

I OGÓLNOPOLSKI KONGRES ZARZĄDZANIA CIĄGŁOŚCIĄ DZIAŁANIA

PARTNER

KAŻDY POWINIEN BYĆ GOTOWY NA KRYZYS



Zarządzanie ciągłością działania ma coraz większe znaczenie dla funkcjonowania zarówno prywatnych firm, jak i sektora publicznego

– Istnieje około stu definicji kryzysu. Wynika z tego, że jest bardzo dużo podejść do zarządzania kryzysowego – powiedział podczas jednego z pierwszych wystąpień na I Ogólnopolskim Kongresie Zarządzania Ciągłością Działania Jakub Arcisz z wydziału bezpieczeństwa i zarządzania kryzysowego Podlaskiego Urzędu Wojewódzkiego w Białymstoku. Stu kilkudziesięciu specjalistów od ciągłości działania, zarządzania kryzysowego, ryzyka operacyjnego oraz bezpieczeństwa informacji przez dwa dni omawiało w podwarszawskiej Jachrance różne aspekty związane z ryzykiem dla niezagrażonego funkcjonowania firm, instytucji finansowych, a także administracji publicznej.

Dariusz Romańczuk, partner zarządzający w firmie Business Continuity Management Group, która wspólnie z DGP była organizatorem kongresu, podkreślał znaczenie odpowiedniego ujęcia problematyki ciągłości działania w ładzie korporacyjnym każdej firmy. – Kluczowa jest tu rola zarządów i rad nadzorczych. Jeśli na tym poziomie nie ma świadomości zarządzania ciągłością działania, to trudno tu mówić o jakimkolwiek systemie zarządzania – podkreślał Romańczuk.

Wskazał, że problematyka została dostrzeżona przez Komisję Nadzoru Finansowego w odniesieniu do firm finansowych, a także przez Giełdę Papierów Wartościowych w zakresie spółek publicznych. KNF latem ubiegłego roku wydała „Zasady ładu korporacyjnego dla instytucji nadzorowanych” regulujące zasady corporate governance podmiotów rynku finansowego. Szef BCMG podkreślał niektóre zapisy zasad przyjętych przez KNF. Zgodnie z nimi nadzorowane instytucje powinny „sporządzić i stosować plany ciągłości działania mające na celu zapewnianie ciągłości działania i ograniczenia strat na wypadek poważnych zakłóceń w działalności”. Powinny też „skutecznie zarządzać ryzykiem występującym w działalności, w szczególności poprzez opracowanie i wdrożenie adekwatnego i skutecznego systemu zarządzania ryzykiem”.

– Giełda w 2002 r. po raz pierwszy przyjęła kodeks dobrych praktyk spółek publicznych. Podejście GPW jest podobne jak innych europejskich giełd: notowane spółki nie muszą stosować wszystkich zasad, ale muszą oświadczyć, z których rezygnują i dlaczego – dodał Dariusz Romańczuk. Tu kluczowa jest zasada, że „spółka powinna prowadzić przejrzystą i efektywną politykę informacyjną, zarówno z wykorzystaniem tradycyjnych metod, jak i z użyciem nowoczesnych technologii oraz najnowszych narzędzi komunikacji zapewniających szybkość, bezpieczeństwo oraz efektywny dostęp do informacji”.

Z perspektywy problematyki ciągłości działania kluczowe jest funkcjonowanie w firmie systemów informatycznych. Szef BCMG wskazał w tym zakresie obowiązującą normę ISO/IEC 38500, dotyczącą zasad nadzoru nad IT w firmie.

Z funkcjonowaniem IT związane jest bezpieczeństwo informacji. Mówił o tym Andrzej Lewiński, zastępca generalnego inspektora ochrony danych osobowych. Przedstawił on zmiany, jakie od początku tego roku wprowadzono w ustawie o ochronie danych osobowych. – Kluczowe znaczenie będzie miał teraz administrator bezpieczeństwa informacji – zaznaczył Lewiński. Administrator, czyli ABI, ma się zajmować sprawdzaniem zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych, zapoznawaniem z tymi przepisami osób upoważnionych do przetwarzania danych. ABI jest też odpowiedzialny za dokumentację dotyczącą sposobu przetwarzania danych i wykorzystywanych do tego środków. Dotychczas w rejestrze ABI jest ok. 800 podmiotów, które zgłosiły swoich administratorów. Jest na to czas do 30 czerwca br.

Andrzej Lewiński podkreślał też, że kwestia ochrony danych osobowych będzie wymagała od przedsiębiorstw coraz większej uwagi: – Wpływy danych są niebezpieczne m.in. dlatego, że powodują ryzyko pojawienia się roszczeń. Dziś zgłaszać przypadki wpływu danych muszą tylko operatorzy telefoniczni. To się jednak zmienia. A w bankach o wpływie danych trzeba będzie powiadamiać klientów.

Skąd biorą się wycieki danych? Według Joanny Brylikowskiej, dyrektor biura bezpieczeństwa informacji w Provident Polska, najczęściej ich źródłem są byli lub obecni pracownicy firm. Według przywołanych przez nią badań dotyczy to ponad



trzech czwartych przypadków wyciekania informacji. – To oznacza, że zagrożenie ma zwykle charakter wewnętrzny. Ja dzielę osoby, które doprowadzają do wycieku danych, na trzy grupy: nieświadomych, mściwych oraz zapobiegliwych, którzy pożyczają informacje z nadzieją, że przydadzą im się one w przyszłości – mówiła Brylikowska. Jej zdaniem najskuteczniejszym sposobem ochrony przed takimi sytuacjami jest edukacja pracowników. – To niezbędny element skutecznego systemu zarządzania bezpieczeństwem informacji. Ale trzeba też powiedzieć, że jeśli to ma być skuteczne, to powinien być to proces, a nie doraźne działanie – oceniła przedstawicielka Providenta.

Uczestnicy kongresu podkreślali znaczenie współpracy biznesu z administracją. – Żadnego z istotnych problemów dzisiejszego świata nie da się rozwiązać bez biznesu – argumentował Andrzej Sadłowski, dyrektor departamentu bezpieczeństwa w Banku Ochrony Środowiska. Według niego firmy są na pierwszej linii frontu. One też dysponują pieniędzmi na opracowywanie nowych rozwiązań, a ponadto mają doświadczenie w wykorzystywaniu zaawansowanych metod zarządzania i nowoczesnych technologii. Sadłowski zaznaczył jednak, że w Polsce biznes i administracja to wciąż dwa różne światy, a rola organów państwa cały czas jest postrzegana jako „represyjna, a nie organizatorska”. Inne jest też podejście: w biznesie mówi się o zarządzaniu ciągłością działania, natomiast państwo nadal posługuje się koncepcją zarządzania kryzysowego, czyli reakcji na pojawiające się zagrożenia, a nie przeciwdziałania im zawczasu.

Paweł Gromek z Katedry Inżynierii Bezpieczeństwa Szkoły Głównej Służby Pożarniczej zwracał z kolei uwagę na korzyści, jakie biznes może odnosić ze współpracy ze strukturami państwowymi, na przykładzie straży pożarnej. – Warunek jest taki, by szukać możliwości w ograniczeniach, a nie ograniczeń w możliwościach – zaznaczył. Wskazywał, że firmy i tak są zobowiązane do realizacji obowiązków wynikających z przepisów przeciwpożarowych. Podał też kilka przykładów udanej kooperacji firm i straży pożarnej, np. w organizacji ćwiczeń, audytach bezpieczeństwa pożarowego czy wspólnych inicjatywach naukowo-badawczych.

W trakcie kongresu zaprezentowano kilka studiów przypadku dotyczących zarządzania ciągłością działania i ochroną informacji w konkretnych firmach. Monika Sobczyk, kierownik ds. bezpieczeństwa informacji w firmie Medcover, przybliżyła proces certyfikacji systemu zarządzania bezpieczeństwem danych w ramach normy ISO 27001. Zwracała również uwagę na znaczenie kierownictwa. – Bez wsparcia zarządu, osób decyzyjnych nic by

się nie udało. W takim procesie ważne jest to, by nie zabić biznesu, by nie tworzyć procedur, które uniemożliwiają bieżącą pracę – tłumaczyła. Ale też zwracała uwagę na korzyści z wykonanej pracy: opracowane dokumenty były wykorzystane do budowania strategii i procedur na niższym szczeblu. Podkreślała też ograniczenia, jakie w dziedzinie bezpieczeństwa informacji ciążyą na podmiotach działających w branży ochrony zdrowia – np. to, że dane medyczne mają status szczególnie chronionych, a dokumentacja medyczna nie może istnieć wyłącznie w postaci zdigitalizowanej.

Jeszcze bardziej skomplikowana sytuacja w dziedzinie dostępu do informacji jest w międzynarodowych grupach finansowych, jak np. Citigroup. Dariusz Dylski, menedżer odpowiedzialny za ID Administration w Citibanku na Węgrzech, mówił o tym, że w tej grupie, działającej praktycznie na całym świecie, funkcjonuje równocześnie ok. 10 tys. różnych systemów mających przeszło milion użytkowników. Tu problemem jest zapewnienie bezpiecznego dostępu. – Największym zagrożeniem, a jednocześnie najsłabszym punktem systemu ochrony jest proces wnioskowania i weryfikacji – stwierdził Dylski.

Sprawne procedury dotyczące zapewnienia ciągłości działania są istotne w branży finansowej, ale także dla firm zajmujących się dostarczaniem mediów, np. dostawców energii elektrycznej. Według Aleksandra Rzepey, koordynatora BCP w biurze ryzyka i systemów bezpieczeństwa firmy Energa-Operator, wdrożenie i certyfikacja rozwiązań z dziedziny business continuity przyczyniły się nie tylko do wzmocnienia bezpieczeństwa pracy i funkcjonowania firmy, lecz także do oczekiwanej przez klientów i akcjonariuszy niezawodności w działaniu. Rzepa podawał dane dotyczące tempa przywracania zasilania po przejściu w 2014 r. orkanu „Ksawery” i tegorocznego orkanu „Felix”. Rok temu jeszcze po trzech dniach nie udało się załatwić wszystkich awarii. W tym roku na pełne przywrócenie zasilania trzeba było czekać niespełna 48 godzin.

Istotna jest jednak nie tylko sprawność operacyjna. Jak argumentowała Alina Geniusz-Siuchnińska, rzeczniczka prasowa Energi-Operatora, dla ochrony reputacji spółki kluczowa jest komunikacja kryzysowa. Można ją zapewnić na różne sposoby – najlepiej jeśli odpowiednie narzędzia powstaną, zanim nastąpi sytuacja kryzysowa. W przypadku Energi-Operatora są to np. bieżące informacje na stronie internetowej dotyczące wyłączeń prądu czy umożliwienie klientom zgłaszania awarii SMS-em.

Jan Dajek jan.dajek@infor.pl