Warszawa, dnia 25 maja 2018 r.

DL-III-0520-48/18

BM-I-0520 - 375/1812

180530 - 00389

Pani
Maria Koc
Wicemarszałek Senatu
Rzeczypospolitej Polskiej

Szanowna Pani Marszałek,

W odpowiedzi na oświadczenie złożone dnia 16 kwietnia 2018 r. przez senatora Andrzeja Kobiaka, podczas 59. posiedzenia Senatu RP, dotyczące działań zmierzających do zabezpieczenia internautów przed oszustwami oraz złośliwym oprogramowaniem, uprzejmie wyjaśniam, co następuje.

Tytułem wstępu należy wskazać, że w aktualnym porządku prawnokarnym czyny zabronione związane z tzw. cyberprzestępczością oraz tematyką zawartą w oświadczeniu Pana senatora, zostały stypizowane w ustawie z dnia 6 czerwca 1997 r. – Kodeks karny (Dz. U. z 2017 r. poz. 2204, z późn. zm., dalej: k.k.). Mowa tu przede wszystkim o przestępstwie oszustwa (art. 286 § 1 k.k.) oraz posługiwania się danymi innych osób (tj. kradzież tożsamości, 190a § 2 k.k.), ale także o wpływaniu na automatyczne przetwarzanie, gromadzenie lub przekazywanie danych informatycznych (art. 165 § 1 pkt 4 k.k.), nielegalnego uzyskania informacji (art. 267 k.k.), szkody w bazach danych (art. 268a § 1 k.k.), zakłócania pracy w sieci (art. 269a k.k.), bezprawnego wykorzystania programów i danych (art. 269b k.k.), sfałszowania faktury (270a k.k.), czy samym oszustwie komputerowym (art. 287 § 1 k.k.).

W polskim ustawodawstwie karnym brak jest definicji legalnej pojęcia „cyberprzestępczość". W jej ustaleniu może natomiast okazać się pomocna analiza treści preambuły zawartej w Konwencji Rady Europy o cyberprzestępczości z dnia 23 listopada

2001 r. (Dz. U. z 2015 poz. 728), której stroną jest również Polska. Na marginesie należy jedynie dodać, że w celu implementowania do prawa polskiego przepisów Konwencji o cyberprzestępczości znowelizowane zostały odnośne przepisy ustawy karnej, w tym w szczególności zawarte w rozdziale XXXIII k.k. zatytułowanym *Przestępstwa przeciwko ochronie informacji*. We wspomnianej preambule czytamy m.in., że celem Konwencji jest powstrzymanie działań skierowanych przeciwko poufności, integralności i dostępności systemów informatycznych, sieci i danych informatycznych, jak również nieprawidłowemu wykorzystywaniu tych systemów, sieci i danych, poprzez uznanie takiego postępowania za przestępstwo. Przez określenie cyberprzestępczość należy zatem najogólniej rozumieć czyny zabronione pod groźbą kary przez ustawę dokonywane przeciwko bezpieczeństwu systemów informatycznych, sieci, elektronicznie przetwarzanych danych, jak również przy użyciu tych systemów, sieci i danych.

Należy zauważyć, że katalog czynów zabronionych w aspekcie cyberprzestępczości nie ogranicza się do przestępstw kodeksowych, bowiem odpowiedzialność karna może wynikać również z ustaw szczególnych, np. jeżeli w związku z elektronicznym przetwarzaniem danych w obrocie bankowym dojdzie do naruszenia ustawowo chronionej tajemnicy np. tajemnicy bankowej, zastosowanie znajdzie art. 171 ust. 5 ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe (Dz. U. z 2017 r. poz. 1876, z poźn. zm.) przewidujący odpowiedzialność karną za nieuprawnione ujawnienie lub wykorzystanie informacji stanowiących tajemnicę bankową.

Obok wielu korzyści, jakie przyniosła nam rewolucja techniczna, pojawiło się jednak wiele nowych zagrożeń związanych z bezpieczeństwem informacji. Największym z nich jest dostęp do informacji, których nie chcemy ujawniać. Jest to tym większy problem, że dane zastrzeżone są obecnie przechowywane w wielu miejscach, a ich ochrona często jest niedostateczna. Ewentualna kradzież informacji odbywać się może bez naszej wiedzy. Co więcej, nie jesteśmy w stanie przewidzieć wszystkich jej następstw oraz czasu, w którym przechwycona informacja zostanie wykorzystana przeciwko nam. Wyciek informacji może okazać się bardzo niebezpieczny i kosztowny, dlatego też wiele uwagi poświęca się mechanizmom i procedurom zabezpieczania informacji zastrzeżonej. Z drugiej strony coraz więcej grup pragnie uzyskać dostęp do tego rodzaju danych, łamiąc tworzone zabezpieczenia i osiągając przy tym wymierne korzyści finansowe (zob. B. Hołyst, J. Pomykała, *Cyberprzestępczość, ochrona informacji i kryptologia*, Prokuratura i Prawo (2011), Nr 1).

Przestępcy zajmujący się kradzieżą informacji dysponują ogromnym arsenałem środków technicznych pozwalających na dokonywanie włamań. Ze względu na charakter tych narzędzi, można podzielić je na kilka kategorii:

1) *Wirus komputerowy* – to program, którego głównym wyróżnikiem w stosunku do innych narzędzi jest zdolność do samopowielania. Najczęściej wirusy komputerowe są pisane w językach niskiego poziomu (takich jak *assembler*). Dzięki temu wirus zajmuje stosunkowo mało miejsca, co utrudnia jego wykrycie. Poza tym języki niskiego poziomu nie nakładają na programistę wielu ograniczeń co do kodu programu. Powoduje to, że program może pracować niepostrzeżenie dla przeciętnego użytkownika. Wirus komputerowy, podobnie jak zwykły wirus, nie jest w stanie funkcjonować sam. Do jego działania jest potrzebny inny program. Wirus komputerowy infekuje program, stając się jego częścią. Programiści tworzący wirusy komputerowe wykorzystują wszelkie możliwe luki, aby w możliwie szybki i skuteczny sposób zainfekować komputer. Efekty działania wirusów są trudne do przewidzenia. Czasami wirus jest tworzony jedynie po to, by przynieść rozgłos jego twórcy. Jedynym niepożądanym efektem działania może być wtedy np. pojawienie się komunikatu o zainfekowaniu. Najczęściej jednak ukryty kod wirusa ma za zadanie przechwycenie istotnych informacji (np. haseł) i przesłanie ich do twórcy wirusa, wykorzystanie zainfekowanego komputera np. do wysyłania spamu bądź też zakłócenie działania systemu (spowolnienie działania, wyłączenie komputera, uszkodzenie części komputera itp.);

2) *Robak komputerowy* – to program, który rozprzestrzenia się samodzielnie, ale nie infekuje innych plików. Jego działanie polega na instalacji na komputerze ofiary oraz próbie rozprzestrzeniania się. W przypadku robaka wyróżnia się tylko pojedynczą kopię kodu robaka. Jego kod jest „samodzielny", a nie dodawany do istniejących plików na dysku. Robaki komputerowe rozprzestrzeniają się poprzez załączniki do wiadomości e-mail, wiadomości wysyłane z komunikatorów (takich jak np. IRC), sieci P2P lub też bezpośrednio do sieci LAN czy Internetu, wykorzystując lukę w zabezpieczeniach oprogramowania. Instalacja robaka internetowego często jest wytrychem, który umożliwia dalszą inwigilację naszego komputera. Zainstalowany robak może np. pobrać z Internetu kolejne szkodliwe oprogramowanie (np. konie trojańskie) i zainstalować je bez naszej wiedzy;

3) *Koń trojański* – to oprogramowanie, które podszywając się pod przydatne lub ciekawe dla użytkownika aplikacje, dodatkowo implementuje niepożądane, ukryte przed użytkownikiem funkcje. Najczęściej konie trojańskie zawierają programy szpiegujące (np. wysyłają do twórcy programu wszystkie znaki wpisywane poprzez klawiaturę, informują o otwieranych programach, stronach internetowych, umożliwiają kradzież danych itd.), lub bomby logiczne,

które aktywują się w pewnym momencie zależnym od daty bądź jakiegoś działania użytkownika. Zainfekowany program umożliwia często twórcy złośliwego oprogramowania na całkowite przejęcie kontroli nad komputerem przy pomocy „ukrytych drzwi" (*backdoor*);

4) *Botnet* – to grupa komputerów zainfekowanych złośliwym oprogramowaniem. Użytkownik zainfekowanego komputera (komputer taki określamy mianem zombie) nie jest świadomy, iż ktoś inny wykorzystuje zasoby zainfekowanego komputera i w istocie sprawuje nad nim pełną kontrolę. Główną siłą sieci *botnetu* jest jej wielkość. Osoba, która przejęła kontrolę nad wieloma tysiącami komputerów, może wykorzystać je np. do wysyłania spamu. Komputery zombie mogą być również wykorzystywane do otwierania stron reklamowych (z czego zyski czerpie osoba sterująca *botnetem*), wykorzystywanych następnie w kolejnych działaniach nielegalnych (np. typu *„phishing"*). *Botnety* są wykorzystywane również jako narzędzie do zdobywania informacji oraz blokowania dostępu uczciwym użytkownikom do stron *www*;

5) *Atak typu odmowa usług (DoS, DdoS)* – ma za zadanie uniemożliwienie funkcjonowania zaatakowanego serwera, sieci lokalnej lub strony WWW. Zazwyczaj polega on na zarzuceniu atakowanego serwera ogromną liczbą nieustających zleceń lub żądań, czego konsekwencją jest spowolnienie lub uniemożliwienie reagowania systemu na żądania uczciwych klientów (więcej na ten temat: zob. B. Hołyst, J. Pomykała, *Cyberprzestępczość, ochrona informacji i kryptologia*, Prokuratura i Prawo (2011), Nr 1).

Warto w tym miejscu zwrócić uwagę na trudności dowodowe związane z procesem pozyskiwania i zabezpieczania dowodów elektronicznych w celu zapewnienia możliwości wykorzystania ich jako pełnowartościowych dowodów w postępowaniu przed sądem, wymagające uwzględnienia specyficznych właściwości tych dowodów, które wymuszają stosowanie odmiennych niż w przypadku tradycyjnych przestępstw zasad gromadzenia materiału dowodowego, opartych na fachowości i specjalistycznej wiedzy osób uczestniczących w czynnościach procesowych, w toku których dochodzi do zabezpieczenia śladów dowodowych w postaci elektronicznej.

z upoważnienia
MINISTRA SPRAWIEDLIWOŚCI
Marcin Warchoł
PODSEKRETARZ STANU