"DRONY CHRONIĄ NAS PRZED CYBERTERRORYSTAMI" [WYWIAD]

O zmieniającym się krajobrazie zagrożeń w cyberprzestrzeni, cyberterroryzmie i systemie bezpieczeństwa Finlandii w cyberprzestrzeni mówi w wywiadzie dla Cyberdefence24 szef laboratorium F-Secure Mikko Hypponen.

Andrzej Kozłowski: Mamy do czynienia z dynamicznie zmieniającym się krajobrazem zagrożeń. Czy jesteśmy bezpieczniejsi niż 20 lat temu?

Mikko Hypponen: Bezpieczeństwo naszych systemów operacyjnych i aplikacji zdecydowanie wzrosło. Dziesięć lat temu najbardziej powszechnym systemem operacyjnym był Windows XP, który nie miał nawet wbudowanego firewalla. Jeżeli porównamy to do obecnych technologii zastosowanych w systemie operacyjnym Windows 10, to widzimy ogromny postęp. Problem polega jednak na tym, że zmienił się również przeciwnik. Jeżeli dzisiaj mierzylibyśmy się z zagrożeniami, które istniały 10 lat temu, bylibyśmy względnie bezpieczni, a penetracja naszych systemów mocno utrudniona. Niestety nasz przeciwnik używa coraz częściej zaawansowanych metod i narzędzi ataku, powodując, że przybiera to wszystko schemat odwiecznej gry w kotka i myszkę. Za każdym razem, kiedy usprawnimy systemy bezpieczeństwa, nasz przeciwnik stosuje nowe metody ich atakowania. Sytuacja wygląda podobnie jak w historii wojskowości z mieczem i tarczą.

A. K.: Co w takim razie musimy zrobić, żeby nasza obrona była potężniejsza od zdolności ofensywnych przeciwnika?

M.H.: Możemy problem podzielić na dwie różne kategorie. Pierwszą z nich są błędy w oprogramowaniu używanych przez nas aplikacji i systemów operacyjnych. Drugą stanowią błędy ludzkie, które bardzo ciężko naprawić, ponieważ trudno jest zwalczyć głupotę. Skupmy się jednak na błędach w oprogramowaniu. Wydaje się, że ich całkowite wyeliminowanie jest niemożliwe. Uważam jednak, że można to zrobić. Nie jest to oczywiście kwestia najbliższej przyszłości, tylko proces długoterminowy. Powodem, dla którego programy zawierające luki umożliwiają przypuszczenie ataku, jest błąd programisty. Przed nastaniem ery internetu, złośliwe programy mogły uszkodzić komputer. Obecnie, kiedy wszyscy są podłączeni do internetu, można w ten sposób uzyskać zdalny dostęp do systemu. Możemy jednak wyeliminować błędy w oprogramowaniu. Moim zdaniem w przeciągu 20, 30 lat większość programów będzie pisana przez komputery. Dawno temu napisałem program komputerowy, który następnie pisał programy komputerowe i je kompilował. Jest to możliwe, sam to zrobiłem.

A.K: Brzmi interesująco, ale jaka jest pewność, że pierwszy program będzie bezpieczny i bez błędów?

M.H.: To akurat nie ma znaczenia, ponieważ to sztuczna inteligencja będzie odpowiadała za pisanie programów. Będą one bardzo złożone i skomplikowane, przez co ludzie nie będą w stanie ich

zrozumieć i nawet jeżeli będą posiadały błędy i podatności, człowiek nie będzie miał wiedzy i umiejętności, żeby je wykorzystać.

A.K: Podkreślałeś wielokrotnie zagrożenie związane ze sztuczną inteligencją, gdzie w takim razie leży granica, przed którą powinniśmy się zatrzymać?

M.H.: To będzie bardzo, bardzo groźne. Tak naprawdę to nie wiem. Prawdopodobnie będzie to jedna z najpoważniejszych decyzji dla ludzkości. Jak przeprowadzić proces wdrażania sztucznej inteligencji bezpiecznie. Wiem tylko, że to się stanie, tak samo jak wprowadzenie samoprogramujących się programów, i rozwiąże problem luk w oprogramowaniu. Wciąż jednak będzie istniał problem użytkowników.

A.K: Prawdopodobnie jest to o wiele większy problem. Co w takim razie możemy zrobić, żeby nawet nie wyeliminować, ale chociaż zmniejszyć zagrożenie?

M.H.: Myślę, że nowa generacja użytkowników internetu może przynieść tu pożądaną zmianę. Jesteśmy niestety dinozaurami. Mamy problemy z nauczeniem się nowych rzecz związanych z internetem, ponieważ nie jest on naszym naturalnym środowiskiem. Spójrzmy na młodsze pokolenie - 20 latków, internet zawsze dla nich istniał i oni są "cyfrowymi tubylcami". Moim zdaniem będą lepiej przygotowani do bezpiecznego poruszania się w świecie wirtualnym. Jesteśmy dinozaurami, zestarzejemy się i umrzemy, miejmy nadzieję, że następna generacja będzie lepiej przygotowana do radzenia sobie z tymi wyzwaniami.

A.K: Jakie Twoim zdaniem będą konsekwencje rosnącej liczby cyberataków, które oddziałują na środowisko materialne jak Stuxnet, cyberataki na Ukrainę i Niemcy?

M.H.: Ich liczba stale wzrasta, a dzieje się tak dlatego, że coraz więcej rzeczy jest kontrolowanych przez komputery podłączone do internetu, co zwiększa liczbę możliwości i ścieżek przeprowadzenia ataków o efekcie kinetycznym. W przyszłości będzie ich zdecydowanie więcej i będą stanowiły o wiele większe zagrożenie. Obecnie większość fabryk jest kontrolowanych przez systemy komputerowe podłączone do internetu. Może to prowadzić do scenariusza jaki widzieliśmy w Niemczech, kiedy jeden z młynów został uszkodzony. W tym przypadku nie znamy motywu, dlaczego zaatakowano akurat ten obiekt. Należy podkreślić, że możliwość ataku istnieje i najgroźniejszym scenariuszem nie jest wojna czy ataki przeprowadzane przez państwa, tylko ekstremiści jak np. grupy terrorystyczne. Chcą oni przeprowadzić pewien rodzaj ataków, którym nie jest zainteresowana żadna inna strona, czyli taki, który po prostu powoduje zniszczenie np. komponentów w losowych fabrykach w różnych częściach świata. Nie ma nikogo innego, kto chciałby przeprowadzić podobne operacje.

A.K.: To kwestia cyberterroryzmu, szeroko dyskutowanego w dyskursie publicznym. Wspomniałeś, że posiadają zdolności oraz są zainteresowani takim rodzajem działalności. Wciąż jednak nie mieliśmy do czynienia z żadnym aktem cyberterroryzmu, dlaczego?

M.H.: Terroryści, a dokładnie Państwo Islamskie, nie są w stanie w 100 proc. wykorzystać swojego potencjału ze względu na ataki dronów. Siły wojskowe Stanów Zjednoczonych zabijają hakerów Daesh. Znane są dwa takie przypadki. W ten sposób Amerykanie chcą rozwiązać problem, zanim stanie się on poważniejszy. Jak widać jest to bardzo efektywne i skuteczne. W ostatnim czasie Daesh odniosło wiele sukcesów w rekrutacji hakerów z państw Zachodnich, którzy dołączali do tej organizacji w Syrii. Obecnie przeprowadzanie takich działań jest o wiele trudniejsze, od kiedy Stany Zjednoczone wyeliminowały dwóch przywódców, którzy byli odpowiedzialni za operacje Daesh w cyberprzestrzeni. Udowodnili oni, że mają zdolności i chęci do przeprowadzania cyberataków. Obecnie jest o wiele trudniej zrekrutować hakerów.

A.K.: Biorąc jednak pod uwagę, że zwolennicy i agenci Daesh występują też w państwach Europy Zachodniej, czy uważasz, że to możliwe, że sympatyzujący z tą organizacją hakerzy, mogą przeprowadzić ataki z terytoriów państw europejskich czy Stanów Zjednoczonych?

M.H.: Oczywiście jest to możliwe. Mam nadzieję jednak, że to się nie stanie. Wprawdzie nie byliśmy jeszcze świadkami cyberterroryzmu, jednak problem ten będzie rósł w przyszłości.

A.K. Co w takim razie możemy zrobić?

M.H.: Odnosząc się do problemu ekstremizmu, podoba mi się obecne postępowanie Google. Google używa swojej wyszukiwarki profilów w celu znalezienie ludzi, którzy są na skraju radykalizmu, tak samo jak używają tej technologii, żeby znaleźć osoby zainteresowanie np. wędkarstwem czy samochodami marki Ferrari. W ten sposób można zidentyfikować osoby wyszukujące materiały o Daesh, co może symbolizować ich radykalizację. Dla tych ludzi Google pokazuje reklamy video, które mają na celu zatrzymać proces radykalizacji, który znajduje się dopiero na początkowym etapie. Metoda ta w praktyce okazała się być bardzo skuteczna. Można sobie wyobrazić młodą osobę, która jest bardzo zainteresowana radykalnym islamem, ale wciąż żyje w zachodnim społeczeństwie. Jeżeli możemy do niej dotrzeć na początku jej drogi i zasiać wątpliwości o tym, czy ma to sens, jesteśmy w stanie wpłynąć na jej zachowanie. Google właśnie to robi.

A.K. To bardzo ciekawa technika, ale jak walczyć z aktywnością terrorystów na Facebooku i na Twitterze? Czy można zastosować tę samą technikę, którą stosuje Google?

M.H.: Oni ją stosują i próbują dezaktywować wiele kont powiązanych z działalnością islamistów. Podobnie postępuje Telegram, który próbuje wyłączyć prywatne kanały komunikacyjne ekstremistycznych grup islamskich. Jedną rzeczą trudną do zauważenia przez zewnętrznych obserwatorów jest to, że część kont jest celowo utrzymywana. Służby wiedzą, że należą one do terrorystów i w ten sposób mogą monitorować poruszane tematy. Dla zewnętrznych obserwatorów może to okazać się dziwne, dlaczego Twitter nie zamyka tych kont. Taka polityka może jednak w rzeczywistości pomagać operacjom wymierzonym w terrorystów.

A.K.: Finlandia uważana jest za państwo z najwyższym poziomem bezpieczeństwa. Dlaczego?

M.H.: Moim zdaniem jest wiele powodów tej sytuacji. Ale jednym z głównych elementów jest nasz system edukacyjny, który został zbudowany w bardzo dobry sposób, zaczynając już od edukacji na najniższym poziomie. Przynosi on bardzo dobre rezultaty i to pozytywnie skutkuje w wielu obszarach, nie tylko w systemie IT czy bezpieczeństwie IT. Nasze uniwersytety prowadzą kursy poświęcone szyfrowaniu i kryptografii od lat 50. W innych państwach były one niedostępne ze względu na restrykcyjne prawo. W Finlandii nigdy taka sytuacja nie występowała i to jest prawdopodobnie jeden z elementów naszego sukcesu. Bardzo ważna jest również kultura nordycka, która wspiera umysły ścisłe. Mamy wiele nerdów i geeków. Mamy długą zimę, więc nie przebywamy na zewnątrz, tylko piszemy linijki kodu na komputerze. Finlandia ma bardzo bogate doświadczenie w ramach cyberbezpieczeństwa i specjalistów z zakresu IT. Ponadto tym, co nas wyróżnia jest reputacja ludzi i narodu, któremu można zaufać oraz brak korupcji. Finlandia jest państwem z najmniejszym wskaźnikiem korupcji na świecie.

A.K.: Obecnie mamy do czynienia z napiętą sytuacją polityczną między państwami zachodnimi i Rosją. Czy w Finlandii widać szczególne przejawy wrogiej rosyjskiej aktywności?

M.H.: Jesteśmy świadkami raczej aktywności na niewielką skalę - jak kształtowanie opinii czy armie trolli i tym podobne. Jeżeli jednak mówimy o innych działaniach niż informacje operacyjne, cyberoperacje, Rosja nie jest specjalnie aktywna przeciwko Finlandii.

A.K.: Jaki jest w takim razie główny cel rosyjskiej wojny informacyjnej przeciwko Finlandii?

M.H.: Głównym celem jest szerzenie dezinformacji i chaosu informacyjnego wśród ludzi. Spowodowanie, żeby ludzie nie byli pewni, nie ufali źródłom informacji i wątpili w rzeczywistość. Wówczas Rosja będzie mogła zrealizować swoje długoterminowe plany. To jest coś, w czym była dobra przez wieki - kształtowanie opinii, i co robi również obecnie.

A.K: Ostatnio NATO na szczycie w Warszawie uznała cyberprzestrzeń za kolejny obszar prowadzenia działań wojennych. Czy w świecie wirtualnym jest miejsce dla tradycyjnego sojuszu wojskowo-politycznego jakim jest NATO i jaką rolę może taka organizacja odgrywać?

M.K.: Jest to dobre pytanie. W internecie nie ma granic, nie ma geografii, nie ma dystansów do pokonania, nie ma map i nie można zastosować tradycyjnych sojuszów. Wiem, że część z krajów NATO wprost stwierdziła, że będą traktowali ataki w cyberprzestrzeni jako operacje, które można skończyć odwołaniem do artykułu V i prośbą skierowaną do innych członków o wsparcie i kontratak nawet w świecie realnym. To jest przerażająca sytuacja, ponieważ bardzo łatwo jest popełnić błąd przy przypisywaniu ataku. Atak pochodzący z kraju A może tak naprawdę pochodzić z kraju B i jeżeli odpowiesz wystrzeleniem pocisku w świecie rzeczywistym na kraj A, będzie to poważny problem. To jest dokładnie powód, dla którego cyberataki są tak popularne. Są one skuteczne, tanie oraz łatwo im zaprzeczyć, ponieważ bardzo trudno wskazać podmiot odpowiedzialny za atak. Wydaje się, że jest to główny powód świadczący o ich popularności.

A.K.: Chciałbym zapytać o kwestię atrybucji, ponieważ mamy raport firmy Mediant 2013 dokładnie identyfikujący konkretnych hakerów w ramach chińskich jednostek. W strategii Pentagonu z 2015 roku stwierdzono, że Stany Zjednoczone są w stanie zlokalizować cyberatak, co potwierdził na Twitterze Edward Snowden. Czy Twoim zdaniem nowa technologia zwiększy nasze szanse na wskazanie, kto stoi za atakiem?

M.K: Oczywiście cały czas widzimy tutaj postęp, ale zawsze będzie to bardzo trudne. Większość spraw, w których stwierdzono, kto stoi za atakiem w 100 proc. to przypadki, gdy hakerzy rządu A włamali się do sieci rządu B. Obserwują przygotowania do ataku oraz jak on przebiega. Miało to miejsce w przypadku ataków na Sony. NSA złamało zabezpieczenia północnokoreańskich systemów i obserwowało hakerów Kim Dzona Ila dokonujących ataku. W ten sposób udało się ustalić sprawcę. Jest to dość dziwny sposób, ponieważ wymaga użycia narzędzi ofensywnych. Znajdujemy się właśnie na początku nowego wyścigu zbrojeń, który będzie miał miejsce w świecie wirtualnym.

A.K.: Czytamy coraz większą liczbę pesymistycznych prognoz dotyczących przyszłości internetu. Czy uważasz za możliwe, że odłączymy od internetu niektóre technologie?

M.K.: Nie wszystko musi być podłączone do internetu. Jest wiele technologii, które działają lepiej niepodłączone do sieci. Przykładowo systemy odpowiedzialne za ochronę infrastruktury krytycznej: generatory mocy, elektrownie jądrowe, urządzenia odpowiedzialne za dystrybuowanie wody. Oczywiście czerpią one korzyści z bycia online, ale nie powinny być podłączone do sieci. Rozpatrując bezpieczeństwo w długoterminowych ramach, uważam, że nie wszystkie urządzenia powinny być online.

Czytaj też: Failure is option – Wystąpienie Mikko Hypponena na konferencji SCS