MEC. ROBERT NOGACKI – jeden z najlepszych ekspertów w zakresie bezprawia urzędniczego – ocenia wydarzenia przez pryzmat interesów klientów swojej kancelarii.

Jak nie stracić płynności w sieci

Do niedawna najgorszym koszmarem policjanta był dwumetrowy mięśniak na sterydach i z bronią w ręku. Dziś stoimy u progu ewolucyjnej zmiany. Najgroźniejszy nie jest już gang szalikowców wyładowujących frustracje po meczu, ale metodyczny geek, z wyobraźnią i dostępem do internetu.

Niemal 30 mln dolarów zarobili Vitaly Korchevsky i Arkadiy Dubovoy. Dwaj finansiści, którzy postanowili skorzystać z oferty przedstawionej im przez ukraińskich hakerów. Schemat działania był równie prosty, co skuteczny. Działający z terytorium Ukrainy cyberprzestępcy regularnie włamywali się do serwerów firm, które publikują komunikaty prasowe na temat fuzji i przejęć giełdowych. Informacje te przekazywali współpracującym z nimi w USA inwestorom, przed podaniem ich do publicznej wiadomości, a ci dokonywali transakcji, na których zarabiali dziesiątki milionów dolarów. W rękach policji poza wymienionymi na wstępie mężczyznami znalazło się także siedem osób, a Departament Sprawiedliwości wydał również nakazy aresztowania przebywających na Ukrainie hakerów. Jak się okazuje to oni byli pomysłodawcami i realizatorami tego procederu. Informacje sprzedawali odbiorcom, a zyski lokowali w firmach – przykrywkach, w Makao i Estonii. Jak szacuje FBI, osiągnęli w ten sposób zysk w wysokości ok. 100 mln dolarów.

Natomiast amerykańska skarbówka nie jest pewna, do danych ilu obywateli uzyskali dostęp hakerzy, których działania wykryto w maju bieżącego roku. Początkowo informowano, że przejęto ok. 120 tys. profili podatników znajdujących się na serwerach IRS. Obecnie liczba ta urosła trzykrotnie i może wzrosnąć jeszcze, ponieważ przestępcy mieli dostęp do serwisu o wiele dłużej niż przypuszczano.

Oba te przypadki nie tylko ukazują modus operandi hakerów, ale przede wszystkim ich wyobraźnię i ogrom zasobów, do jakich mogą uzyskać dostęp. W przypadku IRS nie wykradli bowiem informacji, które mogliby w sposób wymierny wycenić i spieniężyć, a uzyskali dostęp do historii podatkowej. Niepokoi więc nie to, z jaką łatwością dokonali kradzieży informacji przez internet, ale sposób ich późniejszego wykorzystania.

Do niedawna wydawało się, że problem cyberprzestępczości omija nasz kraj, ale w ostatnim czasie kilka instytucji boleśnie przekonało się, że tak już nie jest. Konflikt na linii Warszawa – Moskwa, oraz naturalna i zupełnie przewidywalna tendencja wynikająca z rozwoju gospodarczego i technologicznego zwiastują, że w nadchodzących latach coraz częściej będziemy mieli w Polsce do czynienia z cyberprzestępczością. Jej celem będą zarówno instytucje rządowe, banki, przedsiębiorstwa, jak i osoby prywatne. Wystarczy wspomnieć o niedawnych kłopotach PLL LOT, który co prawda nie potwierdził, że padł ofiarą ataku hakerów, jednak nie podał również żadnego innego racjonalnego wyjaśnienia awarii systemu komputerowego służącego do planowania lotów. Pewne jest jedno: zawiódł system zabezpieczeń, mający chronić przed takimi incydentami.

Żadnych wątpliwości nie ma natomiast co do tego, że ofiarą ataku hakerskiego padło kilkuset klientów biznesowych Plus Banku. Haker o pseudonimie „Polsilver" na początku roku wykradł ich dane, jak również okradł kilka kont. Podobnie jak w przypadku LOT, ktoś wybrał niewłaściwego dostawcę rozwiązań technicznych, który miał dbać o bezpieczeństwo teleinformatyczne.

Według danych PwC roczne straty globalnej gospodarki wynikające z cyberprzestępczości wynoszą ok. 500 mld dolarów. Skala procederu jest więc niewyobrażalna i przekracza wartość czarnorynkowego obrotu narkotykami. To powinno nam uświadomić, że nie mamy już do czynienia jedynie z problemem rządów i banków. Hakerzy stanowią potencjalne zagrożenie dla bezpieczeństwa finansowego i spokoju każdego posiadacza konta bankowego, telefonu komórkowego, o komputerze nie wspominając. Aby uniknąć kłopotów związanych z wyciekiem danych, utratą aktywów, czy szkodą na wizerunku, należy podjąć odpowiednie działania zabezpieczające. Równocześnie należy zadbać o uświadomienie rodziny, przyjaciół, pracowników, że niebezpieczeństwo choć dotyczy sieci komputerowych, nie jest wcale wirtualne. Tak, jak w przypadku jakiejkolwiek innej formy zagrożenia, zapobieganie jego wystąpieniu jest lepszym rozwiązaniem, niż przeciwdziałanie konsekwencjom. ■

Mec. Robert Nogacki, założyciel Kancelarii Prawnej Skarbiec

BAROMETR PRZEDSIĘBIORCY

TAK

W ciągu zaledwie sześciu miesięcy od wprowadzenia w Wielkiej Brytanii korzystnej reformy podatku stamp duty, rynek nieruchomości w Anglii i Walii odnotował nieprzeciętny wzrost wolumenu przeprowadzonych transakcji. Jak wskazuje Nationwide Building Society, ilość transakcji wyniosła w tym czasie niemal 235 tys. a zarazem wpływ podatku do brytyjskiego budżetu został zmniejszony o kwotę 275 mln GBP. Szacuje się, że przeciętny nabywca nieruchomości w Wielkiej Brytanii zachował w kieszeni prawie 1800 GBP.

NIE

Grecja zamierza walczyć z zadłużeniem... prześwietlając majątki swoich obywateli. Władze podatkowe pracują nad bazą danych zawierającą szczegółowe informacje o aktywach podatników. Po jej opracowaniu, każdy podatnik zostanie zobowiązany do aktualizacji informacji dotychczas zebranych przez grecki urząd skarbowy i tym samym wykazania wszelkich posiadanych nieruchomości, samochodów, rachunków bankowych, udziałów i akcji oraz pieniędzy w gotówce. Ujawnieniu będą podlegały również źródła przychodów, które znajdują się poza granicami kraju. Regulacje prawne w Grecji mają wejść w życie w 2016 r.

MATERIAŁ: KANCELARIA PRAWNA SKARBIEC

SKARBIEC KANCELARIA PRAWNA