Cyberdefence 24

23.01.2019

BEZPIECZEŃSTWO SIECI 5G WŚRÓD NAJWAŻNIEJSZYCH WYZWAŃ NA 2019 ROK WEDŁUG ŚWIATOWYCH EKSPERTÓW CYBERBEZPIECZEŃSTWA

Najważniejsi decydenci, w tym instytucje publiczne, powinny działać odpowiedzialnie w poszukiwaniu odpowiedzi na największe zagrożenia cyberbezpieczeństwa, jak wynika z najnowszych *Rekomendacji CYBERSEC 2018* Instytutu Kościuszki. Publikacja to wynik debat podczas IV Europejskiego Forum Cyberbezpieczeństwa, konferencji angażującej ponad 150 międzynarodowych ekspertów i ponad 1000 uczestników, w tym przedstawicieli rządów, organizacji międzynarodowych oraz sektora prywatnego, mających wpływ na kierunki rozwoju strategii i polityk dla cyberbezpieczeństwa. Motywem przewodnim tegorocznego Forum było zaufanie w cyberprzestrzeni, a jego dyskusje odbywały się w czterech równoległych ścieżkach tematycznych: Państwo, Obrona, Przyszłość i Biznes.

- Prelegenci mówili jednym głosem – musimy budować zaufanie, a żeby je zapewnić, potrzebujemy narzędzi. Musimy być elastyczni i stale gotowi do działania – podkreśla dr Joanna Świątkowska, Dyrektor Programowy CYBERSEC Forum. Do tej rekomendacji dołącza się Izabela Albrycht, Przewodnicząca Komitetu Organizacyjnego konferencji. - Przewidujemy, że rok 2019 będzie definiowany przez jeszcze bardziej złożone incydenty w cyberprzestrzeni. Nie wygramy tej bitwy bez koncentracji wysiłków naszych rządów i firm na zabezpieczeniu cyfrowego DNA świata – podkreślała, ogłaszając motto piątej, jubileuszowej edycji CYBERSEC Forum, która odbędzie się w dniach 29-30 października 2019

Cyberbezpieczeństwo powinno zostać wzmocnione poprzez zamówienia publiczne

Kraje powinny uwzględniać kryteria bezpieczeństwa w zamówieniach na kluczową infrastrukturę ICT, a cena nie powinna być czynnikiem decydującym. Aby realnie wspomóc krajowe organy w radzeniu sobie z obecnym wyzwaniami, szczególnej analizie powinny zostać poddane plany działania, cele, kryteria zamówień i certyfikaty w kwestii bezpiecznych zamówień publicznych. Zdecydowanie zaleca się, aby instytucje oraz organy publiczne pozostawały w stałym kontakcie z agencjami bezpieczeństwa i konsekwentnie wdrażały strategie cyberbezpieczeństwa m.in. poprzez instrument zamówień publicznych.

W najbliższym czasie przeglądowi zostanie poddany niezwykle ważny akt prawny - **unijna dyrektywa ds. zamówień publicznych**. Biorąc przykład z rozdziału zatytułowanego "zielone zamówienia publiczne" wymuszającego wymóg zamówień "przyjaznych dla środowiska", w dyrektywie należałoby uwzględnić rozdział zatytułowany "bezpieczne zamówienia publiczne".

Kraje Trójmorza powinny przygotować plany inwestycyjne i zebrać fundusze na realizację

projektów w ramach filaru cyfrowego. Cyberbezpieczeństwo musi być fundamentem każdego podejmowanego działania w ramach inicjatywy.

Aby móc wdrożyć projekty w filarze cyfrowym, kraje członkowskie Inicjatywy Trójmorza powinny wspólnie ubiegać się o środki finansowe dostępne w nowych Wieloletnich Ramach Finansowych UE. Priorytetowym przedsięwzięciem w tej dziedzinie powinna być Cyfrowa Autostrada Trójmorza (*3 Seas Digital Highway*) – projekt zainicjowany przez Instytut Kościuszki oraz grupę think-tanków z Europy Środkowo-Wschodniej. Możliwe źródła jej finansowania to m.in. instrument "Łącząc Europę", program "Cyfrowa Europa", a także zasoby krajowe oraz fundusz Inicjatywy Trójmorza.

- Aby zrealizować projekt Cyfrowej Autostrady Trójmorza, każde państwo powinno zachęcić regionalne firmy telekomunikacyjne do budowy wzajemnych połączeń i wspólnych inwestycji - mówi prezes Exatel, Nikodem Bończa Tomaszewski podczas wywiadu dla CYBERSEC TV. **– Kraje Trójmorza powinny rozważyć możliwość inwestycji we wspólną infrastrukturę światłowodową budowaną np. wzdłuż autostrad.** Infrastruktura ta mogłaby być dostępna w całym modelu sprzedaży dla każdego kto byłby nią zainteresowany. Stanowiłaby silną zachętę dla całej gospodarki - nie tylko cyfrowej, lecz także dla tradycyjnego przemysłu, co ożywiłoby integrację całego regionu - twierdzi prezes Exatel.

Cyberbezpieczeństwo, a także postawa *security by design* musi stanowić podporę dla wszystkich działań i projektów w każdym z filarów Inicjatywy Trójmorza, czyli energii, transportu i cyfryzacji. Należy porzucić sposób działania w stylu "zrób rzeczy szybko i napraw je później", zwłaszcza że rozwiązania cyfrowe są dziś podstawą niemal wszystkich kluczowych procesów, od których zależy bezpieczeństwo społeczno-ekonomiczne.

- Inicjatywa Trójmorza jest niezwykle ważna, ponieważ kryje w sobie potencjał stworzenia silnej sieci cyfrowej łączności - podkreśla John Frank, wiceszef Microsoft. - Bez łączności, lokalne gospodarki nie mogą się rozwijać i korzystać z niewiarygodnych możliwości, które są dzisiaj dla nas dostępne. Nie żyliśmy nigdy w lepszych czasach aby skorzystać z okazji i popłynąć z nurtem technologii i innowacji.

Rozwój 5G musi być nieodłącznie skorelowany z działaniami zapewniającymi cyberbezpieczeństwo

Rozwijając technologię 5G należy mieć na uwadze, że potrzeby klienta nie mogą przysłaniać potrzeby zapewnienia cyberbezpieczeństwa - bezpieczeństwo i funkcjonalność muszą iść ze sobą w parze. **Słowo klucz to odpowiedzialność:** producenci urządzeń podłączonych do sieci powinni planować odpowiedzialne działania dążące do podniesienia świadomości użytkowników; wszyscy użytkownicy (prywatni i publiczni) powinni z kolei czuć się odpowiedzialni za swoje zachowania i przestrzegać „zasad higieny” w cyberprzestrzeni.

- Świadomość użytkowników jest bardzo ważna, ale musimy pamiętać, że bezpieczeństwo 5G znajdzie się w rękach właścicieli infrastruktury - zaznacza Nikodem Bończa Tomaszewski, szef Exatel podczas panelu dyskusyjnego CYBERSEC 2018. – Właśnie dlatego w Polsce i krajach regionu jedną z fundamentalnych kwesti jest sposób, w jaki zbudujemy tę infrastrukturę.

Operatorzy i właściciele infrastruktury 5G powinni budować swoje modele biznesowe w ramach systemu publiczno-prywatnego, który zapewni efektywność, zwiększy zaufanie oraz podniesie poziom cyberbezpieczeństwa. Dzięki wdrożeniu infrastruktury 5G, to operatorzy i właściciele będą mieli największy wpływ na cyberbezpieczeństwo przyszłości. Właśnie dlatego kluczowa jest decyzja kto i z kim współpracował będzie w łańcuchu wartości telekomunikacyjnych.

Rozwój zdolności ofensywnych nie powinien być już tematem tabu dla państw

Jeśli chodzi o wykorzystywanie narzędzi ofensywnych do celów obronnych, należy skupić się na rozwinięciu zasad zaangażowania, kontroli politycznej i legalności. Charakter ofensywnych działań w cyberprzestrzeni jest tematem wyjątkowym i będzie wymagał wzmożonego wysiłku. Ofensywne działania prowadzone w cyberprzestrzeni maja często „jednorazową" wartość. To sprawia, że państwa członkowskie NATO niechętnie ujawniają swoje metody i zdolności, ponieważ obecny model zmusza ich do dostarczenia efektów, nie zaś narzędzi. Sytuacja ta stwarza nowe potrzeby z zakresu planowania współpracy - szczególnie w kontekście międzynarodowym.

- Należy podkreślić, że jakakolwiek decyzja czy działanie podjęte przez państwo pozostanie w ramach prawa międzynarodowego. Prawo międzynarodowe dotyczy cyberprzestrzeni. Prawo międzynarodowe stosuje się do zdolności i działań ofensywnych. Nie ma co do tego wątpliwości - podkreśliła ambasador Marina Kaljurand, przewodnicząca Światowej Komisji ds. Stabilności Cyberprzestrzeni i była minister spraw zagranicznych podczas Forum CYBERSEC 2018.

Wykorzystanie zdolności ofensywnych wymaga dokładnej analizy konsekwencji, a przy ich wdrożeniu należy wziąć pod uwagę szeroką perspektywę i powiązania pomiędzy domenami operacyjnymi.

Zabezpieczanie cyfrowego łańcucha wartości powinno być wbudowane w DNA każdego działania w cyberprzestrzeni

Koncepcja bezpieczeństwa cyfrowego łańcucha wartości ma zasadnicze znaczenie dla wszystkich działań w obszarze cyberbezpieczeństwa. Jak wyjaśnia Edna Conway, Chief Security Officer, Global Value Chain w Cisco Systems - **łańcuch wartości, w kontekście technologii informacyjnej i komunikacyjnej, to kompleksowy cykl życia dowolnego rozwiązania, czy to oprogramowania, usługi czy sprzętu.** Obecnie w naszym usieciowionym świecie jesteśmy całkowicie współzależni. Kluczową kwestią jest identyfikacja podmiotów trzecich, na których polegamy, a następnie spełnienie i wdrożenie wymagań pozwalających zapewnić bezpieczeństwo. Myśląc o cyberbezpieczeństwie, musimy myśleć kompleksowo, biorąc pod uwagę bezpieczeństwo fizyczne, logiczne, operacyjne, a także bezpieczeństwo behawioralne, bezpieczeństwo informacji i bezpieczeństwo technologii.

Najważniejsza jest współpraca publiczno-prywatna. Musimy określić podstawowe wymogi bezpieczeństwa w oparciu o rozwiązania międzynarodowe. Powinniśmy myśleć nie tylko o rozwiązaniach regionalnych czy krajowych, lecz także globalnych.

Państwa członkowskie UE i NATO powinny podjąć zdecydowane działania pod względem atrybucji

W przypadku cyberataku, kwestię przypisania odpowiedzialności należy traktować nie tylko jako wyzwanie techniczne, lecz także polityczne, wymagające spojrzenia z perspektywy wszystkich domen operacyjnych.

- Rola atrybucji wzrasta coraz mocniej - mówi Ciaran Martin, CEO Narodowego Centrum Cyberbezpieczeństwa w Wielkiej Brytanii w wywiadzie dla CYBERSEC TV. Martin wyjaśnia, iż chodzi przede wszystkim o zdobycie dowodów i zwiększenie transparentności , dzięki czemu można przekonać obywateli, kto kryje się za konkretnym cyberatakiem. – Atrybucja daje nam informacje, które możemy przekazać firmom, instytucjom publicznym i obywatelom. Możemy dzięki temu także przekazać im narzędzia do ochrony przed przyszłymi atakami. - dodaje dyrektor NCSC.

Eksperci podczas CYBERSEC 2018 zalecili również rozbudowę Zestawu Unijnych Narzędzi Dyplomacji Cyfrowej (*EU Cyber Diplomacy Toolbox*), który stanowi ramy wspólnej dyplomatycznej reakcji UE na wrogą działalność w cyberprzestrzeni. Kolejną propozycją działań jest wzmocnienie współpracy

między podmiotami, które mogą pomóc w ustalaniu sprawców ataków, w tym - sektorem prywatnym i państwom spoza Unii Europejskiej.

Czas na zmianę podejścia z biernego na aktywne

Powinniśmy działać zaczynając od pozornie podstawowych kroków - w rzeczywistości to właśnie one istotnie zwiększą cyberbezpieczeństwo w poszczególnych podmiotach. Rząd brytyjski stworzył ramy "aktywnej obrony" składające się z zestawu nieodpłatnych, zautomatyzowanych środków, które pomagają użytkownikowi wyeliminować liczne cyberzagrożenia. Podobne działania można wprowadzić na całym świecie.

- Aktywna obrona polega na działaniu. Chodzi po prostu o to, by nie być biernym. - wyjaśnia Ciaran Martin, szef NCSC. Chodzi o wzmocnienie istniejącej technologii, zabezpieczenie przepływu danych, powstrzymanie fałszowania, likwidowanie szkodliwych stron internetowych, po to, by chronić użytkowników cyberprzestrzeni - dodaje Martin.

Aby zabezpieczyć cały ekosystem cyberbezpieczeństwa, rynek pracy powinien być postrzegany całościowo

Utrzymanie bezpiecznego i stabilnego rozwoju jest absolutną podstawą pozwalającą chronić cały ekosystem i zapobiegać potencjalnym zagrożeniom. Do osiągnięcia tych celów potrzebujemy programistów stawiających bezpieczeństwo na pierwszy miejscu.

- Ekosystem cyberbezpieczeństwa składa się nie tylko z osób zajmujących się wykrywaniem błędów obniżających bezpieczeństwo oraz naprawiających owe błędy, lecz przede wszystkim z tych, którzy im zapobiegają dzięki poprzez pisanie bezpieczniejszego kodu - mówi Katie Moussouris, założycielka i prezes Luta Security oraz sławna hakerka i pionierka *bug bounty*. - Aby zabezpieczyć globalny ekosystem, wszystkie ręce muszą być na pokładzie. - dodaje Moussouris.

Planując metody ochrony danych, myśl przyszłościowo

Musimy pamiętać, że , że zaszyfrowane dane, które dzisiaj uważamy za przetwarzane w sposób bezpieczny , w bliskiej przyszłości mogą zostać odczytane ze względu na rozwój technologii kwantowych. Już teraz należy zaplanować skuteczne sposoby ochrony przed potencjalnymi działaniami odszyfrowującymi.

Europa musi przyspieszyć budowę własnych komputerów kwantowych. Poza sprzętem kwantowym istnieje również potrzeba opracowania oprogramowania. **Rekomendowane jest stworzenie i opracowanie europejskiej polityki kryptograficznej.**

Istnieją dwa obszary, na których należy się skoncentrować:

- **Brak dowodu zaufania** - jak aktualizować starsze urządzenia i starsze metody szyfrowania aby chronić użytkowników;
- **Ustanawianie standardów** w zakresie zdolności kryptograficznych wewnątrz organizacji.

Rozwiązania w technologii chmury mogą znacznie zwiększyć zaufanie i bezpieczeństwo, przy jednoczesnej oszczędności budżetu przeznaczonego na cyberspecjalistów

Wdrażanie wielu nowoczesnych technologii, takich jak przetwarzanie w chmurze, wymaga zaufania. Zaufanie opiera się na przejrzystości technologii oraz weryfikacji bezpieczeństwa i prywatności (przy użyciu, między innymi, certyfikatów lub standardów). Mechanizmy budowania zaufania do technologii cyfrowych powinny być zatem promowane w całym regionie.

- Zaufanie ma kluczowe znaczenie dla nas wszystkich i dla wszystkiego co robimy. Korzystanie z technologii chmury i przeniesienie dużych ilości danych na serwery stron trzecich może stawiać pytania o to, jak te duże centra danych chronią nasze dane - powiedział Pablo Chavez, wiceprezes w Google Cloud podczas CYBERSEC 2018. - Mamy możliwość pokazania naszym klientom, że dane w chmurze rzeczywiście są bardzo bezpieczne i że znajdują się pod ich kontrolą.

Wiele firm nie może sobie pozwolić na zatrudnianie wysoce wykwalifikowanych specjalistów ds. cyberbezpieczeństwa. Dostawcy usług w chmurze są natomiast w stanie dostarczać klientom bezpieczne rozwiązania zarządzania danymi. Chmura często zapewnia również wyższy poziom odporności. Przykładowo, ataki typu "odmowa usługi"(DoS) mają stosunkowo niskie szanse powodzenia w środowisku chmury w porównaniu do środowiska korporacyjnego. Chmura umożliwia także szybsze łatanie błędów w podstawowej infrastrukturze.

Europejski system certyfikacji bezpieczeństwa chmury (*European cloud security certification scheme*), który zostanie oparty na istniejących rozwiązaniach i określi wspólne kontrole bezpieczeństwa na poziomie europejskim, może znacząco zwiększyć zaufanie i przejrzystość struktury. W przyszłości powinniśmy jednak opracować szczegółowe wytyczne i wymagania dla poszczególnych sektorów korzystających z usług w chmurze.