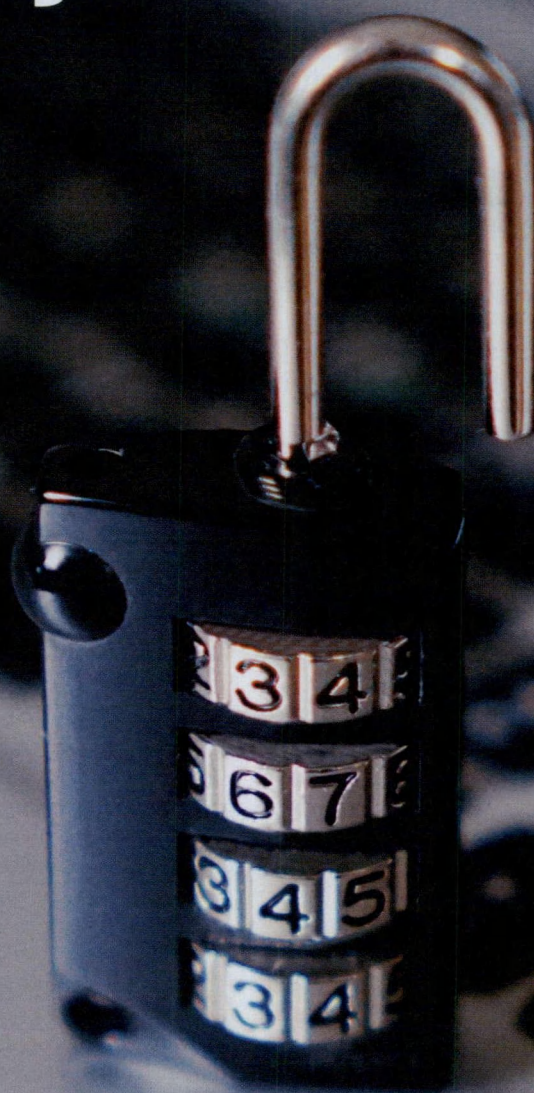


Próba oceny ryzyka przed wejściem RODO

W łańcuchu zabezpieczeń każdy element ma znaczenie, a ich złamanie polega na złamaniu najsłabszego ogniwa. Przy połączeniu systemu z siecią publiczną nad zabezpieczeniem tego systemu czuwa jedna, najwyżej kilka osób.

W tym samym czasie nad złamaniem zabezpieczenia mogą pracować tysiące osób z różnych miejsc na całym świecie. Przygotowując się do wejścia w życie RODO, powinniśmy wiedzieć, jakie ryzyka i zagrożenia niesie stosowane w szkole czy urzędzie rozwiązanie wykorzystywane do przetwarzania danych.

Autor: Dominik Krzysztofowicz



Generalny inspektor ochrony danych osobowych organizuje cykl szkoleń dla administratorów bezpieczeństwa informacji (ABI), którzy pod koniec maja staną się inspektorami ochrony danych osobowych. „Wspólnota” objęła patronatem jedno z takich szkoleń skierowane dla ABI ze szkół podstawowych i ponadpodstawowych, podczas którego Andrzej Kaczmarek, dyrektor Departamentu Informatyki w biurze GODO, opowiadał o tym, na co zwrócić szczególną uwagę oceniając bezpieczeństwo danych w szkole.

Jak rozumieć bezpieczeństwo?

Oceniając rozwiązania w zakresie przetwarzania informacji zastosowane w szkole, urzędzie czy jakiegokolwiek innej organizacji, należy skoncentrować się na tym, czy są one bezpieczne, czy nie dochodzi do ujawnienia informacji, nielegalnej zmiany informacji itd. Istotne jest, aby zrozumieć, czym jest bezpieczeństwo w przypadku danych. Rozumiane powinno ono być jako stan, w którym jednostka nie odczuwa zagrożenia swojego istnienia, a także przetrwania danych nawet w okresie kryzysowym. Chodzi o sytuację, w której istnieją formalne, instytucjonalne i praktyczne gwarancje ochrony. Rozpatrując bezpieczeństwo informacji, warto skoncentrować się na atrybutach bezpieczeństwa związanych z dostępem do niej. Chodzi o zapewnienie, by ta informacja była poufna (jeśli taka ma być), nie nastąpił nielegalny dostęp do niej itp.

Dla bezpieczeństwa informacji najważniejsze są 3 atrybuty, które określa norma PN-ISO/IEC 27000:2014: poufność, integralność i dostępność. Poufność należy rozumieć jako właściwość zapewniającą, że informacja nie jest udostępniana lub ujawniana nieautoryzowanym osobom, procesom, czyli jest dostępna tylko dla osób upoważnionych. Integralność to właściwość zapewniająca, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany, że te, które są przetwarzane, nie ulegną zmianie. Dostępność z kolei umożliwia wykorzystanie informacji na żądanie, w założonym czasie, przez kogoś, kto ma do tego prawo.

Bezpieczeństwo informacji w szkole

Mówiąc o przetwarzaniu danych w szkołach jeszcze niedawno mieli

śmy na myśli dane zgromadzone w segregatorach, szafach. Zresztą w niektórych przypadkach takie przetwarzanie nadal istnieje. Mówiąc więc o zabezpieczeniu danych, mamy na myśli zabezpieczenie dostępu do segregatorów i szaf. Rozwój techniki zawitał jednak do szkół, gdzie zastępuje rozwiązania „analogowe”, np. zamiast dzienników papierowych są systemy informatyczne. To o wiele większe wyzwanie dla zapewnienia bezpieczeństwa informacji, które często gromadzą firmy zewnętrzne. W przypadku systemów informatycznych należy pamiętać, że coraz częściej łączą się z innymi jednostkami, np. z systemem ZUS, przetwarzając dane pracowników, komisji egzaminacyjnej. Zabezpieczenie danych gromadzonych cyfrowo wiąże się z zabezpieczeniem nie tylko komputera, z którego można uzyskać dostęp do takich danych, ale i linii komunikacyjnych, przez które dane są przesyłane i oczywiście miejsc ich przechowywania, np. chmury obliczeniowej.

Identyfikacja źródeł zagrożenia

Na bezpieczeństwo systemu informatycznego wpływa wiele elementów, które należy wziąć pod uwagę w procesie analizy ryzyka: zarządzanie ludźmi (ich uprawnienia, kompetencje), zarządzanie bezpieczeństwem informacji, bezpieczeństwo środowiska systemu, procedury, zabezpieczenia fizyczne, strefy bezpieczeństwa, dostęp do pomieszczeń, zarządzenia związane z przetwarzaniem informacji. Każde z nich może stanowić zagrożenie dla bezpieczeństwa systemów informatycznych. Zagrożenia związane z bezpieczeństwem biorą się bowiem ze słabości.

Słabość rozwiązań informatycznych może skutkować podatnością na ujawnienie czy utratę integralności danych. W wielu przypadkach wciąż są wykorzystywane podstawowe protokoły do przesyłania informacji, np. TCP/IP. Jak najbardziej możemy ich używać, jeśli przesyłamy dane w obrębie jednego budynku i mamy pod kontrolą połączenia między komputerami. Jeśli jednak przesył odbywa się pomiędzy naszą organizacją a instytucjami zewnętrznymi, należy zdać sobie sprawę, że informacja poprzez publiczne linie telekomunikacyjne przekazywana jest dalej. W przypadku da-

nych osobowych nie można zatem używać niezabezpieczonych protokołów, ale takich, które zabezpieczenia posiadają, np. IPsec i IP v6. W przypadku przeglądania stron internetowych warto zamiast standardowego protokołu HTTP używać zabezpieczonego HTTPS, który szyfruje dane. A w przypadku poczty elektronicznej standardowym protokołem jest SMTP, który umożliwia uzyskanie informacji, kto jest nadawcą, odbiorcą, a nawet treści przesyłanej wiadomości. Do bezpiecznego przesyłania poczty służy inny protokół: S/MIME. To, czy nasza poczta albo strona, z której korzystamy, są bezpieczne, można sprawdzić za pomocą strony www.internet.nl. Warto jednak pamiętać, że to rozwiązanie ocenia bezpieczeństwo poczty na linii nadawca – serwer. Nie ocenia zaś bezpieczeństwa od serwera do komputera odbiorcy.

Innym źródłem zagrożeń może być korzystanie z publicznych sieci, np. hot-spotów. W przypadku łączenia się z siecią w taki sposób trzeba mieć świadomość, że każdy ma dostęp do treści, które są tam przesyłane. Taka sieć może być zatem przydatna w przypadku sprawdzania rozkładu jazdy autobusu, ale nie można z niej korzystać wykonując transakcję w banku.

Żeby skutecznie zabezpieczyć system, należy usunąć wszystkie jego słabości i podatność na znane rodzaje ataków, jak i ataki, które mogą pojawić się w przyszłości. Trzeba mieć świadomość niebezpieczeństwa wiążącego się z tym, że nasz komputer jest widoczny w całej sieci internet.

W łańcuchu zabezpieczeń każdy element ma znaczenie, a złamanie zabezpieczeń polega na złamaniu najsłabszego ogniwa. Przy połączeniu systemu z siecią publiczną nad jego zabezpieczeniem czuwa najczęściej jedna, najwyżej kilka osób. W tym samym czasie nad złamaniem zabezpieczenia mogą pracować tysiące osób na całym świecie. Dlatego tak ważne jest stosowanie systemów antywirusowych, antyspamowych i innych elementów, które poprawiają bezpieczeństwo i zablokują ataki. Problem jednak w tym, że jeśli padniemy ofiarą dedykowanego ataku, to ktoś przygotowywał się do niego nawet przez rok i stosuje narzędzia, których system nie będzie w stanie wykryć.

Socjotechnika

Źródłem zagrożenia nie muszą być wyłącznie systemy i technologie. Nie bez znaczenia jest świadomość użytkowników w zakresie tego, jakie ataki mogą wystąpić i skąd mogą przyjść. Osoby planujące atak często wykorzystują socjotechnikę do pozyskania informacji. O co chodzi?

Kevin Mitnick stwierdził kiedyś, że socjotechnika nie polega na łamaniu haseł, systemów, a na łamaniu ludzi. Używany jest podstęp. Jedną z metod jest rosyłanie maila do pracowników, który miał być adresowany wyłącznie do działu HR, a „przypadkiem trafił do wszystkich”. Znajdująca się w nim informacja (np. o planowanych premiach) zachęca do otwarcia załącznika, a ten z kolei może zawierać wirusa. Oczywiście informacja stwarza pozory legalności i w stopce jest informacja, że „jeśli wiadomość

W procesie szacowania ryzyka pomocne mogą być np. normy PN-ISO/IEC 27001, PN-ISO/IEC 27002 w zakresie bezpieczeństwa informacji. Istotne będą też normy zarządzania jakością PN-ISO/IEC 9001:2015. W przypadku zarządzania ryzykiem przydatna stanie się norma ISO 31000 oraz PN-ISO/IEC 27005:2011.

nie jest skierowana do ciebie to ją zignoruj”. Mało kto jednak powstrzyma się od sprawdzenia, co się w załączniku znajduje.

Inny sposób to np. telefon wykonany do ABI po jego wyjściu z pracy w piątek z prośbą od szefa o hasło do jakichś zasobów, które są pilnie potrzebne. Powszechnie znane są również strony podszywające się pod prawdziwe, np. bankowe.

Szacowanie ryzyka – wzór

Przystępując do analizy ryzyka, najważniejszą sprawą jest posiadanie informacji o strukturze organizacji. O wszystkich procesach, narzędziach, jakie są w niej wykorzystywane i w ja-

kim celu. Jeśli taką wiedzę mamy, to możemy zidentyfikować zagrożenia, ocenić ryzyko ich wystąpienia oraz przewidzieć skutki. Mając prawdopodobieństwo i skutek, możemy z kolei ocenić ryzyko.

Ryzyko można wyliczyć np. jako iloczyn prawdopodobieństwa wystąpienia i skutku. W takim rozwiązaniu skutek jest oceniany dla utraty poufności, dla utraty integralności i dla dostępności danych.

Podczas doboru wartości przypisywanej skutkowi utraty poufności (S_p) należy przyjąć zasadę, że:

$S_p = 0$ jeśli utrata poufności jest niemożliwa

$S_p = 1$ jeśli utrata poufności dotyczy spraw mniejszej wagi i odnosi się do pojedynczych przypadków

$S_p = 2$ jeśli utrata poufności dotyczy informacji wrażliwych lub odnosi się do licznych przypadków, ale nie wiąże się z odpowiedzialnością karną lub administracyjną

$S_p = 3$ jeśli utrata poufności dotyczy informacji wrażliwych lub odnosi się do licznych przypadków, wpływa znacząco na wizerunek urzędu lub organu, jednak nie wiąże się z odpowiedzialnością karną, ale może wiązać się z odpowiedzialnością administracyjną

$S_p = 4$ jeżeli utrata poufności może prowadzić do naruszenia interesów osób trzecich i prowadzić do roszczeń odszkodowawczych oraz wiąże się z odpowiedzialnością karną osób odpowiedzialnych za zapewnienie ochrony danych.

Podobnie oceniamy skutek utraty integralności (S_i) i dostępności (S_d).

Na koniec obliczamy poziom ryzyka według wzoru: $R_p = P \times (S_p + S_i + S_d)$, gdzie: R_p to pierwotny poziom ryzyka; P to wartość przypisana prawdopodobieństwu materializacji zagrożenia, gdzie P może być równe 0, jeśli coś nie może się zdarzyć, bo nie ma np. danego rozwiązania, 1 – mamy rozwiązanie, ale zdarza się bardzo rzadko, 2 – zdarza się częściej itd. aż do 4.

W ten sposób maksymalnie możemy osiągnąć wynik 49. Ten wynik określi nam poziom ryzyka przy założeniu, że według reguły Pereta, jeśli ryzyko jest niższe niż 20 proc., to można bez problemu korzystać z rozwiązania. Dla przykładu, wynik 10 da nam małe ryzyko, 21 – średnie, 37 – wysokie, a 41 – bardzo wysokie ryzyko. ■

Wymagania dotyczące bezpieczeństwa danych wynikające z RODO

W art. 24 ust. 1 RODO zapisano, że uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych, administrator wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z rozporządzeniem i aby móc to wykazać. Dalej w RODO czytamy (art. 35), że uwzględniając charakter, zakres, kontekst, cele i ryzyko, administrator zarówno przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania wdraża odpowiednie środki techniczne i organizacyjne, takie jak pseudonimizacja, minimalizacja danych i inne zabezpieczenia w celu skutecznej realizacji zasad ochrony danych, aby chronić prawa osób, których danych dotyczą.

W RODO znajdziemy takie podpowiedzi dotyczące zabezpieczenia danych, jak np. pseudonimizacja i szyfrowanie danych. To jednak jedynie kierunki działania, a nie konkretne rozwiązania. W praktyce pojawia się wiele wątpliwości: jak rozdzielić dane identyfikacyjne od pozostałych, kiedy szyfrować dane, jakie metody szyfrowania zastosować? W różnych przypadkach mogą zostać zastosowane różne rozwiązania. Tym jednak powinni zająć się specjaliści, a nie administratorzy danych. Często takimi specjalistami będą twórcy i dostawcy narzędzi, z których korzystamy w organizacji. Po naszej stronie jest jednak żądanie uzupełnienia zapisów w umowach licencyjnych. Zgodnie z RODO w przypadku powierzenia danych (np. dziennika elektronicznego prowadzonego na zewnątrz), musimy w umowach zawrzeć dodatkowy element, zgodnie z którym w przypadku naruszenia ochrony danych dostawca rozwiązania pomoże ustalić jego przyczynę i opracować zalecenia w celu zmniejszenia skutków ujawnienia danych. To dotyczy również umów dotyczących systemów finansowych, księgowych, bibliotek itd.