aut. Andrzej Kozłowski 04.01.2018

NOWA STRATEGIA BEZPIECZEŃSTWA USA A CYBERBEZPIECZEŃSTWO [ANALIZA]

Administracja prezydenta Donald Trump opublikowała swoją pierwszą Strategię Bezpieczeństwa Narodowego. Dokument ten wytycza strategiczne kierunki polityki zagranicznej i bezpieczeństwa Stanów Zjednoczonych. Dużą rolę odgrywa w niej cyberbezpieczeństwo oraz obrona przed agresją informacyjną. Ten ostatni temat pojawi się tutaj po raz pierwszy.

Cyberbezpieczeństwo w strategiach bezpieczeństwa Stanów Zjednoczonych

Pierwsza strategia bezpieczeństwa Stanów Zjednoczonych (*National Security Strategy – NSS)* została opublikowana w 1987 roku. Podstawy prawne zostały zdefiniowane w Ustawie Goldwater-Nichols, która była jedną z najbardziej przełomowych jeżeli chodzi o zmiany w systemie bezpieczeństwa Stanów Zjednoczonych. Strategie bezpieczeństwa raczej nie są miejscem na przedstawianie rewolucyjnych rozwiązań, ale służą nakreśleniu strategicznej wizji.

Pierwszy raz problem zagrożeń komputerowych w tych dokumentach pojawił się pod koniec kadencji Clintona, kiedy to przedstawiono różnego rodzaju nowe, hipotetyczne zagrożenia i jako jedna z nich wymieniono ataki cyfrowe na infrastrukturę krytyczną. Opublikowane przez następnego prezydenta George'a Busha Juniora kolejne dokumenty strategiczne, odpowiednio w 2002 i 2006 roku nie poruszały w ogóle tej tematyki. Zmiana dokonała się wraz z prezydenturą Barack Obamy, kiedy to po raz pierwszy poświęcono osobny rozdział w NSS zagadnieniom cyberbezpieczeństwa. Określono, że zabezpieczenie infrastruktury cyfrowej jest priorytetem oraz uznano, że proces ten nie może odbyć się kosztem wolności obywatelskich czy naruszenia prywatności. Konieczne są również inwestycje w nowoczesną technologię i kapitał ludzki. Za zapisami strategii, wdrożone zostały odpowiednie reformy. W drugiej opublikowanej strategii, kwestie cyberbezpieczeństwa nie zostały pominięte. Powtórzono większość zapisów. Z czasem znaczenie cyberbezpieczeństwa rosło.

Strategia bezpieczeństwa Stanów Zjednoczonych Donalda Trumpa

Czytaj więcej: Kontynuacja a nie rewolucja. Rozporządzenie wykonawcze Trumpa [ANALIZA]

Strategia bezpieczeństwa narodowego składa się z 4 filarów zatytułowanych: ochrona ludności i terytorium Stanów Zjednoczonych, i amerykańskiego sposobu życia (*Protect The American People, The Homeland, and The American Way of Life*); promowanie amerykańskiej dobrobytu (*Promote American Prosperity*), utrzymywanie pokoju poprzez siłę (*Preserve Peace Through Strength*), zwiększanie wpływów Stanów Zjednoczonych (*Advance American Influence*).

W pierwszym filarze znajduje się podrozdział *Keep America Safe in the Cyber Era* (Bezpieczeństwo Stanów Zjednoczonych w erze cyfrowej)

Czytamy w niej, że cyberprzestrzeń oferuje zarówno aktorom państwowym, jak i pozapaństwowym

możliwość prowadzenia kampanii wymierzonych w politykę, ekonomię oraz bezpieczeństwo Stanów Zjednoczonych bez fizycznego przekraczania granic. Cyberataki mają oferować przeciwnikom Stanów Zjednoczonych możliwość zadania poważanych strat, czasowej destabilizacji infrastruktury krytycznej, negatywnego wpływu na amerykańskich biznes, osłabienia sieci federalnych oraz ataków na narzędzia używane przez Amerykanów w codziennej komunikacji i prowadzeniu biznesu.

Podatności amerykańskiej infrastruktury krytycznej na ataki fizyczne, cybernetyczne i elektromagnetyczne oznacza, że przeciwnicy mogą zakłócić struktury dowodzenia, operacje finansowe i bankowe czy sieci energetyczne.

Zagrożone mają być również sieci federalne. Umożliwiają one rządowym agencjom wykonywanie najważniejszych zadań oraz oferowanie usług publicznym Amerykanom. Rząd musi zwiększyć skuteczność ochrony danych oraz prywatności amerykańskich obywateli. W tym celu sieci federalne muszą zostać zmodernizowane i zaktualizowane.

W strategii zauważono również, że większość czynności wykonywanych przez Amerykanów bazuje na komputerach i technologiach połączonych ze sobą, co zwiększa podatności na cyberataki. Zarówno pojedynczy użytkownicy jak i firmy prywatne muszą mieć możliwość bezpiecznego działania w środowisku wirtualnym.

Autorzy strategii zauważają, że bezpieczeństwo nie było priorytetem, kiedy internet został stworzony. Wraz z jego ewolucją, jednak rząd i sektor prywatny musi zaprojektować systemy, które będą posiadały zwiększoną odporność na ataki od samego początku. Sytuacja, że są one dodawane w późniejsze fazie jest nie od zaakceptowania. Czyli podkreślono konieczność tzw. security by design. Podkreślono, jednak że proces ten musi się odbywać z poszanowaniem wolności rynkowych, konkurencji gospodarczej oraz ograniczonej roli rządu sprowadzającego się głównie do wdrażania rozwiązań prawnych. Strategia zwraca uwagę, że obecna budowa infrastruktury cyfrowej nowej generacji daje takie możliwość.

W NSS 2017 w ramach pierwszego filaru zasugerowano kilka rozwiązań, które powinny zostać jak najszybciej wdrożone. Po pierwsze autorzy dokumentu rekomendują przeprowadzenie oceny ryzyka w 6 kluczowych obszarach: bezpieczeństwa narodowego, energii, finansów i bankowości, komunikacji, bezpieczeństwa i transportu. Należy stwierdzić, gdzie cyberataki będą miały katastrofalny efekt a gdzie mogą doprowadzić do reakcji łańcuchowej (*cascading conseqences*).

Drugim rozwiązaniem ma być natychmiastowo modernizacja federalnych sieci i systemów. Zostaną użyte najnowsze rozwiązania z sektora prywatnego, współdzielone usługi oraz najlepsze praktyki w celu usprawnienia działania sieci i systemów. W Stanach Zjednoczonych ma również zostać wprowadzony internet 5G na szeroką skalę, co doprowadzi do poprawy jakości życia oraz zwiększy konkurencyjność.

Trzecim postulatem jest odstraszanie oraz neutralizacja wrogich podmiotów. Rząd federalny ma zapewnić właścicielom infrastruktury krytycznej odpowiednie możliwości, informacje oraz zdolności do zapobiegania atakom na elementy amerykańskiej infrastruktury krytycznej. Zapowiedziano również natychmiastowe i dotkliwe konsekwencje dla wszystkich podmiotów zarówno państwowych jak i niepaństwowych, które będą zaangażowanie w poważne działania w cyberprzestrzeni wymierzone w Stany Zjednoczone. Planuje się w tym obszarze również bliską współpracę z sojusznikami. Trudno będzie jednak zrealizować ten postulat, kiedy likwiduje się osobną komórkę w Departamencie Stanu odpowiedzialną za współpracę w cyberprzestrzeni z innymi państwami.

Kolejnym wielokrotnie już powtarzanym postulatem jest zwiększenie wymiany danych, szczególnie z operatorami infrastruktury krytycznej. Chodzi szczególnie o ocenę zapotrzebowania na informacje

oraz na likwidację barier w dzieleniu się danymi, szczególnie tajnymi. Zwiększone mają również zostać zdolności Stanów Zjednoczonych do atrybucji cyberataków.

Ostatnim proponowanym rozwiązaniem jest wprowadzenie obrony wielowarstwowej tak żeby zagrożenia pozostawały w konkretnych sieciach, a nie przedostawały się dalej. W ramach pierwszego filaru strategii podkreślono również po raz pierwszy zagrożenie płynące z działalności innych państw w sferze informacyjnej, której celem może być podważenie systemu demokratycznego w Stanach Zjednoczonych. Wskazano tutaj na Rosję.

Czytaj więcej: Współpraca USA-Rosja w cyberprzestrzeni [ANALIZA]

W ramach drugiego filaru podkreślono, konieczność nadania priorytetów dziedzinom gospodarki, absolutnie kluczowym dla bezpieczeństwa i wzrostu gospodarczego takim jak badania nad danymi, szyfrowaniem, technologiami autonomicznymi, nanotechnologią, zaawansowanymi technikami komputerowymi czy sztuczną inteligencją, która może poprawić komfort jazdy ale również zwiększyć efektywność bojową. W tym celu rząd Stanów Zjednoczonych musi poprawić zrozumienie najnowszych trendów IT i tego jak wpływają one na amerykańskie strategię i programy.

W ramach trzeciego filaru wymieniono również działania sił zbrojnych w cyberprzestrzeni. Wymieniono, że operacje prowadzą w niej zarówno podmioty państwowe (tu wskazano głównie na Rosję i Chiny) jak i niepaństwowe, które wykorzystują cyberataki do wojny informacyjnej, dezinformacji czy wyłudzeń. Mają możliwość spowodowania znacznych zniszczeń przy jednocześnie niskich kosztach inwestycji. Przykładowo są w stanie podważyć wiarę w instytucje demokratyczne oraz globalny system ekonomiczny. Zdaniem autorów dokumentu, wiele państw postrzega zdolności w cyberprzestrzeni jako narzędzie zwiększania swojego wpływu oraz ochrony rządów autorytarnych. Cyberataki. jak słusznie zauważyli autorzy koncepcji, stały się elementem współczesnego konfliktu zbrojnego. Zgodnie z proponowanymi sugestiami, Stany Zjednoczone powinny zwiększyć umiejętności namierzenia przeciwnika, zwiększyć arsenał narzędzi oraz liczbę osób pracujących w obszarze cyberbezpieczeństwa. Zapowiedź ta jest jednak sprzeczna z polityką administracji Trumpa, która zamroziła nowe zatrudnienia pracowników federalnych. Rekomenduje się również efektywniejsze zintegrowanie operacji w cyberprzestrzeni z innymi rodzajami działań wojskowych. Jest to odpowiedź na zarzuty oficerów sił zbrojnych, którzy skarżyli się, że używanie cyberzasobów jest zbyt restrykcyjne, a poziom zarządzania nimi znajduje się na za wysokim szczeblu dowódczym, mocno utrudniając ich wykorzystanie. Ponadto wskazano również na konieczność rozwinięcia nowych koncepcji prowadzenia wojny w cyberprzestrzeni, co może zapowiadać opublikowanie nowej strategii cyberbezpieczeństwa Departamenu Obrony.

Czytaj więcej: Razem czy osobno. Przyszłość NSA i USCYBERCOM [ANALIZA]

W podrozdziale „information statecraft" podkreślono również zagrożenie ze strony przeciwników Stanów Zjednoczonych, którzy „uzbroili informację" w celu zaatakowania instytucji i wartości, które są fundamentem wolnego społeczeństwa. Wrogowie wykorzystują techniki marketingowe, obierając na cel pojedynczych użytkowników bazując na ich aktywności w sieci, zainteresowaniach i wyznawanych wartościach. Szerzą dezinformację i propagandę. Ryzyko dla bezpieczeństwa narodowego Stanów Zjednoczonych będzie tylko rosnąć ze względu ma coraz większe możliwości łączenia informacji pochodzących ze źródeł komercyjnych oraz informacji osobowych przez wykorzystanie sztucznej inteligencji i uczenia maszynowego. Ponadto zwrócono uwagę, że stale zwiększająca się liczba przecieków danych o amerykańskich obywatelach zarówno z sektora prywatnego jak i publicznego daje przeciwnikom ogromną ilość informacji i możliwości.

Czytaj więcej: Wizyta Trumpa w Polsce. Zagrożenia informacyjne [ANALIZA]

Jak zauważają autorzy strategii, Chiny łączą dane i użycie sztucznej inteligencji w celu oszacowania lojalności własnych obywateli. Grupy dżihadystyczne kontynuują prowadzanie kampanie informacyjne pełne przemocy i nienawiści, co ma zachęcić rekrutów do atakowania Amerykanów i ich sojuszników. Strategia podkreśla, że Rosja znowu wykorzystuje działania informacje jako część swojej ofensywny w cyberprzestrzeni w celu wywarcia wpływu na opinię publiczną na świecie. Wykorzystuje w tym kampanie wpływu na które składają się działania wywiadowcze, fałszywe konta w mediach społecznościowych, media państwowe czy trolle. Amerykańska odpowiedź na to zagrożenie była dotychczas dalece niewystarczająca.

Autorzy rekomendują podjęcie szeregu działań. Ich zdaniem kluczowe jest zrozumienie jak działają przeciwnicy i jak osiągają przewagę informacyjną i psychologiczną. Niezwykle istotne jest wzmocnienie dyplomacji publicznej. Jest to klucz do efektywnej rywalizacji na tym polu. Po drugiej, stworzenie spójnej kampanii komunikacyjnej w celu promowania interesów Stanów Zjednoczonych i przeciwdziałania zagrożeniom ideologicznym ze strony radykalnych grup ekstremistycznych i rywalizujących państw. Następna kwestia dotyczy aktywizacji lokalnych społeczności, które mają być najbardziej skuteczne w rywalizacji ideologicznej. Mogą one zaoferować atrakcyjną alternatywę do przekazów medialnych pełnych nienawiści i przemocy. Ponadto podkreślono rolę sektora prywatnego, który może wspomóc promowanie wartości. Stany Zjednoczone nawołują również inne państwa do wzięcia większej odpowiedzialności za walkę z mową nienawiści.

Pomimo, mniejszego osobistego zainteresowania prezydenta Trumpa tematami cyberbezpieczeństwa, widać po najnowszej strategii, że kwestie cyberbezpieczeństwa staja się o tyle ważne i istotne, że po prostu nie można ich pominąć w dokumencie takiej wagi. W żadnej innej strategii nie poświęcono tyle miejsca kwestiom związanym z cyberbezpieczeństwem czy innowacjami technologicznymi, co wskazuje że obecna administracja rozumie zagadnienia cyberbezpieczeństwa. Większość kwestii była już wspominana przy innych dokumentach strategicznych. Zupełna nowością jest jednak bezpośrednie odwołanie się do kwestii bezpieczeństwa informacyjnego i potraktowanie informacji jako możliwej broni. Zapis ten powstał na skutek rosyjskiej ingerencji w ostatnie wybory prezydenckie. Strategia też jest zdecydowanie bardziej konfrontacyjna. Wprost wskazuje na zagrożenia ze strony Rosji i Chin oraz jasno artykułuje, że Stany Zjednoczone odpowiedzą na agresję w cyberprzestrzeni.

Oczywiście, należy pamiętać, że strategia jest tylko pewnym wyznacznik i nie oferuje żadnych konkretnych rozwiązań, ale najczęściej pokazuje drogę, którą pójdzie administracja oraz komunikuje światu priorytety Stanów Zjednoczonych. Z tego dokumentu wynika, że rola cyberbezpieczeństwa wyłącznie rośnie.