IK: KRYTYCZNA OCENA GRANIC LEGALNEGO HAKINGU NA TLE NOWEGO ART. 269C KODEKSU KARNEGO [ANALIZA]

- Regulacja zawarta w art. 269c k.k. sytuuje się w kontrze do ogólnoświatowego trendu walki z cyberprzestępczością, który wskazuje na konieczność podwyższania bezpieczeństwa w sieci i minimalizowania wszelkiego rodzaju zagrożeń. Wspomniana regulacja stworzyła tymczasem zachętę dla hakerów, aby sprawdzać własne umiejętności i włamywać się do baz danych osób prywatnych, firm i instytucji publicznych. Jest to tym bardziej niezrozumiałe, że obowiązek ochrony infrastruktury krytycznej przed cyberatakami powierzono Agencji Bezpieczeństwa Wewnętrznego - pisze w najnowszej analizie ekspert Instytutu Kościuszki dr Paweł Opitek.

Zasoby danych cyfrowych podmiotów publicznych i prywatnych cały czas narażone są na ataki i włamania prowadzone drogą elektroniczną. Chodzi tu o różnego rodzaju złośliwe oprogramowanie, przechwytywanie pakietów informacji, czy inne niepożądane działania typu *spoofing*, łamanie haseł, *exploity* i ataki DDoS. Realizowane są one przez przestępców wykorzystujących różnego rodzaju urządzenia i programy komputerowe. Dlatego, zgodnie z maksymą: „walcz z wrogiem jego własną bronią", najlepszym sposobem przeciwdziałania atakom i włamaniom jest testowanie systemu i sieci przy zastosowaniu identycznego oprzyrządowania, jakiego używają hakerzy. Opisane działania noszą nazwę testów penetracyjnych. Firmy i instytucje państwowe prowadzą je wykorzystując własne zaplecze logistyczne lub też zlecają czynności podmiotom zewnętrznym. Na świecie przyjęło się, że w tym ostatnim przypadku umowa cywilnoprawna szczegółowo reguluje wykonanie pentestu zabezpieczając interesy przedsiębiorcy przed nieuprawnionym wykorzystaniem informacji uzyskanych w procesie badania sieci/systemu. Test realizowany jest za zgodą administratora i w zakresie ściśle przez niego wskazanym. Sytuacja podobnie wyglądała w Polsce do 26 kwietnia 2017 r., ale zmiany wprowadzone ustawą z 23 marca 2017 r. o zmianie Kodeksu karnego przewartościowały całkowicie sytuację.

Nowy art. 269c k.k. znacznie rozszerzył granice legalnego hakingu w Polsce. Z przepisu tego wynika, że nie podlega karze osoba, która:

1) wypełniła swoim zachowaniem znamiona przestępstwa opisanego w art. 267 § 2 k.k. lub art. 269a k.k.,

2) działała wyłącznie w celu zabezpieczenia systemu informatycznego, systemu teleinformatycznego lub sieci teleinformatycznej albo opracowania metody takiego zabezpieczenia,

3) niezwłocznie powiadomiła dysponenta systemu lub sieci o ujawnionych zagrożeniach,

4) jej działanie nie naruszyło interesu publicznego lub prywatnego i nie wyrządziło szkody.

Trudno znaleźć podobne rozwiązanie w ustawodawstwie innych państw. Przeciwnie, ich przepisy decyzję o przeprowadzeniu testu penetracyjnego pozostawiają dysponentowi sieci lub systemu. Zastrzeżenia budzi już sam sposób procedowania nad kształtem noweli. Jej celem była przede wszystkim implementacja dyrektywy Parlamentu Europejskiego i Rady nr 2014/42/UE z 3 kwietnia 2014 r. w sprawie zabezpieczenia i konfiskaty narzędzi służących do popełnienia przestępstwa i korzyści pochodzących z przestępstwa w UE. W trakcie prac nad projektem w Komitecie Stałym Rady Ministrów pojawiła się propozycja wprowadzenia quasi-kontratypu dla czynu zabronionego opisanego w art. 269b § 1 k.k. Chociaż na szczeblu rządowym nie zyskała ona akceptacji, to Senat uchwałą z 16 marca 2017 r. poszedł jeszcze dalej i wprowadził art. 269c k.k. w brzmieniu: „Nie podlega karze za przestępstwo określone w art. 267 § 2 lub art. 269a, kto działa wyłącznie w celu zabezpieczenia systemu informatycznego, systemu teleinformatycznego lub sieci teleinformatycznej albo opracowania metody takiego zabezpieczenia i niezwłocznie powiadomił dysponenta tego systemu lub sieci o ujawnionych zagrożeniach, a jego działanie nie naruszyło interesu publicznego lub prywatnego i nie wyrządziło szkody". W takiej sytuacji hakerowi zostaje przypisane popełnienie przestępstwa, lecz ustawodawca uznał, że z powodu nadzwyczajnych okoliczności motywujących sprawcę, nie należy go karać.

Czytaj też: [Instytut Kościuszki: Hakować czy nie hakować? [ANALIZA]]

W zamyśle ustawodawcy, konstrukcja art. 269c k.k. dedykowana jest osobom, które z różnych powodów zajmują się hakingiem (zawodowo, hobbystycznie, naukowo). Co prawda, bez upoważnienia dokonują włamań, ale kieruje nimi szczególna postać zamiaru, tj. chęć poszukiwania niedociągnięć i „dziur" w architekturze IT, a jeśli zostaną wykryte, powiadomienia o zagrożeniu, zanim wykorzysta je inna osoba w sposób niezgodny z prawem. Komentowany przepis odnosi się do sprawcy, który wypełnił swoim działaniem znamiona czynu opisanego w art. 267 § 2 k.k. lub art. 269a k.k. Pierwszy z nich polega na uzyskaniu bez uprawnienia dostępu do całości lub części systemu informatycznego nawet bez złamania jakiegokolwiek zabezpieczenia chroniącego zasób danych. Celem hakera może być ponadto przejęcie kontroli nad maszyną bez konieczności badania zasobów jej pamięci. Chodzi o wprowadzenie oprogramowania pozwalającego zdalnie przejąć kontrolę komputera i wykorzystać go do zmasowanych ataków na strony internetowe. W trakcie ataków sieciowych, wyczerpujących znamiona art. 267 § 2 k.k., haker zapoznaje się zazwyczaj z przetwarzanymi w systemie danymi. Przestępstwo opisane w art. 269a k.k. dotyczy natomiast zakłócenia w istotnym stopniu pracy systemu komputerowego lub sieci teleinformatycznej poprzez wprowadzenie, transmisję, niszczenie, kasowanie, uszkadzanie lub zmianę danych informatycznych. Jako przykład mogą posłużyć ataki DDoS, a więc wysyłanie wielkiej ilości danych do określonego komputera, jego nadmierne obciążenie i w rezultacie spowodowanie nieprawidłowości w funkcjonowaniu maszyny. Art. 269a k.k. dotyczy istotnego zakłócenia pracy technologii, co oznacza dłuższy czas jego trwania, brak dostępu do systemu, czy znaczne spowolnienie jego działania oraz konieczność poczynienia wysokich nakładów finansowych lub logistycznych warunkujących przywrócenie stanu pierwotnego. Wynika z tego, że omawiany przepis pozwala na realizację czynności skutkujących poważnymi komplikacjami dla dysponenta sieci lub systemu. Ocena, czy konkretne działanie naruszyło interes publiczny lub prywatny lub wyrządziło szkodę ma często charakter subiektywny i zależny od wielu (nie rzadko trudnych do ustalenia) okoliczności. Jeśli na przykład haker teraz nie wykorzystał informacji uzyskanych w wyniku legalnego włamania do sieci lub systemu, to nie sposób wykluczyć, że zrobi to w przyszłości.

Zarzut, jaki należy postawić konstrukcji art. 269c k.k., to niedookreśloność i nieostrość zwrotów w nim zawartych. Weźmy zdanie: „działanie wyłącznie w celu zabezpieczenia systemu informatycznego, systemu teleinformatycznego lub sieci teleinformatycznej albo opracowania metody takiego zabezpieczenia". Znamię czasownikowe „zabezpieczyć", według słownika języka polskiego, oznacza: „zapewnić ochronę przed czymś niebezpiecznym lub szkodliwym", „uczynić bezpiecznym", „zapewnić

utrzymanie się czegoś w dotychczasowym stanie" (Słownik Języka Polskiego, www.sjp.pwn.pl.). Przenosząc to na grunt omawianego artykułu, „działanie wyłącznie w celu zabezpieczenia" może być rozumiane, jako:

- zapewnienie ochrony poprzez przejęcie zarządzania siecią lub systemem aż do czasu powiadomienia ich administratora o wykrytych nieprawidłowościach i przekazania mu sterowności danymi,
- uczynienie sieci lub systemu bezpiecznym, a zatem wprowadzenie/implementowanie nowych rozwiązań w architekturze informatycznej lub teleinformatycznej tak, aby inna osoba nie mogła powtórzyć włamania,
- inny pogląd może sprowadzać się do stwierdzenia, że haker nie ma prawa w żaden sposób „naprawiać" systemu lub sieci, a „działać wyłącznie w celu zabezpieczenia" oznacza tylko i wyłącznie poinformowanie administratora infrastruktury o wykrytych lukach i niedociągnięciach.

Mamy więc do czynienia z niedookreślonością ustawowego zwrotu, która pociąga za sobą jego nieostrość. Podobny zarzut można sformułować w stosunku do następujących pojęć zawartych w art. 269c k.k.: „niezwłocznie", „interes publiczny", „interes prywatny". Rodzi to poważne problemy interpretacyjne i podważa zasadę określoności i precyzyjności przepisów w procesie stanowienia i stosowania prawa (szczególnie ważną w prawie karnym). Wymaga się na przykład od hakera: „niezwłocznego powiadomienia dysponenta systemu lub sieci o ujawnionych zagrożeniach". Jaką formę ma przybrać takie powiadomienie i w jaki sposób powinno być zrealizowane? Czy w grę wchodzi obowiązek dochowania szczególnej staranności i podjęcia wszelkich działań celem nawiązania kontaktu z administratorem sieci lub systemu, a następnie przekazania dokładnych informacji o wykrytych nieprawidłowościach? Zachowanie takie jest pożądane, jednak treść art. 269c k.k. nie wymaga od hakera aż takiej skrupulatności. Spełni on swój prawny obowiązek, jeśli np. prześle informację na ogólnodostępną skrzynkę mailową przedsiębiorcy. I chociaż spływa do niej dziennie setki różnych wiadomości, to sprawca ma prawo domniemywać, że spełnił w ten sposób wymóg „niezwłocznego powiadomienia". W grę wchodzą jeszcze bardziej skomplikowane sytuacje: może się zdarzyć np., że „włamywacz" prześle do polskiego dysponenta sieci lub systemu informację w języku obcym (rosyjskim, arabskim, chińskim itp.). W jego świadomości skutecznie uniknie kary za popełnienie przestępstwa z art. 267 § 2 k.k. lub art. 269a k.k. i trudno będzie organowi procesowemu zakwestionować takie stanowisko. Wynika z tego, że ustawodawca stworzył przestępcom „otwartą furtkę", aby przy odrobinie znajomości prawa mogli uniknąć odpowiedzialności karnej w sytuacji, kiedy działali w innym zamiarze, aniżeli naprawa systemu lub sieci.

Czytaj też: Polska może stać się światowym liderem sektora cyberbezpieczeństwa. Raport Instytutu Kościuszki

Poczynione wyżej ustalenia prowadzą do wniosku, że regulacja zawarta w art. 269c k.k. sytuuje się w kontrze do ogólnoświatowego trendu walki z cyberprzestępczością, który wskazuje na konieczność podwyższania bezpieczeństwa w sieci i minimalizowania wszelkiego rodzaju zagrożeń. Wspomniana regulacja stworzyła tymczasem zachętę dla hakerów, aby sprawdzać własne umiejętności i włamywać się do baz danych osób prywatnych, firm i instytucji publicznych. Jest to tym bardziej niezrozumiałe, że obowiązek ochrony infrastruktury krytycznej przed cyberatakami powierzono Agencji Bezpieczeństwa Wewnętrznego (testy bezpieczeństwa). Zezwolenie „wszystkim chętnym" na testowanie takiej infrastruktury państwa polskiego jest nie do zaakceptowania. Ironizując można zapytać, dlaczego ustawodawca nie poszedł o krok dalej, i nie objął podobną regulacją włamań do samochodów, czy mieszkań – powinny one nie podlegać karze, jeśli sprawca działa wyłącznie w celu zabezpieczenia mienia i niezwłocznie powiadomi właściciela rzeczy o ujawnionych zagrożeniach. Inne pytanie brzmi: czy ktokolwiek z nas życzyłby sobie, aby haker zgodnie z literą prawa włamał się do jego skrzynki mailowej, przeczytał wszystkie wiadomości i powiadomił potem dysponenta poczty o stwierdzonych niedociągnięciach w jej zabezpieczeniu? Nikt zapewne nie chciałby doświadczyć takiej

sytuacji.

Zasadność wprowadzenia do Kodeksu karnego art. 296c k.k. nie znajduje oparcia w twierdzeniu, że umożliwi to pentesterom badanie podatności architektury IT na włamania i ataki, zanim „słabości" systemu lub sieci wykorzystają przestępcy. Otóż, przed 27 kwietnia 2017 r. prawo dopuszczało testy penetracyjne (i rzeczywiście były przeprowadzane na masową skalę) za zgodą administratora sieci lub systemu. Instytucja zgody legalizującej była najlepszym rozwiązaniem. Dawała ona dysponentowi sieci lub systemu wyłączne prawo decydowania o tym, jak administrowane przez niego środowisko cyfrowe ma być chronione i kto może podjąć działania w kierunku przełamania zabezpieczeń. Tymczasem, doświadczenie wielu firm uczy, że „nieproszony" haker, wykrywający niedociągnięcie w ich systemie, prędzej czy później żąda jakieś gratyfikacji (osobistej lub materialnej) za ujawnione nieprawidłowości.

dr Paweł Opitek - ekspert Instytutu Kościuszki, prokurator Prokuratury Rejonowej Kraków-Podgórze, członek Polskiego Towarzystwa Kryminalistycznego oraz Strumienia Blockchain/DLT i Kryptowaluty przy Ministerstwie Cyfryzacji.