aut. Łukasz Boguszewski 27.07.2018

CYBERBEZPIECZEŃSTWO W USA W 2019 ROKU - NDAA [ANALIZA]

Przedstawiciele Izby Reprezentantów i Senatu USA przyjęli na zakończonej w poniedziałek konferencji ustawodawczej projekt ustawy o zadaniach i w konsekwencji wydatkach na obronę narodową w roku budżetowym 2019 (tzw. National Defense Authorization Act). Dokument liczy ponad 2500 stron i w następnym kroku zostanie skierowany do zatwierdzenia przez obie izby parlamentu. Ostatecznie zostanie zatwierdzony przez Prezydenta USA i stanie się oficjalnie obowiązującym prawem, gwarantując od 1 października 2018 roku siłom zbrojnym USA ponad 716 mld. dolarów.

Przyjęty przez negocjatorów obu izb dokument jest istotny ze względu na zapisy dotyczące cyberbezpieczeństwa w Stanach Zjednoczonych. Projekt ustawy wskazuje na podmioty/aktorów miedzynarodowych, mające istotny wpływa na środowisko bezpieczeństwa cybernetycznego w USA. Ustawa wymienia szczególnie państwa takie jak Rosja, Chiny, Iran i Korea Północna. Mając na uwadze bezpośrednie, zidentyfikowane zagrożenie atakami cyber ze strony tych krajów, kongresmeni skierowani do prac przy projekcie ustawie zaproponowali kluczowy zapis dotyczący odpowiedniej, proporcjonalnej odpowiedzi w przypadku wykrycia ataków cybernetycznych, między innymi na infrastrukturę krytyczną. Przypomnijmy, że od 2017 roku, system wyborczy USA jest włączony w zakres infrastruktury krytycznej. Była to konsekwencja udowodnionej przez służby USA ingerencji Rosji na proces wyborczy w 2016 roku.

Trzy dni przed szczytem Putin -Trump w Helsinkach Departament Sprawiedliwości ogłosił akt oskarżenia wobec 12 oficerów rosyjskiego wywiadu. Według raportu przygotowanego przez specjalnie powołanego prokuratora do nadzorowania federalnego śledztwa w sprawie zarzutów o ingerencję Rosji w wybory prezydenckie, Roberta Muellera oficerowie GRU odpowiedzialni byli za włamanie się do systemów komputerowych Partii Demokratycznej i sabotowanie wyborów prezydenckich.

Czytaj też: GRU na celowników amerykańskiego Departamentu Sprawiedliwości [ANALIZA]

Co ciekawe, amerykanie uznali, że zaczynają tracić dominację w cyberprzestrzeni. W związku z tym ustawa narzuca na administrację Białego Domu utworzenie cyber strategii, w tym w obszarze działań NATO. Wszystko to dzieje się po tym, jak Prezydent Trump zwolnił koordynatora do spraw cyberbezpieczeństwa w *National Security Council*. Ustawa proponuje także przeznaczenie określonych środków finansowych na działania związane z przeciwdziałaniem rosyjskich operacji informacyjnych. O ile powyższe nie zaskakuje, to interesujący może być kontekst tych zapisów i koniunkcja z zakończonym niedawno Szczytem NATO oraz spotkaniem w Helsinkach prezydentów Trumpa i Putina.

Czytaj też: Szczyt w Helsinkach. Putin i Trump będą dyskutować o cyberprzestępczości

Projekt National Defense Authorization Act (NDAA) zakłada także bardziej proaktywne i ofensywne działania rządu USA w zakresie cyberbezpieczeństwa. Oznacza to w praktyce zwiększenie uprawnień dla Departamentu Obrony, o czym mówił na ostatniej konferencji w Aspen szef amerykańskiej Agencji Bezpieczeństwa Narodowego (National Security Agency - NSA) i jednocześnie dowódca US Cyber Command, generał Paul Nakasone. Mając na uwadze skomplikowany proces identyfikacji podmiotu atakującego, USA chce w pierwszej kolejności podjąć rozmowy na szczeblu rządowym, w celu powstrzymania ataku (zazwyczaj udaje się zidentyfikować grupy hakerskie „powiązane" z rządem innego państwa). Jeśli takie działania nie odniosą skutku USA zastrzega sobie prawo do jednostronnego działania, czyli wprost mówiąc do działań ofensywnych.

Czytaj też: NSA tworzy specjalną grupę zadaniową do walki z cyber zagrożeniami

Według analityków, tak szerokie uprawnienia dla Departamentu Obrony mogą nie zostać jednak zaakceptowane przez Prezydenta Trumpa, który posiada prerogatywy w kontekście gwarancji interesu narodowego USA, poprzez użycie między innymi sił zbrojnych do kształtowania polityki zagranicznej. Pomimo tego, zarówno administracja Trumpa, jak i parlament skłaniają się w NDAA do uznania operacji cyberprzestrzeni jako „tradycyjnych operacji wojskowych". Takie rozumienie cyber operacji może mieć istotne znaczenie w kontekście ataków np. na sieci elektryczne USA, co przypomnijmy miało miejsce nie tak dawno. Zatwierdzony przez kongresmenów projekt NDAA nadaje także tzw. uprawnienia *National Command Authority* dowództwu Operacji Cybernetycznych Departamentu Obrony do podejmowania proporcjonalnych działań w przypadku wykrycia ataków cybernetycznych prowadzonych przez Rosję, Chiny, Iran czy Koreę Północną.

Bardzo interesujący, z punktu widzenia ostatnich relacji Waszyngton-Pekin jest także zapis dotyczący wprost zakazu używania technologii dostarczanych przez chińskie firmy ZTE Corp i Huawei Technologies Co Ltd. W projekcie ustawy nie znalazł się jednak pierwotny zapis, nakładający sankcję na ZTE za nielegalny eksport produktów z USA do Iranu i Korei Północnej.

Czytaj też: USA:Chiński koncern ZTE może częściowo wznowić działalność