**aut. Andrzej Kozłowski** 31.07.2020

# UNIJNE SANKCJE ZA CYBERATAKI. SUKCES DYPLOMATYCZNY, KTÓRY NIE ZATRZYMA HAKERÓW [KOMENTARZ]

Wczorajsza decyzja Unii Europejskiej o nałożeniu pierwszych w historii sankcji za cyberataki ma znaczenie głównie symboliczne. Wysyła bowiem sygnał do społeczeństw europejskich, że Bruksela reaguje na cyberataki i stara się problem rozwiązać. Trzeba być jednak niepoprawnym optymistą, żeby wierzyć, że sankcje powstrzymają rosyjski wywiad wojskowy czy oficerów chińskiej armii przed dalszymi atakami.

Rada UE podjęła w czwartek w Brukseli decyzję o nałożeniu sankcji na sześć osób i trzy podmioty odpowiedzialne za różne cyberataki lub w nie zaangażowane. Ograniczeniami objęto czterech funkcjonariuszy GRU oraz Główny Ośrodek Specjalnych Technologii GRU. Dodatkowo, za inne ataki na państwa członkowskie UE, restrykcje zostały nałożone na dwóch obywateli Chin, jedną firmę chińską oraz jedną północnokoreańską.

Rosjanie z GRU zostali oskarżeni o próbę cyberataku na Organizację ds. Zakazu Broni Chemicznej, która miała miejsce w 2017 roku. Incydent został przerwany przez holenderskie służby specjalne we współpracy z brytyjskimi. Chińczycy zostali ukarani na atak na dostawców technologii IT w ramach światowej kampanii hakerskiej „Cloud Hopper". Północnokoreańska firma została ukarana za zaangażowanie w światowy atak ransomware WannaCry. Sankcje obejmują zakaz podróżowania na terytorium UE i zamrożenie aktywów. Ponadto osobom i podmiotom z UE zabrania się udostępniania funduszy tym osobom.

Czterech Rosjan oraz jeden obywatel Chin zostali wcześniej oskarżeni przez Departament Sprawiedliwości USA.  Gao Qiand, który znalazł się na liście UE, nie został oskarżony przez Amerykanów. Z drugiej strony dziwi brak na liście Zhu Hua i Park Jin Hyoka z jednostki APT 10, którzy wcześniej zostali oskarżenia przez FBI o udział w kampanii „Cloud Hopper".

Na liście brakuje rosyjskiego hakera Dmitrija Badina, który miał być odpowiedzialny za cyberatak na Bundestag w 2015 roku. Od czerwca pojawiały się informacje, że Berlin będzie chciał wykorzystać unijny mechanizm sankcji, aby nałożyć sankcje na Badina i szefa GRU. Według doniesień niemieckiej prasy przygotowania do nałożenia obostrzeń na osoby zaangażowanie w atak na niemiecki parlament są cały czas w toku. Członkowie UE mieli stwierdzić, że przedstawione dowody są wystarczające więc wydaje się, że kolejne sankcje to kwestia kilku najbliższych tygodni.

Nałożenie sankcji za cyberataki jest możliwe dzięki decyzji Rady Unii Europejskiej z  17 maja 2019 r. Wtedy to ustanowiono przepisy pozwalające nakładać unijne ukierunkowane środki ograniczające, by zapobiegać cyberatakom stanowiącym zewnętrzne zagrożenie dla Unii lub jej państw członkowskich. Przepisy te można również stosować do cyberataków wymierzonych przeciwko państwom trzecim lub organizacjom międzynarodowym, jeżeli uzna się to za konieczne do osiągnięcia

celów wspólnej polityki zagranicznej i bezpieczeństwa. Sankcje są jednym z narzędzi toolboxa cyberdyplomacji UE, którego celem jest zapobieganie cyberatakom oraz skuteczna odpowiedź na zagrożenia.

**Sankcje skuteczne środek odstraszania?**

Nałożenie sankcji na rosyjskie, chińskie i północnokoreańskie podmioty jest z pewnością dużym sukcesem dyplomatycznym samej UE - w szczególności, że sankcje wymagają zgody wszystkich 27 członków wspólnoty, które często mają odmienne zdanie, interesy oraz inaczej postrzegają zagrożenia rosyjskie czy chińskie. Wiele państw UE w oficjalnych komunikatach wyraziło zadowolenie z podjętej decyzji. Pochwały napłynęły również ze Stanów Zjednoczonych, Kanady i Wielkiej Brytanii. Sukces dyplomatyczny nie musi być jednak równoważny z sukcesem sankcji jako efektywnego środka walki z cyberatakami. Nawet w kręgach urzędników w Brukseli powątpiewa się czy sankcje faktycznie mogą okazać się skuteczne.

Nałożenie ich pierwszy raz w historii rodzi też szereg pytań. Z pewnością ciekawą kwestią pozostaje, które państwo dostarczyło danych wywiadowczych na tematów ataku. Wiemy, że w przypadku ataku na OPCW był to wywiad holenderskich. W pozostałych przypadkach nie wiadomo, które państwo podzieliło się takimi informacjami. Wymiana takich informacji wywiadowczych wymaga ścisłej koordynacji i zaufania pomiędzy państwami członkowskimi. Warto tu przypomnieć obawy służb holenderskich co do szczelności austriackiego kontrwywiadu. Obawiano się, że tę drogą informacje mogą przeciekać do Rosji.

Należy zadać główne pytanie, w jakim celu UE zastosowała mechanizm sankcji w odpowiedzi na cyberataki? Z odpowiedzią przychodzi dokument o priorytetach przyszłych trzech prezydencji Rady UE. Według niego sankcje maja wpłynąć na zachowanie agresorów, zmniejszyć zagrożenia płynące z cyberprzestrzeni, przysłużyć się zapobieganiu konfliktom w środowisku wirtualnym oraz gwarantować większą stabilność w cyberprzestrzeni. Odstraszanie potencjalnych podmiotów za pomocą sankcji ma niewielkie szanse powodzenia. Trudno sobie wyobrazić, że Korea Północna czy rosyjski wywiad wojskowy zaprzestaną działalności w cyberprzestrzeni w obawie przed unijnymi sankcjami. W przypadku reżimu Kim Dzonga Una może podejrzewać, że niedługo nie będzie północnokoreańskich podmiotów na które będzie można nałożyć sankcje.

Jeżeli UE nakładając sankcje chciała przysłużyć się większej stabilności w cyberprzestrzeni  to ich ogłoszenie bez przedstawienia konkretnych dowodów nie jest dobrym pomysłem.  Z drugiej jednak strony, zakładając, że UE posiada wystarczające dowody o zaangażowaniu konkretnych podmiotów w operacje, są to najczęściej wrażliwe informacje pochodzące od wywiadów państw europejskich i nie powinny być udostępniane publicznie. Pojawia się więc problem pomiędzy transparentnością podejmowania konkretnych decyzji o nałożeniu sankcji, a ochroną własnych aktywów wywiadowczych i kontrwywiadowczych. Zmniejszenie zagrożeń z cyberprzestrzeni, o którym również mowa jako jednym z celów nałożenia sankcji, będzie zdecydowanie skuteczniejsze poprzez wzmocnienie swoich sieci i systemów oraz działania edukacyjne uczulające pracowników na potencjalne zagrożenia niż sankcje, których raczej nikt się nie przerazi. W szczególności jeśli te nie są przestrzegane przez państwa, która same je nakładają. Warto tu wspomnieć przykład podróży szefa Służby Rosyjskiego Wywiadu Zagranicznego do Waszyngtonu pomimo obowiązujących amerykańskich sankcji czy przykład niemieckiego Siemensa, który łamał unijne sankcje nałożone na Rosję po aneksji Krymu i ataku na Ukrainę.

UE nie jest pierwszym podmiotem, który nałożył sankcje za cyberatak. Wcześniej zrobiły to Stany Zjednoczone, które w ten sposób ukarały Koree Północną za ataki na Sony Pictures w 2014 roku. Oczywiście sankcje w żaden sposób nie zniechęciły Pjongjangu do dalszej aktywności w cyberprzestrzeni. Podobne środki stosowane przez Amerykanów w stosunku do Iranu, Chin i Rosji

również nie odniosły żadnych skutków. Jedynym realnym środkiem, który skutecznie odstraszył wrogich hakerów, była operacja USCYBERCOM wymierzona w rosyjskie podmioty przed wyborami do Kongresu w 2018 roku. Skutecznie powstrzymało to rosyjskie zapędy przed ingerencją w wybory. W przypadku UE takie działanie nie są jednak możliwe.

Podsumowując, nałożenie sankcji jest z pewnością sukcesem dyplomatycznym pokazującym, że państwa członkowskie mimo różnych interesów potrafią się dogadać nawet jeżeli dotyczy to mocarstw pokroju Chin czy Rosji. Jest to również przykład pokazujący, że mechanizm sankcji za cyberataki nie jest tylko martwym zapisem na papierze a realne działania. Niestety sukces dyplomatyczny nie przełoży się raczej na faktyczne zmniejszenie liczby cyberataków. Zyski płynące z takich operacji zdecydowanie przewyższają ewentualne koszty w postaci sankcji.