Cyberdefence 24

aut. Szymon Palczewski 24.02.2021

ROSJA MUSI ZAPŁACIĆ ZA „HACK DEKADY". ROŚNIE PRESJA NA ADMINISTRACJĘ BIDENA

Stany Zjednoczone muszą podjąć działania na rzecz wzmocnienia cyberobrony w efekcie „hacku dekady", za który odpowiada Rosja – to główny wniosek płynący z obrad Senackiej Komisji Sił Zbrojnych USA. Podczas dyskusji wskazano również na konieczność opracowania katalogu potencjalnych odpowiedzi na określone cyberataki, w tym operacji Rosji, a także stworzenia powszechnie obowiązujących norm penalizujących wrogie działania na gruncie międzynarodowym.

Operacja hakerska, w wyniku której doszło do naruszenia federalnej infrastruktury i włamania do naczelnych instytucji w Stanach Zjednoczonych została ujawniona 13 grudnia ubiegłego roku. Celem wrogich działań był m.in. Departament Stanu, Departament Handlu, Departament Bezpieczeństwa Wewnętrznego, Pentagon, Departament Energii oraz Narodowy Instytut Zdrowia USA. Poszkodowane zostały również firmy prywatne.

Amerykanie o wrogą kampanię oskarżyli Rosję. Według specjalistów oraz polityków w Stanach Zjednoczonych operację przeprowadziła grupa rosyjskich hakerów powiązana z FSB (APT29). Zdaniem ekspertów były to działania o charakterze „klasycznego szpiegostwa", które należy uznać za „hack dekady". Amerykańscy senatorowie poszli jeszcze o krok dalej, stwierdzając, że cyberatak jest „praktycznie wypowiedzeniem wojny".

Do przeprowadzenia kampanii hakerzy wykorzystali backdoora w popularnym oprogramowaniu do zarządzania IT „Orion", który jest produktem firmy SolarWinds. To narzędzie popularne wśród podmiotów rządowych używane w wielu państwach (np. Wielkiej Brytanii) oraz organizacjach międzynarodowych (m.in. NATO).

Obecnie „hack dekady" jest przedmiotem licznych dyskusji w Stanach Zjednoczonych w kontekście kondycji cyberbezpieczeństwa tego państwa. Wspomniany cyberatak był również głównym wątkiem wtorkowego (23 lutego br.) przesłuchania w ramach Senackiej Komisji Sił Zbrojnych USA, w której uczestniczyli gen. Herbert J. Carlisle (prezes National Defence Industrial Association), Brad Smith (prezes Microsoft), dr Eric E. Schmidt (współzałożyciel Schmidt Futures), Kevin Mandia (CEO FireEye) oraz George Kurtz (CEO CrowdStrike). Podczas dyskusji specjaliści odnieśli się także do ogólnego problemu i wyzwania związanego z operacjami hakerskimi.

Rosja musi „zapłacić cenę"

Richard Blumenthal, senator z Partii Demokratycznej, wskazał, że incydent SolarWinds zwrócił uwagę na konieczność wzmocnienia obrony łańcucha dostaw, a Rosja musi „zapłacić cenę" za prowadzenie wrogich operacji w cyberprzestrzeni. Polityk jednoznacznie podkreślił, że do tej pory nie było żadnej proporcjonalnej odpowiedzi na działania Moskwy i pociągnięcie Kremla do odpowiedzialności za „hack dekady" jest niezbędne, aby w ten sposób ukształtować zasady panujące w sieci.

Stanowisko senatora poparł prezes Microsofta Brad Smith, który zaznaczył, że administracja Joe Bidena wspólnie z sojusznikami powinna pociągnąć do odpowiedzialności hakerów za ich działania – niezależnie od tego czy działają na rzecz państwa czy własnych korzyści i motywacji. Jak podkreślił, odpowiedź jest konieczna, lecz zależy ona od „różnych okoliczności". Według szefa koncernu należy stworzyć swego rodzaju „menu" potencjalnych reakcji na cyberataki i w określonych przypadkach wykorzystać przewidziane w katalogu działania.

> *Będziemy potrzebować silnej władzy wykonawczej, która posiada zaufanie i wsparcie amerykańskiej opinię publicznej, aby przeprowadzić działania w reakcji na incydent.*
>
> Brad Smith, prezes Microsoft

Ponadto, prezes Microsofta odniósł się również do szerszego problemu związanego z cyberatakami wymierzonymi w Stany Zjednoczone, wychodząc poza tematykę związaną z „hackiem dekady". Podczas dyskusji w senackiej komisji odniósł się m.in. do próby zatrucia wody w Oldsmar (Floryda) przez hackerów. W tym kontekście Brad Smith jednoznacznie wskazał, że Stany Zjednoczone muszą wyciągnąć wnioski z ostatnich wydarzeń, ponieważ wrogie działania w cyberprzestrzeni stanowią poważne zagrożenie także dla cywilów.

> *Pomyślmy o niebezpieczeństwie dla amerykańskiej ludności cywilnej, jeśli nastąpi przerwa w dostawach wody. Następnie pomyślmy o przyszłości, w których państwa nie będą musiały wysyłać rakiet ani samolotów bojowych, ponieważ będą mogły po prostu wykorzystać cyberataki do walki.*
>
> Brad Smith, prezes Microsoft

Szef amerykańskiego giganta przed senacką komisją wskazał na konieczność wzmocnienia amerykańskiej infrastruktury cyfrowej, w tym zabezpieczeń, co dotyczy nie tylko sektora publicznego, ale również prywatnego. Wynika to z faktu, że cyberbezpieczeństo, aby było skuteczne, wymaga kompleksowego podejścia.

Co więcej, Brad Smith zasugerował również, żeby rząd USA zajął się lukami w wymianie danych wywiadowczych między podmiotami prywatnymi a państwem. W tym miejscu odniósł się do kultury wywiadowczej, którą określił „kulturą potrzeby dzielenia się". Powinno się to jednak odbywać przy pełnym poszanowaniu prywatności. W procesie można wykorzystać możliwości jakie daje sztuczna inteligencja w celu zwiększenia efektywności prowadzonych działań.

Stanowisko prezesa Microsoftu poparł Kevin Mandia. CEO FireEye wskazał, że podmioty, które znajdują się na pierwszej linii niesienia pomocy w przypadku cyberataku – takie jak np. jego firma – powinny być zobowiązane prawnie do zgłaszania incydentów określonej agencji rządowej, która traktowałaby je jako poufne. Jak dodał, w odniesieniu do swoich przedmówców, konieczne jest również zidentyfikowanie konkretnego winnego odpowiedzialnego za „hack dekady" i podjęcie działań w

ramach odpowiedzi.

Przekonać Amerykanów

Ron Wyden, senator USA z Partii Demokratycznej, wskazał, że głównym zadaniem służb badających „hack dekady" jest sprawdzenie czy podmioty federalne, których infrastruktura została naruszona rzeczywiście podjęły odpowiednie środki w celu zapewnienia bezpieczeństwa. To kluczowy aspekt w kontekście dalszych działań, jakie mogą podjąć Stany Zjednoczone wobec działań wroga – punktem wyjścia musi sprawdzenie „samego siebie".

Zdaniem polityka, aby podjąć decyzję o potencjalnej odpowiedzi na incydent oraz zwiększeniu inwestycji w zakresie cyberbezpieczeństwa, konieczne jest przekonanie opinii publicznej, że rząd oraz amerykańskie firmy nie mogły zrobić nic więcej, żeby uniknąć wrogiej kampanii.

Przedstawiciele amerykańskich firm jednogłośnie zasugerowali podczas komisji, że rząd USA powinien podjąć bardziej aktywne działania na rzecz promowania międzynarodowych zasad postępowania w cyberprzestrzeni, w tym m.in. wprowadzenia powszechnego zakazu cyberataków wykorzystujących luki w oprogramowaniu.

Rosyjska „lekkomyślność" zagrożeniem dla bezpieczeństwa zbiorowego

W tym miejscu warto podkreślić, że Prezydent Stanów Zjednoczonych Joe Biden jest świadomy zagrożeń występujących w sieci i sam wezwał społeczność międzynarodową do stworzenia norm zachowań w cyberprzestrzeni podczas Monachijskiej Konferencji Bezpieczeństwa.

Jak informowaliśmy na naszym portalu, prezydent USA podczas swojego przemówienia zwrócił się do państw demokratycznych z apelem o stworzenie swego rodzaju odpowiedników zasad ruchu drogowego w obszarze technologii i cyberbezpieczeństwa, co ma być elementem walki z Chinami i Rosją.

> *Musimy ukształtować zasady, które będą kierowały postępem technologicznym oraz stworzyć normy zachowań w cyberprzestrzeni, sztucznej inteligencji, biotechnologii, tak aby ludzie z nich korzystali, a nie żeby była źródłem problemów.*
>
> Joe Biden, Prezydent USA

Odnosząc się niejako do „hack dekady", Joe Biden jednoznacznie wskazał, że Kreml atakuje demokracje i używa do tego celu hakerów. W związku z tym – zdaniem prezydenta – walka z rosyjską „lekkomyślnością" i wrogimi działaniami wymierzonymi w amerykańską i europejską infrastrukturę stało się „krytyczne dla ochrony naszego zbiorowego bezpieczeństwa".

W tym miejscu warto również podkreślić, że administracja Joe Bidena przedstawiła „trzy kroki", jakie zostaną podjęte przez Stany Zjednoczone w następstwie włamania do federalnych instytucji. Konkretne działania przedstawiła Anne Neuberger, która w Białym Domu odpowiada za cyberbezpieczeństwo. Po pierwsze, zadaniem specjalistów będzie zidentyfikowanie, a następnie „wyrzucenie" wroga z sieci. Po drugie, modernizacja federalnej infrastruktury oraz minimalizacja ryzyka ponownego wystąpienia tego typu zdarzenia w przyszłości. Ostatnim krokiem, o jakim mówiła

Anne Neuberger jest wypracowanie mechanizmów umożliwiających reagowanie na podobne incydenty w dalszej perspektywie. Specjalistka wskazała, że aby zrealizować przedstawione „kroki”, potrzeba cierpliwości, ponieważ wiążę się to kilkumiesięcznymi działaniami.

Czytaj też: Hack Dekady: Biały Dom prezentuje plan na usunięcie rosyjskiej ingerencji