POLSKA POLICJA ŁAPIE PRZESTĘPCÓW ZA TOREM [WYWIAD]

O polskich cyberprzestępcach, reformie Policji w obszarze cyberbezpieczeństwa oraz wyzwaniach na przyszłość mówi w wywiadzie dla cyberdefence24.pl Łukasz Jędrzejczak, Naczelnik Wydziału Rozpoznania Biura Do Walki z Cyberprzestępczością Komendy Głównej Policji.

Doktor Andrzej Kozłowski: Jak wygląda krajobraz polskiej cyberprzestępczości?

Łukasz Jędrzejczak: Krajobraz cyberprzestępczości jest na całym świecie taki sam, dlatego, że Internet nie ma granic, tym samym nie mają ich również cyberprzestępstwa. Polscy cyberprzestępcy są na tym samym poziomie rozwoju technologicznego, co ich koledzy na całym świecie. Środowisko cyberprzestępców ma dostęp do informacji i możliwości technologicznych, dlatego wszyscy cyberprzestępcy prezentują podobny poziom rozwoju. Polskie prawo organom ścigania daje jednak dużo możliwości. Ponadto cały czas trwa współpraca na poziomie europejskim ukierunkowana na zwiększaniu możliwości organów śledczych do walki z cyberprzestępczością. Ostatnio opracowywane są w Brukseli na spotkaniu komisji Rady Europy dotyczącym E-Evidence, możliwości wymiany elektronicznych dowodów pomiędzy organami ścigania w Europie.

Czy mógłby Pan powiedzieć czy cyberprzestępczość w Polsce ma charakter głównie indywidualny czy grupowy? Mógłby Pan zidentyfikować największych polskich cyberprzestępców?

Od jakiegoś czasu obserwujemy stałą tendencję światową, gdzie cyberprzestępcy przestali być pojedynczymi hakerami działającymi tylko dla sławy. Obecnie w zdecydowanej większości działają dla konkretnych korzyści.

Czyli grupy hakerskie są międzynarodowe? Nie ma grup cyberprzestępców złożonych tylko z Polaków?

Tak to wygląda, dlatego, że internet nie ma granic, tak samo jak cyberprzestępcy. Logują się na swoich zamkniętych forach i tam nie ma znaczenia kraj pochodzenia, ale to kto Cię polecił oraz jakich czynów dokonałeś i czy możesz to udowodnić. Ludzie dogadują się na poziomie międzynarodowym i wymieniają się informacjami, wiedzą, oprogramowaniem i wspólnie popełniają przestępstwa. Sytuacja taka, że działa w sieci pojedynczy haker, który jest psychopatą jest coraz rzadziej spotykana.

Od kiedy Państwo w policji zajmują się zwalczaniem cyberprzestępczości?

Biuro Do Walki z Cyberprzestępczością Komendy Głównej Policji powstało 1 grudnia 2016 roku. Natomiast zwalczaniem cyberprzestępczości zajmujemy się na poważnie od początku XXI wieku.

Czyli wcześniej ten problem nie istniał czy nie został zauważony?

Wcześniej nie było to określane jako cyberprzestępczość, tylko jako przestępstwo komputerowe. Na przykład kopiowanie płyt i sprzedawanie ich na rynku to nie jest cyberprzestępczość. W Polsce Internet stał się powszechny w latach 1996-1998. W Policji na początku funkcjonowały zespoły pracujące w komendach wojewódzkich, w wydziałach do walki z przestępczością gospodarczą. Były to zespoły do tzw. przestępczości intelektualnej i komputerowej. Już od kilku lat w każdej komendzie wojewódzkiej Policji działają wydziały do walki z cyberprzestępczością. Są to zespoły liczące ok. 20 osób. Komendant Główny Policji uznał, że potrzebny jest profesjonalny, solidny nadzór nad pracą tych wydziałów zapewniający wsparcie zarówno merytoryczne, jak i techniczne. Tak powstało Biuro do Walki z Cyberprzestępczością Komendy Głównej Policji, które obecnie jest na końcowym etapie zbierania kadr.

Ile biuro ma liczyć osób?

Biuro ma liczyć około 60 etatów.

Jakie główne cele będą tego biura?

Do głównych zadań biura należy koordynacja działań wszystkich jednostek Policji w kraju, zajmujących się zwalczaniem cyberprzestępczości. Biuro składa się z 4 wydziałów: Wydział Ogólny, który zajmuje się sprawami logistyczno-administracyjnymi, Wydział Operacyjny - jednostka odpowiedzialna za poważne sprawy operacyjne w Internecie, Wydział Badań i Analiz, zajmujący się informatyką śledczą oraz Wydział Rozpoznania. Policjanci Wydziału Badań i Analiz jeżdżą na miejsca zdarzeń, zabezpieczają sprzęt, odzyskują dane z komputerów oraz innych nośników. To policjanci, którzy są już konkretnie na realizacji, zajmują się zabezpieczaniem i analizą nośników cyfrowych. Wydział Rozpoznania, którego mam przyjemność być naczelnikiem jest najliczniejszy w Biurze. Posiada sekcję obsługi całodobowej, czyli całodobowy monitoring Internetu pod kątem cyberzagrożeń, oraz zespół rozpoznania.

Czy ta instytucja działa jak CERT?

Nie jest to CERT, ponieważ nie chodzi tylko o zagrożenia. To jest zespół do spraw monitoringu internetu. Wyselekcjonowani funkcjonariusze posiadający upoważnienie Komendanta Głównego Policji do natychmiastowego żądania uzyskiwania informacji od ISP i ICP monitorują sieć. Zakres działania tego zespołu jest bardzo szeroki. Są to działania od stricte cyberzagrożeń, po zwykłe ludzkie, kiedy ktoś napisze na jakimś forum lub portalu społecznościowym, że chce popełnić samobójstwo. Policjanci w oparciu o posiadane upoważnienie uzyskują informacje, kto udostępnił taki post. Całkiem niedawno na podstawie przekazanych informacji w ciągu półtorej godziny od ujawnienia takich informacji w Internecie, zespół psychologów policyjnych pojechał do dziecka, które jednak stwierdziło, że nie miało zamiaru popełniać samobójstwa, tylko był to głupi żart. My jednak musimy reagować, zarówno w przypadkach cyberprzestępstw, jak i ratowania ludzkiego życia, w tym znaczeniu, że jeżeli jakiekolwiek informacje, incydenty i sytuacje zagrożeń pojawią się w Internecie.

Wracając do historii, powiedział Pan, że walka z cyberprzestępczością rozpoczęła się na początku XXI wieku. Czy był jakiś konkretny incydent, który spowodował że ten problem nagle pojawił się na agendzie?

Myślę, że nie było takie incydentu. Było to po prostu następstwo rozwoju technologicznego i przenoszenie się wszystkich form przestępczości do Internetu. Nie można było pozostać obojętnym wobec tego zjawiska i Policja to dostrzegła.

Wcześniej nie było takiej instytucji?

Kiedyś można było użyć wyrażenia: „jestem informatykiem”. Teraz to nic nie znaczy. Nie ma już kogoś takiego jak człowiek-informatyk. Jest programista, grafik komputerowy, webmaster, administrator sieci, administrator stron internetowych itp. W Policji dostrzegamy potrzebę specjalizacji w walce z cyberprzestępczością. Mamy osoby odpowiedzialne za monitoring Internetu czyli zajmujące się szukaniem zorganizowanych grup hakerskich czy wyszukiwaniem określonych ludzi, którzy stwarzają zagrożenie.

Czy monitorowanie obejmuje DarkNet i polską społeczność w sieci TOR? Czy mamy odpowiednik polskiego Dark Marketu czy innych forów karderskich, które były w przeszłości?

Tak, ale nie mogę powiedzieć, które fora monitorujemy. Wielokrotnie w sądzie pytano mnie, jak uzyskałem dane informacje. Wówczas prosiłem o utajnienie spotkania i w tej sytuacji mogłem wyjaśnić, jak złapałem przestępcę oraz jakich narzędzi użyłem.

Członkowie tych społeczności wiedzą, że Państwo czytacie ich fora?

Często się domyślają, nie zawsze jednak wiedzą. Wiadomo, że jest to czynnik ludzki. Na niektórych forach są jednak bardzo pewni siebie i dość często pojawiają się tam wpisy, że to forum jest najlepsze, bo żaden policjant tego nie czyta.

Internet i cyberprzestępczość nie mają granic. W takim razie jak wygląda współpraca z innymi państwami i niekoniecznie mam tu na myśli Unię Europejską i Europol, ale np. naszych wschodnich sąsiadów, czyli Białoruś, Ukrainę, Rosję czyli państwa uznawane za kolebkę cyberprzestępczości ?

To, że te państwa są uznawane za kolebkę cyberprzestępczości wynika m.in. ze słabości obowiązującego tam prawa. Retencja danych ma ogromne znaczenie dla organów ścigania. Jest to obowiązek przechowywania danych przez dostarczycieli usług internetowych na potrzeby prowadzonych postępowań bądź czynności przed procesowych. W tej chwili mamy w Polsce dość długi obowiązek retencji danych na koszt operatora i dostarczenia do organów ścigania każde żądanie policjantów posiadających określone upoważnienia komendanta. To nie tak, że mogą je uzyskać wszyscy. Są one dostępne tylko dla specjalnie wybranych policjantów pracujących w naszych komórkach, działających w upoważnieniu Komendanta Głównego Policji albo Komendanta Wojewódzkiego Policji.

Czy zmiany te wprowadziła ustawa antyterrorystyczna?

Nie. Zmiany zostały wprowadzone przez Ustawę o Policji i inne akty prawne. Mamy jedno z najlepszych rozwiązań prawnych do zwalczania cyberprzestępczości w Europie.

W Rosji też nie ma retencji danych?

W Rosji sytuacja wygląda inaczej, ale oni są niechętni przekazywaniu danych. Białoruś nie ma retencji danych. Problem dotyczy również niektórych państw Unii Europejskiej. W Czechach np. jest krótszy obowiązek retencji danych.

Wyobraźmy sobie sytuację, że policjant składa wniosek o dostęp do danych. Jaki organ decyduje czy ten wniosek zostanie zaakceptowany w Policji i jest uzasadniony ze względu na prowadzoną sprawę, żeby uniknąć sugestii, że chcemy szpiegować obywatela albo go inwigilować?

Mamy kontrolę następczą sądu. Nie ma zaś kontroli poprzedzającej.

Czyli dopiero po fakcie uzyskania? A jeżeli sąd by stwierdził, że uzyskanie dane nie były uzasadnione?

Taka sytuacja nie miała miejsca. Liczba wniosków nie jest duża.

Czy jest Pan w stanie powiedzieć ile?

Kilka tysięcy rocznie, co przy liczbie osób oszukanych na platformach handlowych nie jest dużą liczbą. Każdy taki wniosek przesyłany jest do dostarczyciela usług internetowych, a potem podlega kontroli UKE (Urząd Komunikacji Elektronicznej) i ewentualnej kontroli następczej sądu. Wnioski takie mogą być składane tylko przez wybraną grupę funkcjonariuszy Policji. Za każdym razem, kiedy policjant taki wniosek składa, działa on wówczas w imieniu Komendanta Głównego Policji albo Komendanta Wojewódzkiego Policji.

Mam pytanie odnośnie systemu walki z cyberprzestępcami? Czy czerpią Państwo wzorce z innych krajów i jeżeli tak to z jakich?

Tak, wymieniamy się doświadczeniami. Jest grupa powołana w Europolu, gdzie znajduje się centrum do zwalczania cyberprzestępczości. Nazywa się to EC3. Tam odbywają się szkolenia, w których uczestniczymy.. W Stanach Zjednoczonych funkcjonuje NCFTA *(The National Cyber-Forensics & Training Alliance)*. Jest to stowarzyszenie powołane przez FBI i NSA i kilka innych najpoważniejszych organizacji, gdzie są prowadzone staże w zakresie zwalczania cyberprzestępczości. Miałem przyjemność ukończyć taki staż podobnie jak kilku moich współpracowników. Wysyłamy naszych ludzi również do Interpolu. W Singapurze znajdują się biura zwalczania cyberprzestępczości tej organizacji. Powyższe przykłady pokazują współpracę służb policji w zakresie zwalczania cyberprzestępczości. Dodatkowo, podobnie jak nasi przeciwnicy, mamy własne, specjalistyczne fora np. dla ekspertów od informatyki śledczej. Nasi przeciwnicy na nasze fora nie wejdą dlatego, że one nie są w Internecie. One są w naszych sieciach lokalnych, które nie są podłączone do sieci globalnej i my też się od siebie uczymy. Uważam, że organy ścigania są dobrze przygotowane, żeby zwalczać cyberprzestępczość. Problem leży jednak w prawie, które nie nadąża za zmianami.

No tak, ale przed chwilą Pan powiedział, że polskie prawo jest w zakresie walki z cyberprzestępczością jednym z lepszych?

Tak prawo w Polsce w tym zakresie jest dobre, najlepsze jakie może być.

W czym się to wyraża?

Przykładowo w retencji danych.

Tylko w retencji danych?

Moim zdaniem to jest najważniejszy element. Retencja danych sprawia, że Policja dysponuje narzędziem do walki z cyberprzestępcami.

Czy polska Policja jest w stanie zidentyfikować użytkowników sieci TOR?

Tak. udało nam się zatrzymać wielu sprawców działających za TORem.

Czyli polska Policja jest też w stanie to zrobić?

Polska policja zatrzymuje użytkowników za TORem.

Ile rocznie osób skazuję się za działania cyberprzestępcze?

Nie są prowadzone takie statystki, dlatego, że nie ma czegoś takiego jak cyberprzestępstwo. Nie ma katalogu przestępstw w kodeksie karnym.

Czyli prawo nie definiuje czym jest cyberprzestępstwo?

Mamy trzy artykuły wymienione w polskim prawie, które mówią o klasycznym przełamaniu hackingu i tworzeniu narzędzi do hackingu itd. Jednak czy oszustwo na portalu aukcyjnym jest cyberprzestępstwem, czy nie? Trudno odpowiedzieć na to pytanie, ponieważ kwalifikacje prawne przyjmowane przez sądy i prokuratury są różne. Na podstawie materiałów funkcjonariuszy zajmujących się kwestiami cyberprzestępczości wszczęto około 800 postępowań w 2015 roku i 1100 postępowań w 2016 roku. Znam statystyki tego, co robią ludzie podlegający pod Biuro.

A jak ocenianie jest pirackie oprogramowanie?

Jest to również kwalifikowane jako cyberprzestępczość, dlatego, że w tym miejscu musi dojść do przełamania zabezpieczeń i wytworzenia nielegalnej kopii, utworu czyli w jakiś sposób muszą być złamane zabezpieczenia producenckie po to, żeby móc zrobić tą kopię.

Czy można o to oskarżyć zwykłego użytkownika, który takie oprogramowanie ściągnie i zastosuje cracka?

Crack jako narzędzie służące do obchodzenia zabezpieczeń jest uznawany za narzędzie cyberprzestępcze. Mówi o tym art. 269 b kodeksu karnego Każda sprawa jest jednak inna i kwalifikacja danego czynu zależy od pozostałych okoliczności sprawy.

Chciałbym zapytać o sposób rekrutowania ludzi od Państwa zespołu, czy są jakieś specjalne kryteria?

Wszyscy funkcjonariusze, którzy pracują w biurze to funkcjonariusze Policji, którzy przechodzą takie samo szkolenie jak każdy policjant.

Dopiero potem jest specjalizacja?

Tak. Prowadzimy wewnętrzną rekrutację z funkcjonariuszy Policji, bądź pracowników cywilnych, którzy są już w instytucji. Osoby, które nie są informatykami też mogą z nami współpracować lub u nas pracować. Rekrutacja przebiega w standardowym sposób. Odbywamy normalne rozmowy, mamy własne szkolenia. Poza tym szkolimy się za granicą i na terenie kraju.

Jakie według Pana są największe wyzwania w kwestii zwalczania cyberprzestępczości dla policji w Polsce?

Największe wyzwania w kwestii zwalczania cyberprzestępczości są w zasadzie takie same dla policji na całym świecie. TOR i anonimizacja użytkownika Internetu, to jest wyzwanie.

A co z łatwiejszym dostępem narzędzi hakerskich?

Moim zdaniem nie jest to wielkie zagrożenie, dlatego, że z kolei te gotowe wzorce wykorzystywane przez amatorów wielokrotnie sprawiły, że udało nam się zatrzymać sprawców cyberprzestępstw.

Kom. Łukasz Jędrzejczak

Naczelnik Wydziału Rozpoznania Biura do Walki z Cyberprzestępczością Komendy Głównej Policji.