Oswoić cyberbezpieczeństwo. Wywiad z Robertem Koślą

Kategoria: Wywiady
Opublikowano: piątek, 20, wrzesień 2019 11:26
Małgorzata Orłowska

„Z cyberbezpieczeństwem jest jak z dbaniem o własne zdrowie" – mówi Robert Kośla, Dyrektor Departamentu Cyberbezpieczeństwa w Ministerstwie Cyfryzacji i wyjaśnia, dlaczego tak ważne jest, byśmy zainteresowali się tematem bezpieczeństwa w sieci.

Pojęcie cyberbezpieczeństwa pojawia się coraz częściej, coraz więcej się o nim mówi. Wejście w życie zasad RODO również w znacznym stopniu uczuliło nas na kwestię bezpieczeństwa w sieci, a jednak mam wrażenie, że wciąż trochę traktujemy je po macoszemu. Czasem wydaje nam się, że to nas nie dotyczy, że zajmie się nim kto inny. Dlaczego tak ważne jest, aby na to cyberbezpieczeństwo jednak zwracać uwagę, zwłaszcza w jednostkach samorządu terytorialnego?

Robert Kośla: Podczas tegorocznego Forum Sekretarzy, w swojej prezentacji podkreślałem, że z cyberbezpieczeństwem jest jak z dbaniem o własne zdrowie. To analogiczna sytuacja – jedni się tym w ogóle nie przejmują dopóki coś się ze zdrowiem nie stanie, inni dbają od samego początku, stosują profilaktykę, mają świadomość zagrożeń dla zdrowia. To samo dotyczy cyberbezpieczeństwa. To jest tylko trochę bardziej miękka sfera, dlatego że to sfera cyfrowa. Cyberbezpieczeństwo dotyczy każdego z nas, bo wszyscy korzystamy z usług cyfrowych – osób wykluczonych cyfrowo jest dzisiaj coraz mniej i miejmy nadzieję, że niedługo nie będzie ich już w ogóle. Zatem praktycznie wszyscy mamy do czynienia z usługami cyfrowymi w życiu prywatnym, jak również w życiu zawodowym. Stąd konieczność przede wszystkim podnoszenia świadomości – musimy wiedzieć, co nam grozi i skąd owo zagrożenie płynie. Z drugiej strony musimy zdać sobie sprawę, co jest przedmiotem, co chcemy chronić. Trzeba wiedzieć, gdzie znajdują się nasze najcenniejsze informacje, a także to, czy mamy kopię tych informacji. To dotyka użytkowników indywidualnych, ale również przedsiębiorstwa, jednostki samorządu terytorialnego, służby publiczne. Mamy przykłady ze Stanów Zjednoczonych, gdzie ataki na systemy wymusiły na policji zapłacenie okupu za odszyfrowanie danych. W tej chwili na tym polega najprostszy model biznesowy przestępców – włamują się do systemu, który jest eksploatowany na poziomie jednostki samorządu terytorialnego i zaszyfrowują dane. Jeśli nie ma kopii tych danych poza macierzystym systemem, to urząd rzeczywiście jest uzależniony i w tym momencie jest to kwestia albo rezygnacji z możliwości przetwarzania danych osobowych, albo zapłata okupu. Takie przypadki są coraz częstsze i będą występowały na pewno jeszcze przez długi czas. Dzieje się tak pomimo tego, że dostępnych jest coraz więcej usług, które zwiększają odporność na ataki związane z szyfrowaniem i nieuprawnionym dostępem do informacji. One najczęściej bazują na wykorzystaniu usług chmur obliczeniowych, gdzie dostawcy wraz z usługą przetwarzania informacji dają usługę sporządzenia automatycznych kopii - kopii, które umożliwiają powrót do naszych danych od 30 do 60 dni wstecz. Więc gdybyśmy nawet padli ofiarą na skutek własnych, nieświadomych – bądź świadomych - działań wewnątrz organizacji, np. gdyby któryś z pracowników celowo doprowadził do zainfekowania wewnętrznego systemu, to jesteśmy w stanie odzyskać te dane, bo ich kopie są codziennie tworzone. To jest ten model, który będzie przewidywany, stąd ważność kwestii cyberbezpieczeństwa to tak naprawdę ważność tego, w jaki sposób – niezakłócony, niezachwiany, poprawny – możemy funkcjonować na niwie zarówno zawodowej, jak i prywatnej.

Co możemy robić, by o to bezpieczeństwo dbać na co dzień? Czy istnieją konkretne modele zachowań, narzędzia? W jaki sposób Ministerstwo Cyfryzacji pomaga w tym zakresie jednostkom samorządu terytorialnego?

Robert Kośla: Wejście w życie ustawy o Krajowym Systemie Cyberbezpieczeństwa, które *de facto* zostało wymuszone wejściem w życie dyrektywy o bezpieczeństwie sieci informacji, umożliwiło nam podjęcie prac nad budową Krajowego Systemu Cyberbezpieczeństwa. To nie jest jednorazowe działanie,

a złożony proces. Polega on przede wszystkim na podnoszeniu kompetencji osób funkcjonujących w administracji publicznej, zarówno w administracji rządowej i samorządowej, w podmiotach prywatnych, które odpowiadają za świadczenie usług kluczowych w sześciu sektorach: ochrona zdrowia, energia, transport, bankowość, finanse, usługi cyfrowe. To są również inwestycje w odpowiednie środki techniczne, to też system wymiany informacji o zagrożeniach. Te wszystkie elementy są wpisane w ustawę. Odpowiedzialność Ministra Cyfryzacji polega na tym, że ma zbudować system do wymiany informacji, do przekazywania zaleceń konfiguracyjnych, do wspomagania wszystkich podmiotów – czy to podmiotów prywatnych, czy publicznych, po to żeby przekazywać informacje o możliwych metodach ataków i sposobach ochrony przed nimi. Ale również system, który umożliwi zgłaszanie informacji o incydentach, jeśli ktoś już stanie się ofiarą ataku. Dowie się też wówczas w jaki sposób uzyskać pomoc. To są działania, które wynikają bezpośrednio z ustawy. Te działania są wspomagane przez rozpoczęte już programy budowy platformy edukacyjnej, e-learningowej nie tylko dla pracowników jednostek samorządu terytorialnego, ale generalnie dla obywateli. One zawierają moduły związane z cyberhigieną, czyli podstawami dbania o cyberbezpieczeństwo, ale również są przeznaczone dla osób, które odpowiadają za bezpieczeństwo w jednostkach samorządu terytorialnego, dla administratorów. Co więcej, w ślad za materiałami i programami edukacyjnymi w postaci elektronicznej, już w tym miesiącu rozpoczynamy szkolenia bezpośrednio w poszczególnych jednostkach samorządu terytorialnego. W pierwszej kolejności będą to szkolenia we współpracy z Urzędem Marszałkowskim Województwa Podlaskiego, następnie będą to kolejne miejscowości. Chcielibyśmy, by w przyszłym roku zostały przeszkolone już wszystkie województwa. Do szkoleń dochodzi jeszcze warstwa techniczna, czyli platforma do korzystania przez jednostki samorządu terytorialnego z zaufanych i bezpiecznych usług chmur obliczeniowych. Tutaj działania prowadzone są w ramach Wspólnej Infrastruktury Informatycznej Państwa (WIIP) – ta infrastruktura zakłada przeprowadzenie przetargu przez Centrum Obsługi Administracji Rządowej w KPRM na wybór komercyjnych usług chmur obliczeniowych. Po wyborze tych dostawców powstanie katalog usług i również dedykowany portal, na którym samorządy i administracja rządowa będą mogły zamawiać konkretne usługi, na przykład systemy baz danych, z katalogu, który zostanie wybrany w ramach przetargu. Co więcej – ten wybór i bezpośredni zakup usług będzie odbywał się już w trybie bezprzetargowym. De facto można porównać to do wizyty w sklepie i zakupu konkretnego rozwiązania, które z jednej strony będzie gwarantowane pod kątem standaryzacji bezpieczeństwa, jak również będzie zapewniało odpowiednią jakość usług, która będzie ujęta w samym postępowaniu przetargowym. Także mamy edukację, wsparcie w zakresie technicznym, a także liczymy na wejście w życie planów działania, które będą wynikały z nowej strategii cyberbezpieczeństwa. Tutaj dochodzą jeszcze kwestie partnerstwa publiczno-prywatnego, również rola przemysłu w udostępnianiu informacji – w jaki sposób korzystać z technologii, które są dostarczane do jednostek samorządu terytorialnego.