Cyberdefence 24

aut. Andrzej Kozłowski 21.07.2020

SAMORZĄDY POZA KONTROLĄ. MINISTERSTWO CYFRYZACJI NIE SPRAWDZI OPROGRAMOWANIA

Interpelację odnoszącą się do cyberataków na samorządy w Gminie Kościerzyna oraz Lututów skierowała grupa posłów Konfederacji. Posłowie pytali o poniesione straty, podmioty zaangażowane w rozwiązanie problemu, regulacje dotyczące używanego oprogramowania w samorządach oraz kwestie ubezpieczeń dla gmin od skutków cyberataku.

Minister cyfryzacji Marek Zagórski odpowiedział, że w przypadku ataku na gminę Kościerzyna udało się odzyskać dane we współpracy z Kaspersky Lab oraz zespołem NASK PIB. Prośby o pomoc do podmiotów zewnętrznych kierowane były przez gminę Kościerzyna za pośrednictwem osoby prywatnej zaangażowanej w działalność społeczną na szczeblu samorządowym, która wspierała gminę w koordynacji obsługi incydentu. Ministerstwo Cyfryzacji nie prowadziło analiz dotyczących strat poniesionych przez gminę, zwłaszcza wobec odzyskania przez nią danych, ponieważ incydent nie dotyczył rejestrów ani systemów we właściwości resortu. Minister cyfryzacji poinformował, że Prokuratura i Urząd Ochrony Danych Osobowych prowadzą postępowania w związku z tym incydentem.

W przypadku cyberataku na gminę Lututów, minister napisał, że dane zostały przywrócone z kopii zapasowych z wcześniejszego stanu. Mimo podjętej przez gminę współpracy m.in. ze specjalistami z Google, Microsoft i NASK klucz szyfrujący nie został złamany. Szef resortu cyfryzacji podkreślił, że nie jest możliwe dokładne określenie wysokości poniesionych strat. Wiele z nich ma charakter niepieniężny (utrata zaufania, wyciek danych osobowych, zmniejszenie poziomu bezpieczeństwa) lub jest trudna do oszacowania (uniemożliwienie dostępu do określonej usługi bądź obniżenie poziomu jakości jej świadczenia).

Posłowie zapytali ministra czy jego resort posiada wykaz jednostek samorządu terytorialnego używających oprogramowania Kaspersky Lab. Posłowie wskazują tutaj na rekomendacje brytyjskich i amerykańskich organizacji zajmujących się cyberbezpieczeństwem, aby przestać używać tego oprogramowania. Minister odpowiedział, że to do decyzji każdego podmiotu należy sposób świadczenia usług publicznych zgodnie z obowiązującymi przepisami regulującymi ochronę danych osobowych, wymogami działania systemów i rejestrów publicznych etc. Samorządy wykonują swoją część zadań publicznych w imieniu własnym i na własną odpowiedzialność. Odpowiedni dobór oprogramowania antywirusowego oraz odpowiedzialność za zakupione oprogramowanie leży w gestii poszczególnych podmiotów. Minister podkreślił, że resort nie ma narzędzi prawnych pozwalających na sprawdzanie, jakie oprogramowanie jest stosowane w poszczególnych jednostkach samorządu terytorialnego.

W interpelacji posłowie poruszyli też kwestie zawarcia polisy cyber przez gminy, powiaty itd., które były im oferowane. Minister zauważył, że konsekwencje przeprowadzonego ataku mogą być niezwykle poważne, stąd następuje stopniowy rozwój rynku tzw. cyberpolis – czyli ubezpieczeń od skutków ataków hakerskich.

Obecnie Ministerstwo Cyfryzacji monitoruje rozwój tego rodzaju usług. Stosowanie ubezpieczeń to dopuszczalny sposób postępowania z ryzykiem – pozwala przenieść je na stronę trzecią (czyli ubezpieczyciela). Nie jest jednak właściwe jako jedyny sposób postępowania z ryzykiem, zwłaszcza przy przetwarzaniu danych obywateli – zauważa minister.

Szef resortu cyfryzacji podkreśla, że Ministerstwo Cyfryzacji inicjuje działania i kampanie mające zwiększyć świadomość o cyberzagrożeniach. Wiele z podstawowych działań zabezpieczających ma charakter organizacyjny i nie wymaga inwestycji – niestety najwięcej zaniedbań jest w obszarze świadomości o cyberzagrożeniach i podstawowych zasadach cyberhigieny, czyli procedur bezpieczeństwa na poziomie użytkownika.

Ministerstwo Cyfryzacji prowadzi intensywne działania związane z podnoszeniem świadomości i kompetencji pracowników administracji publicznej, a w szczególności w jednostkach samorządu terytorialnego. W maju 2020 roku resort rozpoczął kampanię #CyberbezpiecznySamorząd, której głównym celem jest podniesienie poziomu odporności systemów informacyjnych administracji publicznej. Kampania obejmuje szkolenia, warsztaty i ćwiczenia, jak i bezpośrednie wsparcie jednostek samorządu terytorialnego w reagowaniu na zagrożenia w sieci.

Ponadto Ministerstwo w ramach platformy technologicznej udostępni narzędzia do publikacji bezpiecznych stron informacyjnych dla obywateli - samorzad.gov.pl wraz z systemem BIP. Rozwiązanie to będzie zapewniało możliwość integracji z istniejącymi systemami samorządów. Udostępnienie narzędzia jest zaplanowane na 2022 r., przy czym już rozpoczęły się działania pilotażowe z udziałem wybranych samorządów

W ramach „Planu Działań Ministra Cyfryzacji" resort zainicjował Program Wspólna Infrastruktura Informatyczna Państwa (WIIP), który ma na celu poprawę efektywności i bezpieczeństwa świadczenia usług przez administrację publiczną. Jednym z elementów programu jest umożliwienie korzystania przez urzędy z usług chmurowych, od sprawdzonych, zweryfikowanych dostawców, którzy zapewnią łatwiejszy dostęp do nowoczesnych technologii i bezpiecznych rozwiązań. Zapewnienia podmiotom administracji publicznej możliwości nabywania usług chmurowych od dostawców oraz wykorzystania zasobów chmury rządowej dostarczającej mocy obliczeniowej (serwerów oprogramowania, baz danych, sieci, narzędzi analitycznych, itp.), systemów bezpieczeństwa, bezpiecznych sieci teletransmisji itd. Ważnym elementem są, opublikowane przez Ministerstwo, Standardy Cyberbezpieczeństwa Chmur Obliczeniowych (SCCO), które stanowią zbiór wymagań prawnych, organizacyjnych i technicznych zapewniających cyberbezpieczeństwo w modelach wdrażania chmur obliczeniowych zarówno dla administracji publicznej, jak i dostawców usług chmurowych świadczących usługi sektorowi publicznemu. W celu ułatwienia współpracy pomiędzy urzędem a dostawcami w ww. zakresie wdrożono System Zapewniania Usług Chmurowych (ZUCH) dostępny pod adresem chmura.gov.pl, w którym zarejestrowało się już kilkudziesięciu reprezentantów administracji oraz dostawców.