Warszawa, dnia 08 sierpnia 2017 r.

RZECZPOSPOLITA POLSKA
MINISTER CYFRYZACJI

BM-WOP.072.107.2017

Pan
Marek Kuchciński
Marszałek Sejmu RP

Dot. przesłanej przy piśmie z dnia 26 lipca 2017 r. (sygn. DSP.INT.4810.429.2017) interpelacji Posła na Sejm RP Pana Wojciecha Wilka w sprawie *zabezpieczenia Polski przed atakami hakerskimi* (interpelacja nr 14303)

Szanowny Panie Marszałku,

oceny bezpieczeństwa systemów teleinformatycznych określonych instytucji na mocy przepisów ustawy *o działaniach antyterrorystycznych*[1] dokonuje ABW. Ponadto Szef ABW ma obowiązek prowadzenia rejestru zdarzeń naruszających bezpieczeństwo systemów teleinformatycznych[2]. W przypadku odnotowania zdarzenia naruszającego bezpieczeństwo wskazanych systemów ich administratorzy zobligowani są do niezwłocznego zgłaszania przypadków infekcji do Zespołu CERT.GOV.PL[3].

Niemniej jednak, wszystkie podmioty publiczne realizujące zadania w rozumieniu ustawy *o informatyzacji działalności podmiotów realizujących zadania publiczne*[4] (tj. organy administracji rządowej, organy kontroli państwowej i ochrony prawa, sądy, jednostki samorządu terytorialnego i in.) zobowiązane są posiadać system zarządzania bezpieczeństwem informacji. Rozporządzenie *o krajowych ramach interoperacyjności*[5] reguluje konieczne działania wchodzące w skład takiego systemu - w tym zapewnienie odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegające m.in.: na minimalizowaniu ryzyka utraty informacji w wyniku awarii i ochronie przed błędami, utratą czy nieuprawnioną modyfikacją. Należy założyć, że instytucje państwowe

[1] ustawa z dnia 10 czerwca 2016 r. *o działaniach antyterrorystycznych* (Dz. U. 2016 r. poz. 904)
[2] o których mowa w art.5 ust. 1 pkt 2a ustawy z dnia 24 maja 2002 r. *o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu* (t.j.: Dz. U. z 2016 r. poz. 1897)
[3] za pomocą poczty elektronicznej (incydent@cert.gov.pl) lub telefonicznie (48 225 859 373). W celu uproszczenia zgłaszania zdarzeń na stronie internetowej www.cert.gov.pl umieszczony jest formularz, który po wypełnieniu należy wysłać pod wskazany adres e-mail.
[4] Art. 2 ustawy z dnia 17 lutego 2005 r. *o informatyzacji działalności podmiotów realizujących zadania publiczne* (Dz. U. z 2017 r. poz. 570 z późn. zm.)
[5] §20 Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. *w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych* (Dz. U. z 2016 r. poz. 113, z późn. zm.).

spełniające minimalnie wymogi określone w rozporządzeniu, mają odpowiedni poziom bezpieczeństwa.

Działania na rzecz cyberbezpieczeństwa wymagają jednak zbudowania trwałych mechanizmów współpracy w tej dziedzinie. Z tego względu MC oraz instytut badawczy NASK w ramach inicjatywy Narodowego Centrum Cyberbezpieczeństwa[6] budują system partnerski w zakresie współpracy z kluczowymi podmiotami. NC Cyber to centrum wczesnego ostrzegania i szybkiego reagowania, a w razie ewentualnych ataków – koordynowania działań i wymiany informacji. Centrum funkcjonuje w trybie 24/7 przez 365 dni w roku. Szybka wymiana informacji między kluczowymi podmiotami ma szansę zapewnić skuteczne reagowanie na pojawiające się zagrożenia. NC Cyber współpracuje więc z przedsiębiorstwami telekomunikacyjnymi (Orange, Polkomtel, T-Mobile), branżą energetyczną (Energa, PSE, Gaz System, PERN), Związkiem Banków Polskich oraz bankami (Bank Zachodni WBK S.A., Credit-Agricole Bank Polska S.A., Bank Handlowy w Warszawie S.A., mBank S.A., Bank Millennium S.A., PKO BP S.A. oraz Raiffeisen Bank Polska S.A.) oraz innymi podmiotami m.in. z sektora transportowego czy chemicznego. W strukturze NC Cyber działa Zespół CERT Polska odpowiedzialny za reagowanie na incydenty. Zespół ten odpowiada również za rejestrowanie i obsługę zdarzeń naruszających bezpieczeństwo sieci, wykrywanie i analizę zagrożeń wymierzonych w szczególności w polskich internautów lub zagrażających domenie „.pl" oraz dynamiczne reagowanie w przypadku wystąpienia bezpośrednich zagrożeń dla polskich internautów. CERT Polska analizuje zagrożenia i monitoruje stan bezpieczeństwa polskiego Internetu. Przyczyną infekcji często jest niezachowanie należytych środków ostrożności przez użytkowników – stąd też nacisk położony na edukację użytkowników końcowych.

W strukturze Agencji Bezpieczeństwa Wewnętrznego funkcjonuje natomiast Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL. Jednym z jego podstawowych zadań jest zapewnianie i rozwijanie zdolności jednostek administracji rządowej do ochrony przed zagrożeniami płynącymi z cyberprzestrzeni. Od kilku lat Zespół CERT.GOV.PL obserwuje wzrost dynamiki ataków łączących różne metody i narzędzia. Infekcja oprogramowaniem złośliwym następuje przede wszystkim wskutek nieprzestrzegania podstawowych zasad bezpieczeństwa. Podatność komputera na atak zwiększa się z takich powodów jak brak aktualizacji systemu operacyjnego oraz oprogramowania użytkowego czy niestosowanie oprogramowania antywirusowego lub brak jego regularnych aktualizacji. Przyczyną infekcji może być także odwiedzenie zainfekowanej witryny lub nawet przypadkowe uruchomienie załącznika niezaufanej wiadomości z poczty elektronicznej (dotyczy to nie tylko pobierania i uruchamiania plików z sieci, ale również kopiowania danych z niesprawdzonych nośników). Wśród czynników zwiększających skuteczność ataków można wymienić również brak

[6] znajdującego się w strukturze NASK - dalej jako NC Cyber

odpowiednich procedur w instytucjach, brak wyspecjalizowanych zespołów czy pracowników odpowiedzialnych za reagowanie na incydenty, a także zmniejszanie środków finansowych przeznaczonych na bezpieczeństwo teleinformatyczne. W tym kontekście w instytucjach administracji publicznej kluczowe znaczenie mają szkolenia, zarówno dla nowych pracowników, jak i prowadzone cyklicznie dla całej kadry, a także przeprowadzanie testów bezpieczeństwa nowych systemów.

Jeśli chodzi o ilość ataków hackerskich w Polsce, na wstępie należy zaznaczyć, że brak jest definicji tego terminu. Atakiem hackerskim może być nie tylko użycie złośliwego oprogramowania (*malware*) – szpiegującego typu *trojan*, niszczącego pliki jak *wiper* albo szyfrującego typu *ransomware*. Polskie instytucje zajmujące się cyberbezpieczeństwem, takie jak CERT.PL czy też CERT.GOV.PL, na bieżąco śledzą najnowsze rodzaje niebezpiecznego oprogramowania i szukają sposobów jak im zapobiegać, jednak środki techniczne nie mogą pomóc, jeśli ofiara np. akcji phishingowej sama poda swoje dane (będzie to również atak, jednak nie zostanie on zarejestrowany jako próba włamania).

Należy pamiętać również o różnych zagrożeniach, które są związane z Internetem, jak np. przestępstwa (oszustwa, wyłudzenia, fałszywe sklepy), nieuczciwa konkurencja (fałszywe rejestry firm, podszywanie się pod inne firmy), naruszenia własności intelektualnej, niezamówiona korespondencja (spam) czy też cała sfera dotycząca bezpieczeństwa dzieci w Internecie (mowa nienawiści, *grooming*). Wszystkie te obszary przenikają się i nie ma jednolitego sposobu ich klasyfikacji. Z tego też względu brak jest w Polsce instytucji, która prowadziłaby pełne statystyki.

Ministerstwo Cyfryzacji posiada wiedzę o liczbie incydentów zgłoszonych do CERT Polska - w 2016 r. CERT Polska obsłużył 7275 zgłoszeń, na podstawie których zidentyfikowano 1926 incydentów[7]. W 2016 r. CERT Polska przetworzył automatycznie przy pomocy platformy n6 200 mln zgłoszeń dotyczących komputerów z Polski, co stanowiło podobną liczbę jak w poprzednim roku. Warto zaznaczyć, że nie wszystkie incydenty zgłaszane były do CERT Polska. Dane o atakach w infrastrukturze administracji publicznej posiada CERT.GOV.PL - z informacji przekazanych przez ABW wynika, że zespół CERT.GOV.PL w 2016 r., zarejestrował łącznie 19954 zgłoszenia, z których 9288 zostało zakwalifikowanych jako faktyczne incydenty. Znaczna różnica w liczbie zarejestrowanych zgłoszeń w stosunku do liczby incydentów wynika z faktu, iż zgłoszenia poddawane są weryfikacji, w której zostaje określone czy uzyskana informacja nosi znamiona faktycznego incydentu komputerowego, czy też wynika z błędu strony zgłaszającej lub jest tzw. *false positive* (oprogramowanie antywirusowe omyłkowo klasyfikuje „zdrowy" plik jako zainfekowany).

[7] w roku 2015 r. zidentyfikowano 1456 incydentów

Ponadto w ramach sieci instytucji administracji państwowej działa ARAKIS 2.0 GOV – system wczesnego ostrzegania o zagrożeniach teleinformatycznych występujących na styku sieci wewnętrznej podmiotu z siecią internetową. Jego głównym zadaniem jest wykrywanie i zautomatyzowane opisywanie zagrożeń występujących w sieciach teleinformatycznych na podstawie agregacji, analizy i korelacji danych z różnych źródeł. W roku 2016 w sieciach teleinformatycznych podmiotów uczestniczących w projekcie zanotowano łącznie 338 430 181 przepływów, co przełożyło się na 446 915 wygenerowanych alarmów (pojedynczy alarm może składać się z wielu przepływów). Wśród zanotowanych alarmów:

- 279181 miało priorytet pilny – wymagało natychmiastowej reakcji na zagrożenie ze strony administratorów sieci teleinformatycznej, której dotyczy i niosło za sobą duże ryzyko przełamania zabezpieczeń;
- 52766 miało priorytet wysoki – wymagało wzmożonej uwagi w kontekście zagrożenia wskazanego w alarmie, niosło za sobą średnie ryzyko przełamania zabezpieczeń;
- 12365 miało priorytet średni – były to alarmy informujące o znanym zagrożeniu, które niosło za sobą małe ryzyko przełamania zabezpieczeń;
- 102603 miało priorytet niski – były to alarmy czysto informacyjne np. próby skanowań publicznych przestrzeni adresowych.

Jeśli chodzi o straty, to możliwe są jedynie szacunki. Bez jednoznacznego określenia, co jest a co nie jest atakiem hackerskim, nie jest możliwe ustalenie wymiernych strat. Poza tym, nawet jeśli zdefiniujemy ściśle, które ataki nas interesują, zdobycie żądanych informacji jest trudne - wiele strat jest niepieniężnych (utrata zaufania do przedsiębiorstwa, wyciek danych osobowych, zmniejszenie poziomu bezpieczeństwa) lub po prostu trudnych do oszacowania (uniemożliwienie dostępu do określonej usługi bądź obniżenie poziomu jakości jej świadczenia).

Uświadamianie użytkowników – zarówno indywidualnych jak i korporacyjnych – jest podstawowym warunkiem osiągnięcia wysokiego poziomu bezpieczeństwa. Użytkownika, który nie zdaje sobie sprawy z zagrożenia, nie wesprze nawet najwyższej klasy sprzęt i oprogramowanie. NASK, od wielu lat, prowadzi akcje informacyjne skierowane do firm, instytucji i prywatnych użytkowników na temat bezpieczeństwa w cyberprzestrzeni i ochrony przed atakami hackerskimi. W szczególności należy tu wymienić organizowaną przez NASK Konferencję na temat bezpieczeństwa teleinformatycznego SECURE - w tym roku odbędzie się jej 21 edycja.

Również zespół CERT.GOV.PL prowadzi działalność profilaktyczną, w tym szkolenia pracowników administracji rządowej mające na celu wyeliminowanie najczęstszych błędów

oraz braków. Zespół wydaje także rekomendacje i przekazuje ostrzeżenia do instytucji. Informacje o istotnych zagrożeniach, podatnościach oraz aktualizacjach w systemach i aplikacjach najczęściej wykorzystywanych w administracji publicznej oraz dotyczące szeroko rozumianej problematyki bezpieczeństwa teleinformatycznego publikowane są na witrynie internetowej www.cert.gov.pl. Umieszczane są tam również biuletyny bezpieczeństwa udostępnione przez producentów sprzętu i oprogramowania zawierające m.in. ostatnio wykryte luki w bezpieczeństwie ich produktów oraz metody neutralizacji potencjalnych zagrożeń. Zespół CERT.GOV.PL publikuje również raport roczny o stanie bezpieczeństwa cyberprzestrzeni RP zawierający m.in. statystyki incydentów oraz zalecenia i rekomendacje.

Z wyrazami szacunku,

wz. Krzysztof Szubert
Sekretarz Stanu
/podpisano elektronicznie/

Do wiadomości:
Kancelaria Prezesa Rady Ministrów