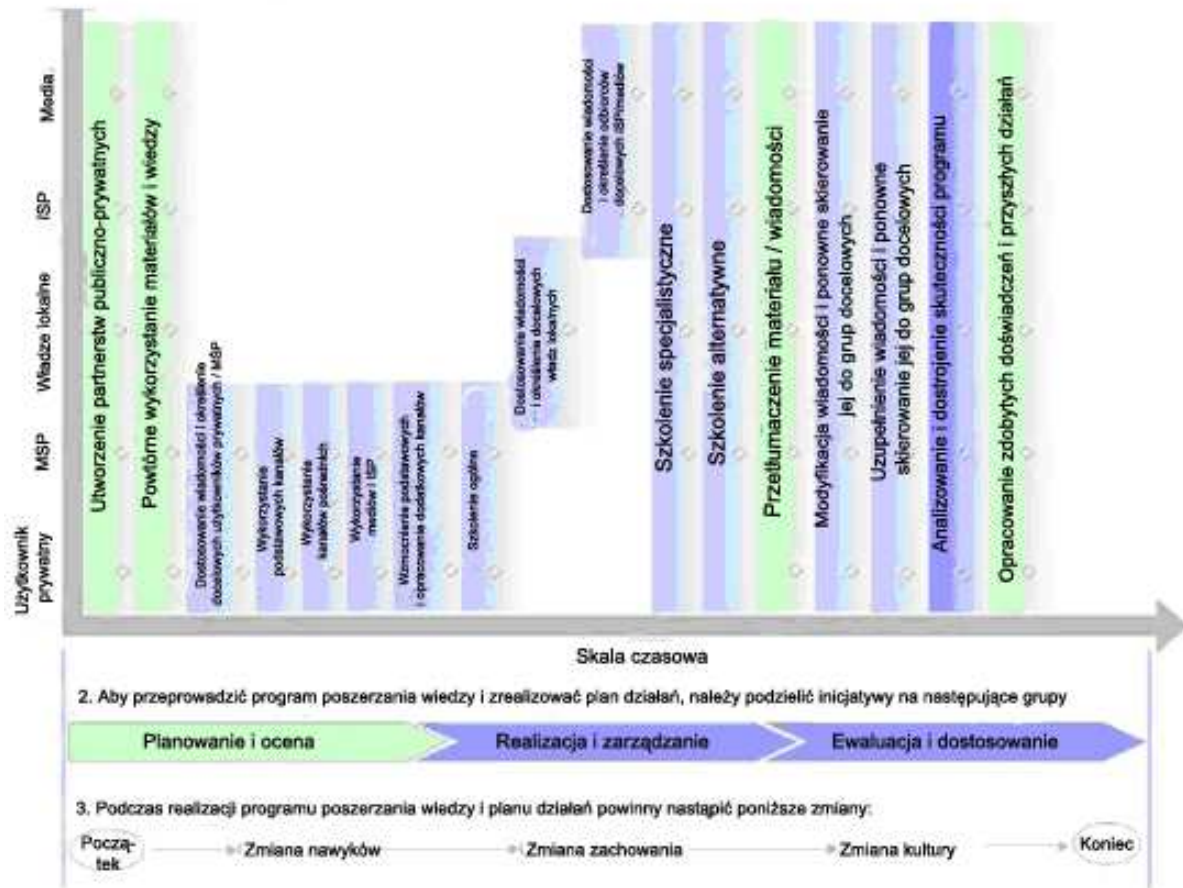
Poniższy schemat ilustruje, w jaki sposób państwo członkowskie może naszkicować i wdrożyć plan działań poszerzania wiedzy służącej zwiększeniu świadomości w dziedzinie bezpieczeństwa informacji. Schemat ten powinien być wykorzystany jedynie jako przykład (ponieważ strategia, zadania i działania mogą różnić się w zależności od celów danego państwa i jego obecnej sytuacji).

Przy analizowaniu schematu należy posługiwać się kluczem kolorystycznym, który pomaga w grupowaniu poszczególnych pozycji planu:

Klucz kolorystyczny:

	Pozycja planu działań jest zwykle wykonywana jednorazowo i dlatego nie musi być prowadzona realizowana w sposób ciągły. W niektórych przypadkach zestaw zadań i działań może zostać powtórzony, ale jedynie w ograniczonym zakresie.
	Pozycja planu działań jest zwykle wykonywana w określonej kolejności i trwa od danego momentu. Dlatego też po zainicjowaniu zestaw zadań i działań jest wykonywany w sposób ciągły
	Pozycja planu działań jest zwykle wykonywana przy rozpoczęciu programu poszerzania wiedzy, w jego trakcie i pod koniec tego programu. Dlatego też zestaw zadań i działań jest wykonywany w sposób ciągły w trakcie całego trwania inicjatywy

1. Przykładowy plan działań poszerzania planu



Klucz do pozycji planu działań:

Utworzenie partnerstw publiczno-prywatnych – np. sięgających od przedsiębiorstw IT po organizacje społeczne

Powtórne wykorzystanie materiałów i wiedzy – np. wykorzystanie materiałów programowych i wiedzy innych państw członkowskich, jeśli jest to możliwe

Dostosowanie wiadomości i określenie docelowych użytkowników prywatnych / MŚP – np. utworzenie kluczowej wiadomości odpowiedniej dla grupy docelowej i dostarczenie tej wiadomości

Wykorzystanie podstawowych kanałów – np. opracowanie i uruchomienie stron internetowych

Wykorzystanie kanałów pośrednich – np. wykorzystanie osób takich jak nauczyciele, które mogą dotrzeć do większej liczby odbiorców

Wykorzystanie mediów i ISP – np. współpraca z mediami i ISP jako kanałami przekazywania informacji i wykorzystywanie ich

Wzmocnienie podstawowych i opracowanie dodatkowych kanałów – np. poprawienie funkcjonalności stron internetowych (zwiększenie interaktywności) lub uruchomienie innych kanałów, takich jak telefoniczne linie specjalne

Szkolenie ogólne – np. wydarzenia publiczne i sesje szkoleniowe w poszerzaniu wiedzy, przeznaczone dla ogółu społeczeństwa

Dostosowanie wiadomości i określenie docelowych władz lokalnych – np. utworzenie kluczowej wiadomości odpowiedniej dla grupy docelowej i dostarczenie tej wiadomości

Dostosowanie wiadomości i określenie docelowych ISP/mediów – np. utworzenie kluczowej wiadomości odpowiedniej dla grupy docelowej i dostarczenie tej wiadomości

Szkolenie specjalistyczne – np. sesje zajęć lub kursy instruktorskie obejmujące funkcje odpowiednie dla ról

Szkolenie alternatywne - np. programy szkoleniowe typu e-learning

Przetłumaczenie materiału / wiadomości - np. przełożenie wiadomości kampanii na wiele języków

Modyfikacja wiadomości i ponowne skierowanie jej do grup docelowych – np. dodanie do kluczowych wiadomości tematów takich jak technologia WiFi i bezpieczeństwo telefonów komórkowych

Uzupełnienie wiadomości i ponowne skierowanie jej do grup docelowych – np. dodanie wiadomości bardziej szczegółowych lub odpowiednich dla danej organizacji, takich jak technologia pull-print, zwiększająca bezpieczeństwo urządzeń drukujących i skanujących

Analizowanie i dostrojenie skuteczności programu – np. przeprowadzenie testów porównawczych z liniami odniesienia, a także zastosowanie statystyk i kluczowych wskaźników wydajności

Opracowanie zdobytych doświadczeń i przyszłych działań – np. opracowanie zaleceń, a także przekazanie wiedzy zespołom i państwom członkowskim

Inne materiały

Polecane materiały

[The Promotion of a Culture of Security for Information Systems and Networks in OECD Countries](#) [Promowanie kultury bezpieczeństwa w sieciach i systemach informacyjnych w państwach OECD], Grupa Robocza ds. Bezpieczeństwa Informacji i Prywatności, grudzień 2005 r. (dokument)

[OECD Annual Report](#) [Raport roczny OECD], 45. rocznica, 2005 r. (dokument)

[Implementation Plan](#) for the OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security [Plan wdrażania wytycznych OECD dotyczących bezpieczeństwa sieci i systemów informacyjnych: w kierunku bezpieczeństwa informacji, 2003 r. (dokument)

Strona internetowa OECD poświęcona kulturze bezpieczeństwa informacji, <http://webdomino1.oecd.org/COMNET/STI/lccpSecu.nsf?OpenDatabase>

[A Users' Guide: How to Raise Information Security Awareness](#) [Poradnik dla użytkowników: Jak poszerzyć wiedzę o bezpieczeństwie informacji] (dokument)

[Measuring effectiveness of awareness programmes](#) [Pomiar skuteczności programu poszerzania wiedzy] (prezentacja)

Pliki elektroniczne

W „Pakiecie informacji na rok 2006” odniesiono się do następujących plików elektronicznych:

Plik	Język
2005_33_sakerhetsinfo_internetanv.pdf	szwedzki/ angielski
accord_afa_famille_avec_logo.pdf	francuski
banniere_cegetel3.gif	francuski
charte_d'engagements_des_op_contenu_multimedia-signée.pdf	francuski
dti_info_security_2006.pdf	angielski
e-crime_wales_action_plan_final2.pdf	angielski
enisa_a_users_guide_how_to_raise_its_awareness.pdf	angielski
enisa_info_security_awareness_programmes_eu.pdf	angielski
enisa_questionnaire_2006_v.5.0_final.pdf	angielski
neufkit2.jpg	angielski
oecd_annual_report_2005.pdf	angielski
oecd_implementation_plan.pdf	angielski
ppp_for_a_safer_internet.pdf	angielski
report_on_the_promotion_of_a_culture_of_security.pdf	angielski
safenethome_annualreport2005.pdf	angielski
sample_kpis.pdf	angielski
sweden_survey.pdf	angielski
the_threats_english.pdf	angielski
thehumanfactor-isf2004040903_v2.pdf	angielski
us_national_cyber_security_awareness_month_2005_summary_2.pdf	angielski