aut. Bartosz Józefiak 19.05.2016

SKĄD WEŹMIEMY EKSPERTÓW OD CYBERBEZPIECZEŃSTWA?

- Zespoły do walki z cyberprzestępczością to nie mogą być tylko informatycy, ale też prawnicy, lingwiści i inni specjaliści. Każda grupa hakerów ma swoją specyfikę, a ustalenie, skąd pochodzą, jest priorytetem. Tutaj standardowy nabór nie pomoże. Trzeba szukać specjalistów, pasjonatów – przekonywali specjaliści podczas konferencji „Bezpieczeństwo i wolność słowa w cyberprzestrzeni”

Eksperci zebrani dziś w warszawskim domu dziennikarza próbowali odpowiedzieć na pytanie: Na ile Polska jest dziś w stanie poradzić sobie z najnowszymi zagrożeniami w cyberprzestrzeni? Skąd weźmiemy fachowców, którzy będą nas chronić?

– Poziom złożoności ataków jest coraz większy. Ciężko powiedzieć, w którą stronę pójdzie to dalej. Mamy coraz częściej do czynienia z atakami hybrydowymi, gdzie przestępcy podejmują wiele działań na raz w celu dostania się do ofiar – mówił Piotr Trąbiński, ekspert Narodowego Centrum Studiów Strategicznych (NCSS) w dziedzinie cyberbezpieczeństwa.

Według niego musimy konieczna jest zupełnie nowe podejście do cyberbezpieczeństwa. – W USA powstają zespoły szybkiego reagowania na incydenty. W ich skład wchodzą nie tylko informatycy, ale też lingwiści, prawnicy, specjaliści z różnych dziedzin. Chodzi o szybkie rozpoznanie problemu, sposobu działania hakerów - to klucz do sukcesów. Potrzebne jest szersze spojrzenie na to, skąd pochodzą hakerzy, skąd się wywodzą, jak działają. Przestępcy z różnych krajów działają w różny sposób, a rozpoznanie, skąd przychodzi atak to podstawa. Sam zespół techniczny tu nie wystarcza.

Skąd weźmiemy fachowców?

Problem w tym, że w Polsce brakuje fachowców od cyberbezpieczeństwa. Problem się pogłębia, bo rynek już dzisiaj mógłby przyjąć kilkanaście tysięcy pracowników od zaraz – a są to ostrożne rachunki.

- To bardzo poważny problem. W zespole ds. bezpieczeństwa cyberprzestrzeni poświęciliśmy na to wiele posiedzeń. Mamy kilka rozwiązań. W sferze publicznej to permanentne szkolenia, cały czas poszerzane o nowe moduły. To oczywiście nie wystarczy. W kluczowych instytucjach problem ekspertów został rozwiązany, w pozostałych, takich jak ministerstwo zdrowia, wciąż ich brakuje. Tym należy się zająć – tłumaczył Paweł Wiszniewski z Biura Bezpieczeństwa Narodowego.

– Coraz więcej wiele uczelni wypuszcza specjalistów od cyberbezpieczeństwa. Niestety, znając poziom polskich uczelni lepiej się temu przyjrzeć. Być może programami studiów nie zaadresujemy faktycznych potrzeb – tłumaczył Piotr Trąbiński. – Tutaj standardowy nabór nie pomoże. Trzeba szukać specjalistów, pasjonatów. Armia USA rekrutując osoby do obsługi dronów szukała wśród graczy komputerowych. Ci ludzie nie mieli żadnego doświadczenia wojskowego. My tracimy informatyków, bo nie mamy dla nich pensji na poziomie międzynarodowym. Większość z nich wyjeżdża. Nie wolno nam się obrażać na tych, którzy wyjechali – trzeba z nimi współpracować na tyle, na ile to możliwe.

Czy warto zatem zatrudniać fachowców zza wschodniej granicy? Tutaj ekspert NCSS, zarazem dyrektor departamentu Santander Universidades, był sceptyczny. – Jeśli to dobry specjalista, należy to oczywiście robić. W swoich strukturach mamy osoby z Białorusi, Ukrainy, Litwy. Jest jednak jeszcze kwestia bezpieczeństwa. Tu chodzi o weryfikację takiej osoby, zanim dopuści się ją do decydowania o wrażliwych systemach. To nie takie proste – tłumaczył Trąbiński.

Przestępcy w sojuszu z bandyckimi państwami

Specjalista Santander podkreślał także, że ważne jest uprzedzanie ataku hakerów. Wbrew pozorom jest to wykonalne zadanie. – To nie jest tak, że nikt nie ma wiedzy, że atak nastąpi. To widać w sieci. Na tydzień przed atakiem phishingowym hurtowo powstają fałszywe strony. Musimy jako kraj przejść z myślenia defensywnego na myślenie ofensywno – defensywne.

Cyberprzestrzeń to wielkie wyzwanie dla prawa międzynarodowego. Problem w tym, że jest zarazem najbardziej nieudokumentowana. Brakuje umów międzynarodowych, które pozwalałyby adresować działalność hakerów. Brakuje uregulowań prawnych i kryminaliści doskonale o tym wiedzą. - Wielu przestępców przenosi się do sieci, bo tam są anonimowi. Mogą atakować z dowolnego punktu na ziemi. cyberatak to teraz najlepszy sposób na łamanie prawa. Żadne przestępstwo na ziemi nie da przestępcy takiego poziomu bezpieczeństwa. Zorganizowane grupy kryminalne czują się bezpieczne w cyberprzestrzeni, a prawo międzynarodowe tu nie pomaga - tłumaczył Trąbiński

Cyberprzestrzeń to także wymarzone pole walki dla „bandyckich państw". – One chętnie korzystają z nowych systemów walki, używają destrukcyjnych praktyk świata kryminalnego. Ta agresja może dotyczyć ataków na infrastrukturę krytyczną ,ale też na nasze umysły. Wojna informacyjna to fakt - podkreślał Paweł Wiszniewski.

Czytaj też: Resort cyfryzacji: ustawa o cyberbezpieczeństwie do końca roku