Kategoria: Wywiady
Opublikowano: sobota, 29, kwiecień 2017 18:52
Sylwia Cyrankiewicz-Gortyńska

O cyberatakach mówimy coraz częściej. O tym, na jakie zagrożenia narażone są systemy informatyczne jednostek samorządu terytorialnego Dziennikowi Warto Wiedzieć opowiada dr Jan Maciej Czajkowski, współprzewodniczący ze strony samorządowej Zespołu ds. Społeczeństwa Informacyjnego Komisji Wspólnej Rządu i Samorządu Terytorialnego, laureat nagrody Polskiej Izby Informatyki i Telekomunikacji za rok 2016 przyznawanej osobom szczególnie zasłużonym dla rozwoju rynku środowiska teleinformatycznego.

Dziennik Warto Wiedzieć: W jakich obszarach JST są szczególnie narażone na cyberataki? Co należy robić, aby im zapobiegać?

Jan Maciej Czajkowski: Specyfika poszczególnych grup JST jest różna. Również pod kątem ochrony bezpieczeństwa systemów informatycznych. Myślę, że warto tu przyjąć motto *periculum in mora* (niebezpieczeństwo w oczekiwaniu, w zwłoce, w działaniu). A to dlatego, że temat ochrony systemów teleinformatycznych w JST jest na tyle pilny z uwagi na rosnące zagrożenia, że nie powinniśmy go odkładać na później.

Niezbędne jest tu stworzenie w tej sprawie stałej formuły współpracy między korporacjami samorządowymi, przynajmniej Związkiem Miast Polskich, Związkiem Powiatów Polskich i Związkiem Gmin Wiejskich RP. Dwie pierwsze z tych organizacji podpisały właśnie porozumienie o współpracy z Polską Izbą Informatyki i Telekomunikacji. To bardzo ważny krok, gdyż taka linia współpracy sektora biznesowego i samorządowego, umożliwiająca na bieżąco wymianę informacji jest potrzebna.

Konieczność zapewnienia cyberbezpieczeństwa dotyczy całej administracji publicznej. Istnieje ostatnio przygotowywany przez Ministerstwo Cyfryzacji dokument: Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022. Obejmuje on całe państwo – sektor publiczny (rząd, samorząd) i prywatny (biznes, mieszkańcy), czyli wszystkie podmioty, które w tym państwie funkcjonują. W części rządowej można pewne rzeczy zadekretować i wprowadzać odgórnie. I tak powinno być. Rząd w aspektach związanych z cyfryzacją powoli zaczyna być postrzegany jako jedna struktura a nie szereg odrębnych ministerstw. Miejmy nadzieję, że ten proces nie zostanie zatrzymany i będzie się rozwijał i trwał.

DWW: Czyli mechanizmy bezpieczeństwa, standardy na poziomie rządowym można wprowadzać odgórnie i wszystkie jednostki rządowe będą się musiały do tego stosować?

JMC: Tak i jest to ta łatwiejsza część związana z cyberbezpieczeństwem w sektorze publicznym. Jeśli natomiast chcielibyśmy mówić o tym, że trzeba się zająć wsparciem cyberbezpieczeństwa w samorządzie, to mamy dużo bardziej skomplikowaną sytuację.

DWW: Co ma Pan na myśli?

JMC: Wynika to z tego, że mamy ok. 2800 różnego rodzaju jednostek samorządowych. Mamy zatem gminy, w tym gminy miejskie i miejsko wiejskie. Mamy miasta na prawach powiatu, które są odrębną kategorią. Mamy ponad 300 powiatów i 16 województw. To już pokazuje, że ta struktura jest złożona a w ślad za tym, również zadania poszczególnych samorządów są bardzo zróżnicowane. Najbardziej bezpośrednie relacje z mieszkańcami i biznesem mają gminy. Gminy, jako podstawowe jednostki samorządu terytorialnego, (w tym także miasta na prawach powiatu) mają do zrealizowania najwięcej zadań na rzecz mieszkańców. I tam też występuje najwięcej problemów, jeśli chodzi o

cyberbezpieczeństwo. Drugą znaczącą grupą, która realizuje ważną część zadań na rzecz mieszkańców są powiaty. Specyfika ich jest nieco inna ze względu na ich główne zadania, z myślą o których je tworzono. Powiaty miały z założenia realizować raczej zadania związane z nadzorem, kontrolą, a także inne zadania zlecone ustawami, mają więc zwykle mniej dochodów własnych w budżecie niż gminy. Województwa z kolei reprezentują już poziom zbliżony bardziej do skali państwa. Ich rola jest bardziej integrująca, postrzegana raczej jako organizatorów polityki regionalnej a także jako centra wsparcia dla powiatów i gmin.

DWW: Gdzie w samorządach powstaje najwięcej zagrożeń związanych np. z utratą danych czy blokad stron?

JMC: Ewidentnie największe zagrożenia są w podstawowych jednostkach samorządu terytorialnego. Przy czym można jeszcze powiedzieć, że wśród gmin sytuacja jest dodatkowo „wewnętrzne" złożona. Są takie gminy, które mają większy potencjał w zakresie ochrony, chociażby ze względu na większe „wolne" dochody własne czy większy dostęp do zasobów informacji czy potencjału ludzkiego, są i takie, które mają te działania bardzo utrudnione, bo mają do dyspozycji znacząco ograniczone środki na najbliższe lata. No i jest jeszcze grupa pośrednia.

DWW: Których jednostek jest najwięcej?

JMC: Niestety tych, które mają te największe problemy. Może ich być nawet ponad tysiąc. Jeśli im nie udzieli się wsparcia, to same przed cyberatakami się nie obronią w takim zakresie, jakbyśmy tego oczekiwali. Dla nich trzeba by było znaleźć dostosowane do ich możliwości i zasobów pomysły na informatyzację realizowanych przez nie zadań publicznych i na zabezpieczenie ich przed cyberatakami. W dużych miastach sytuacja jest o tyle prostsza, że mają nominalnie większe zasoby, choć realnie obciążanie budżetów obsługą zaciągniętych zobowiązań w kolejnych najbliższych latach jest u nich większe, to i tak jest im łatwiej z uwagi na znacznie większą dostępność ekspertów, uczelni etc. Zresztą jest tak, że te największe miasta, budując swoje systemy, w jakimś stopniu zwykle uwzględniały już standardy związane z bezpieczeństwem teleinformatycznym.

Teraz powstają w Polsce duże „referencyjne" rejestry centralne, od kilku lat realizowane są projekty, które je budują. Jednostki z poziomu gminy czy powiatu wprowadzają czy będą wprowadzały bezpośrednio do nich dane, co też może być w pewnych warunkach drogą do przeprowadzenia ataku na sam rejestr centralny. Racjonalne jest oczywiście założenie, że mniejsza jest szansa na to, iż dojdzie do udanego ataku na dobrze zabezpieczony rejestr centralny niż na słabo zabezpieczoną jednostkę lokalną. Trzeba jednak pamiętać, że udany atak na duże centrum przetwarzania danych (a takie już się przecież na świecie zdarzały) niesie za sobą bez porównania większe szkody niż udany atak na lokalną małą jednostkę. Te dwa aspekty powinny być zawsze brane pod uwagę.

Z głównych rejestrów centralnych, do których jednostki z poziomu podstawowego wprowadzają dane można wymienić m.in: bazę usług stanu cywilnego, ewidencję ludności, centralną ewidencję pojazdów i kierowców, ewidencję gruntów i budynków. Są też rejestry branżowe, często zawierające wrażliwe dane, np. system informacji oświatowej czy rejestry związane z systemem ochrony zdrowia. Oprócz tego, że mamy JST, to przecież te jednostki mają także swoje szkoły, domy pomocy społecznej, itp., czyli jednostki organizacyjne. One też są podatne na zagrożenia w sferze informatycznej, a często są włączone w lokalną sieć teleinformatyczną. Jeśli gmina czy powiat ma środki, aby zaprojektować i zabezpieczać wewnętrzną sieć, to jest dobrze. Ale nie zawsze tak jest. Wtedy powstają kolejne miejsca narażone na

ataki. Trzeba zatem pamiętać o tym, że w ramach samorządu są i urzędy JST i ich jednostki organizacyjne, które też trzeba odpowiednio zabezpieczać przed atakami.

DWW: Wracając do małych gmin, warto wspomnieć, że są i takie, gdzie znaczniejsza informatyzacja praktycznie nie istnieje.

JMC: Tak. Są takie jednostki, w których jest elektroniczna skrzynka podawcza, (z uwagi na wymogi prawne) i kilka komputerów z podstawowymi aplikacjami. I tu cyberatak praktycznie nie będzie miał sensu z uwagi na brak poszukiwanych przez przestępców danych w „zasobach elektronicznych" takich JST. Warto zwrócić uwagę, że jeśli mamy myśleć o ich rozwoju i przyszłości w kierunku poszerzania usług świadczonych drogą elektroniczną także w tych jednostkach, to należy wyprzedzająco je zabezpieczyć (a przynajmniej podjąć niezbędne działania edukacyjno-szkoleniowe), aby w przyszłości mogły one wykonywać e-usługi bezpiecznie. Ponieważ nawet jeśli będą to usługi udostępniane im na platformie centralnej czy regionalnej, to ta relacja lokalny – centralny/regionalny będzie podatna na ataki.

DWW: Pojawił się jeszcze nowy aspekt zagrożeń związanych z fałszywymi „*newsami*", które mogą oddziaływać na opinię publiczną i np. wpływać na wyniki wyborów, jak to mogło mieć miejsce m.in. przy wyborach prezydenta USA.

JMC: To na razie dotyczyło wyborów w skali niektórych państw. Nie widzę jednak przeszkód, aby taki tani i łatwy do zastosowania mechanizm nie mógł być wykorzystywany przy wyborach regionalnych czy lokalnych. Jego opanowanie i zabezpieczenie się przed nim nie jest już takie łatwe. W moim przekonaniu takie zjawisko należy zakwalifikować w jakimś szerokim sensie, jako rodzaj „*miękkiego cyberterroryzmu"*.

DWW: Jak można wesprzeć sektor samorządowy z poziomu centralnego w ochronie przed elektronicznymi atakami z zewnątrz lub skutkami niefrasobliwości i braku wiedzy wewnątrz jednostki?

JMC: Wszystko kosztuje. Nie jest tak, że tego rodzaju skuteczne zabezpieczenia można wykonać bez nakładów finansowych.

Jednostki, które podejdą aktywnie do rosnących zagrożeń i będą chciały coś zmienić, będą musiały zainwestować, zaangażować w te działania swoje środki i będą to z reguły środki bieżące, czyli najbardziej wrażliwe, jeśli chodzi o art. 243 ustawy o finansach publicznych i limit indywidualnych zadłużeń. Chcę to wyraźnie podkreślić. Działania związane z ochroną bezpieczeństwa informatycznego muszą obciążyć budżet operacyjny a on już w niektórych przypadkach jest praktycznie obciążony do granic ustawowych. Trzeba mieć to w tyle głowy, aby móc mówić o cyberbezpieczeństwie państwa w części, dotyczącej sektora JST.

Rząd w budżecie jakieś środki zabezpieczy, ale nie bardzo widzę szansę, aby znaczące środki na poziomie samorządów w skali kraju można było na ten cel przeznaczać. Można by jednak próbować racjonalizować w JST np. wydatki na bezpieczeństwo publiczne i pewną (nawet niewielką) część z nich przeznaczać na ochronę cyberbezpieczeństwa, zamiast na „klasyczne" wydatki w tym zakresie.

To, co w relacjach rządowo-samorządowych z pewnością można robić, i o czym od dawna mówimy w samorządach, to prowadzić działania edukacyjne – szkolenia, podręczniki, standardy, wytyczne i

ustawiczne szkolenia dla tych pracowników, którzy zajmują się kwestią informatyzacji, bezpieczeństwa, ochrony danych, itd. Bez tego nie ma szansy na to, aby skutecznie i w możliwie pełnym zakresie realizować założenia strategii cyberbezpieczeństwa. Dotyczy to także poziomu rządowego. O ile wiem, działania rzecz edukacji i specjalistycznych szkoleń pracowników informatyki na kierowniczych stanowiskach w poszczególnych resortach zostały podjęte. W latach 2006-2007 powstał pomysł, aby stworzyć systemowy (np. w postaci rządowo-samorządowego centrum kompetencyjnego) mechanizm ustawicznej edukacji dla osób zajmujących się informatyzacją oraz dla decydentów w całym sektorze publicznym. Warto może do niego wrócić. Zwłaszcza, że 90 % problemów związanych z cyberatakami wywołanych jest czynnikiem ludzkim, najsłabszym ogniwem całego systemu. Ludzie bywają niefrasobliwi, lekceważąc wprowadzane zasady czy procedury, które ich zdaniem tylko utrudniają im pracę. Podkreślę raz jeszcze, że podstawową sprawą jest aktualna wiedza o zagrożeniach i sposobach zapobiegania im, którą pracownikom trzeba udostępnić. Ciągłe aktualizowanie tej wiedzy, z uwagi na wielką dynamikę zmian technologicznych i związaną z tym rosnącą skalą zagrożeń, potrzebne jest każdemu, szefowi urzędu, informatykowi, każdemu użytkownikowi sieci i systemu.

Dzięki temu można pokazać jak np. zmniejszyć ryzyko zagrożeń. Ten problem trzeba pilnie rozwiązać i tu jest moim zdaniem szerokie pole do współpracy nie tylko na linii rząd-samorząd, lecz także między samorządami a takimi organizacjami jak PIIT.

DWW: Czyli edukacja to podstawa. Czy na coś jeszcze warto zwrócić uwagę w kontekście ochrony systemów teleinformatycznych?

JMC: Sądzę, że warto też może pomyśleć o rozsądnym podejściu do wykorzystania na potrzeby e-usług przetwarzania w chmurze prywatnej, ale w części przypadków także i publicznej. Jak wykazują statystyki, te centra przetwarzania danych, które udostępniają usługi chmurowe, na ogół są bardzo dobrze zabezpieczone.

Jest jeszcze jeden aspekt związany z usługami mobilnymi, których – z uwagi na obecnie istniejące trendy rozwoju telekomunikacji się nie uniknie. Będą powstawały także w sektorze usług publicznych e-usługi przeznaczone dla takich właśnie urządzeń. Nadchodząca era ultraszybkich sieci radiowych 5G dodatkowo przyspieszy ten proces. Duża „przestrzenna koncentracja" ilości aktywnych urządzeń mobilnych w obszarach miejskich już powoduje, że właśnie tam urządzenia mobilne stają się celem różnego rodzaju cyberataków, i zjawisko to będzie się nasilało. Te urządzenia, jeśli nie zabezpieczy się ich odpowiednio i nie wyedukuje ich użytkowników, mogą być szczególnie zagrożone.

DWW: Serdecznie dziękuję za rozmowę.