PISM POLSKI INSTYTUT SPRAW MIĘDZYNARODOWYCH
THE POLISH INSTITUTE OF INTERNATIONAL AFFAIRS

NR 10/2022, 17 LUTEGO 2022 © PISM

KOMENTARZ

Cyberatak na Ukrainę

Oskar Szydłowski, Maciej Zaniewicz

Ukraińskie banki i strony rządowe padły ofiarą zmasowanego cyberataku, którego źródłem była prawdopodobnie Rosja. Bardzo prawdopodobne są kolejne ataki z jej strony, w tym na infrastrukturę krytyczną Ukrainy. Na podobne ataki narażone są państwa NATO.

Jak przebiegł atak?

Cyberatak rozpoczął się 15 lutego w godzinach popołudniowych i był kontynuowany przez następne dwa dni. Wymierzony był w strony internetowe ukraińskiego ministerstwa obrony, sił zbrojnych oraz dwóch największych państwowych banków: PrywatBank i Oszczadbank (łącznie 26 mln klientów). Był to atak typu DDoS polegający na przeciążeniu serwerów masowymi, sztucznie generowanymi zapytaniami. W konsekwencji zaatakowane strony rządowe, bankowość internetowa oraz aplikacja mobilna banku przez kilka godzin pozostawały niedostępne. Utrudnione było też działanie niektórych systemów płatności. W odpowiedzi ukraińskie służby monitorujące sieć odłączały dostęp adresom, z których pochodził podejrzany ruch. Jednocześnie klienci banków otrzymywali fałszywe wiadomości SMS z polskich numerów kierunkowych, które informowały o problemach technicznych. Cyberatak nie stanowił jednak zagrożenia dla zdeponowanych środków. Za atakiem stała najprawdopodobniej Rosja – podobny atak miał miejsce w Gruzji w 2008 r. i poprzedzał rosyjską inwazję. USA ostrzegały również, że pełnoskalowa agresja rosyjska na Ukrainę zostanie poprzedzona cyberatakiem. Rzecznik prasowy prezydenta FR zaprzeczył jednak oskarżeniom.

Jaki był cel ataku?

Jeśli potwierdzą się przypuszczenia o rosyjskim źródle cyberataku z 15 lutego, będzie on wpisywał się w metody prowadzonej przez Rosję wojny hybrydowej przeciw Ukrainie. Celem tego ataku nie było dokonanie długotrwałych szkód lub pozyskanie informacji, lecz zasianie paniki w społeczeństwie. Zablokowanie stron internetowych armii i ministerstwa obrony miało na celu obniżenie zaufania Ukraińców do zdolności obronnych państwa. Atak na banki miał z kolei spotęgować poczucie bezpośredniego zagrożenia wśród obywateli i podważyć zaufanie do systemu finansowego. Jednoczesne wykorzystanie fałszywych wiadomości SMS miało na celu skłonienie klientów banków do masowego wybierania gotówki z placówek i bankomatów.

Czy cel został osiągnięty?

Choć cyberatak przeprowadzony 15 lutego był największy pod względem skali atakiem DDoS, Ukraina jest celem tego typu operacji od 2014 r. Z tego względu oddziaływanie psychologiczne takich działań na ukraińskie społeczeństwo jest ograniczone. Sprawna komunikacja na temat zdarzenia ze strony banków oraz szybkie przywrócenie funkcjonowania stron internetowych i systemów płatności zapobiegło rozprzestrzenianiu się paniki. Udało się zapobiec m.in. masowemu pobieraniu gotówki z banków. Pomoc Ukrainie w walce z podobnymi atakami zaoferowały ponadto USA, co zwiększy bezpieczeństwo ukraińskiej cyberprzestrzeni. Rosji prawdopodobnie udało się jednak już wcześniej zinfiltrować ukraińską infrastrukturę krytyczną. Może to zostać wykorzystane do przeprowadzenia cyberataku np. na ukraińską sieć elektroenergetyczną. Tego typu działania Rosja podejmowała już m.in. w grudniu 2016 r., gdy prądu pozbawiona została 1/5 Kijowa oraz rok wcześniej, gdy ten sam problem dotknął ponad 200 tys. mieszkańców Ukrainy.

Jakie wnioski z ataku płyną dla Polski i NATO?

Ryzyko podobnych ataków na Polskę oraz państwa NATO istotnie wzrosło. W celu przeciwdziałania zagrożeniom w cyberprzestrzeni 15 lutego br. zaczął w Polsce obowiązywać pierwszy stopień alarmowy ALFA-CRP. Polska może ponadto rozważyć przetestowanie istniejących mechanizmów wykrywania i zwalczania zagrożeń w sferze cyberprzestrzeni, a także odporności infrastruktury na przeciążenia. Powinno to dotyczyć zarówno instytucji państwowych, jak i dużych podmiotów prywatnych, zwłaszcza operujących w kluczowych sektorach, np. energetyce czy bankowości. Jednocześnie, w odpowiedzi na rosnącą liczbę cyberataków, korzystne byłoby zwiększenie nakładów na cyberbezpieczeństwo. Wskazane byłoby także aktywne uczestnictwo Polski w wymianie informacji i szerszej współpracy w zakresie cyberbezpieczeństwa w ramach NATO oraz z państwami partnerskimi, w tym z Ukrainą. Korzystne, w kontekście zapobiegania podobnym atakom, byłoby wzmocnienie przekazu NATO dotyczącego reagowania także na naruszenia w sferze cyfrowej.