

Proste przyczyny, takie jak brak profilaktyki czy lekkomyślność mogą doprowadzić samorządy do kłopotów, w tym utraty pieniędzy. Cyberprzestępcy nie śpią i atakują także JST.

12 kwietnia w Sali Kolumnowej w Sejmie odbyła się konferencja pt. *Cyberbezpieczeństwo w jednostkach samorządu terytorialnego*. Zorganizowała ją sejmowa Komisja Samorządu Terytorialnego i Polityki Regionalnej, Polska Izba Informatyki i Telekomunikacji, Związek Powiatów Polskich oraz Związek Miast Polskich.

Spotkanie otworzył Andrzej Maciejewski, przewodniczący Komisji Samorządu Terytorialnego i Polityki Regionalnej. W swoim wystąpieniu poseł podkreślał, że jest to spotkanie przedstawicieli środowiska biznesowego i samorządowego. *Spotkanie bardzo potrzebne, ponieważ na temat bezpieczeństwa w Internecie coraz częściej zaczyna się mówić.*

- Długo żyliśmy w niewiedzy, a dziś mamy już doświadczenia. Kilka gmin straciło pieniądze, rekordziscie ubyło ok. miliona złotych. Ataki są banalnie proste. Przeważnie powstają z banalnych przyczyn, takich jak brak profilaktyki, lekkomyślność, czy niedbałość – tłumaczył. Dlatego tak ważna jest edukacja w tym zakresie. Przewodniczący zapowiedział, że cyberbezpieczeństwo będzie jeszcze omawiane w ramach prac Komisji. Jednak należy sobie zdawać sprawę, że kwestia ochrony systemów informatycznych nie jest taka prosta. Jak zapowiedział Andrzej Maciejewski, *do stawienia czoła problemowi bezpieczeństwa w sieci potrzebna będzie koalicja na gruncie praktycznym i ustawodawczym po to, aby walkę móc skutecznie wygrać.*

Dobre praktyki

Taką m.in. rolę spełnić ma porozumienie trójstronne zawarte niedawno między PIIT, ZPP i ZMP. Michał Rogalski, wiceprezes PIIT wyjaśniał, że celem porozumienia *jest stworzenie platformy wymiany informacji na temat technologii teleinformatycznych, ale nie tylko pod kątem nowym rozwiązań technicznych, które stale się pojawiają, ale także w odniesieniu do tego, jak takie rozwiązania wdrażać i jak je zamawiać.* Przypominał, że problem zamówień publicznych ciągle istnieje, przy czym dokonują się pozytywne zmiany w przepisach. Takie, które umożliwiają dokonywanie inwestycji przez JST, w tym w infrastrukturę teleinformatyczną. Przepisy nie uregulują jednak wszystkiego. Dlatego dużą wagę będą miały dobre praktyki. Natomiast powstała platforma ma służyć m.in. wymianie doświadczeń w zakresie walki z atakami hakerskimi.

Edukacja to podstawa

O tym, jaki jest stan cyberbezpieczeństwa polskich samorządów mówił Jan Maciej Czajkowski, współprzewodniczący ze strony samorządowej Zespołu ds. Społeczeństwa Informacyjnego Komisji Wspólnej Rządu i Samorządu Terytorialnego. Podkreślał, że temat cyberbezpieczeństwa jest na tyle ważny i pilny, że nie należy go odkładać. Jest konsekwencją informatyzacji. Wraz z rozwojem technologii, doskonała się także działania hakerów. Im więcej zadań na rzecz mieszkańców wykonują samorządy, tym bardziej narozę są na różne niebezpieczeństwa, w tym takie jak blokowanie stron, czy kradzieże danych. Zagrożeń jest wiele, bo samorządy tworzą zarówno własne bazy danych, jak i wprowadzają dane do rejestrów centralnych. Im mniejsza jednostka, tym co do zasady słabsze jest jej przygotowanie do cyberataku. Problemem są tu głównie środki finansowe. Jak podważył ekspert, *jeśli JST będą chciały podjąć działania przeciw terroryzmowi, to będą musiały zaangażować swoje środki i będą to z reguły środki bieżące, czyli najbardziej wrażliwe jeśli chodzi o art. 243 ustawy o finansach*

Kategoria: Aktualności

Opublikowano: niedziela, 16, kwiecień 2017 08:50

Sylwia Cyrankiewicz-Gortyńska

Odśłony: 1819

publicznych. Ochrona bezpieczeństwa informacyjnego obciąża budżet operacyjny. Dlatego w ocenie Jana Macieja Czajkowskiego warto rozważyć możliwość wprowadzenia wsparcia centralnego dla samorządów. To, co zdaniem eksperta w relacjach rządowo – samorządowych z pewnością można robić, to prowadzić działania edukacyjne – szkolenia, standardy, wytyczne. - *To bardzo ważne, bo 90 % problemów związanych z cyberatakami wywołanych jest czynnikiem ludzkim* – uzasadniał Jan Maciej Czajkowski.

Nie tylko informatyk

Wojciech Dziomdziora, wiceprezes PIIT opowiadał o tym, jak przygotować urząd na atak cyber. W swojej prezentacji tłumaczył, że bardzo ważne jest zaangażowanie nie tylko pracowników działów IT, ale i innych, w tym działów prawnych czy prasowych. Tymczasem, z danych PIIT wynika, iż tylko 11 proc. pracowników samorządowych przeszło szkolenia z zakresu bezpieczeństwa informatycznego. Podawał przykłady cyberataków, które w ostatnim czasie miały miejsce w Polsce, dotyczyły one m.in. urzędów miast czy Komisji Nadzoru Finansowego.

Marcin Spychała z IBM zademonstrował wybrane techniki, dzięki którym można wejść w posiadanie danych zgromadzonych w komputerach czy smartfonach. Zagrożeniem jest choćby wi-fi.

O bezpieczeństwie rozwiązań opartych na technologii chmury mówił Michał Jaworski z Microsoft.

Bartłomiej Michałowski z Orange Polska podpowiadał, jak radykalnie poprawić cyberbezpieczeństwo polskich samorządów. Zwracał uwagę na to, jaką wagę ma kupowanie usług od profesjonalnych dostawców. Janusz Żmudziński z Asseco Data Systems S.A. zwracał uwagę na monitoring cyberbezpieczeństwa.

Joanna Bańkowska i Kamil Galicki reprezentujący firmę IKG Technology tłumaczyli, jakie wymogi w zakresie ochrony danych osobowych niesie rozporządzenie RODO. Z kolei do cyberpolis przekonywał Marcel Góra z kancelarii APLaw.

Natomiast Xawery Konarski i Agnieszka Wachowska, prawnicy z kancelarii Traple, Konarski, Podrecki opowiadali o zakresie odpowiedzialności karnej i administracyjnej za naruszenia cyberbezpieczeństwa.

Transmisja konferencji dostępna jest [TUTAJ](#).