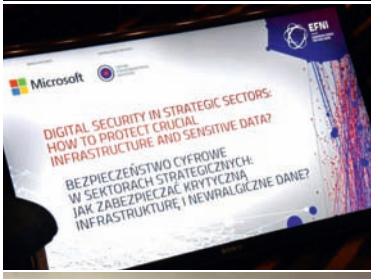
Bezpieczeństwo infrastruktury krytycznej.

JAK JE ZAPEWNIĆ W WARUNKACH CYBERNETYCZNEGO „DZIKIEGO ZACHODU”?

CENTRUM STOSUNKÓW MIĘDZYNARODOWYCH

RELACJE

10/2015 www.csm.org.pl



EFNI
EUROPEJSKIE FORUM NOWYCH IDEI

Zapewnienie bezpieczeństwa w cyberprzestrzeni, którą amerykański prezydent Barack Obama lubi porównywać do Dzikiego Zachodu, wymaga zdecydowanych działań państwa i podmiotów prywatnych. Jednak dla polityków temat bezpieczeństwa w sieci nie należy do atrakcyjnych, bo trudno go dostrzec i sprzedać medialnie. Tymczasem postępująca urbanizacja i rosnąca złożoność infrastruktury współczesnego państwa dramatycznie zwiększają skalę potencjalnych skutków jej uszkodzenia (tzw. efekt kaskadowy).

Infrastruktura krytyczna w erze współzależności

Głęboką współzależność poszczególnych elementów współczesnej kluczowej infrastruktury państwa uwidocznił niedawny pożar Mostu Łazienkowskiego w Warszawie. Oprócz oczywistych niedogodności odczuwanych przez mieszkańców stolicy, pociągnął bowiem za sobą znacznie mniej oczekiwane konsekwencje. Uszkodzenie przebiegających pod mostem linii telefonicznych i światłowodów spowodowało m.in. odcięcie od komunikacji telefonicznej Urzędu Miejskiego w Białymstoku. Z kolei coraz powszechniejsze podłączanie systemów kontroli jej elementów do Internetu przynosi dodatkowe zagrożenia ze sfery cyberprzestrzeni. Jednym z najbardziej spektakularnych przykładów było zainfekowanie irańskiej elektrowni atomowej wirusem Stuxnet, który spowodował czasową utratę kontroli nad wirówkami wzbogacającymi uran.

Choć powszechne jest przekonanie o **znaczeniu infrastruktury krytycznej jako fundamentu stabilnego i bezpiecznego funkcjonowania państw i społeczeństw**, więcej trudności nastręcza pytanie, **co w erze głębokiej współzależności i ekspansji technologii teleinformatycznych powinno być uznane za „krytycznie ważne”.** Obowiązująca w Polsce ustawa o zarządzaniu kryzysowym definiuje infrastrukturę krytyczną jako „systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty, w tym obiekty budowlane, urządzenia, instalacje, usługi kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania administracji publicznej, a także instytucji i przedsiębiorców”. Do jej elementów zaliczone zostały systemy:

- zaopatrzenia w energię, surowce energetyczne i paliwa,
- łączności sieci teleinformatycznych,
- finansowe,
- zaopatrzenia w żywność,
- zaopatrzenia w wodę,
- ochrony zdrowia,
- transportowe,
- ratownicze,
- zapewniające ciągłość działania administracji publicznej,
- produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych.

Nie mniej ważną kwestią praktyczną jest **identyfikacja najbardziej zagrożonych elementów tej infrastruktury oraz tych,**

których uszkodzenie może wywołać najpoważniejsze zagrożenia. W tym kontekście często wskazywana jest **energetyka**, w której szczególnie rozpowszechnione jest stosowanie automatyki przemysłowej (uważanej za szczególnie wrażliwą na cyberataki). Ujawnione niedawno informacje na temat cyberataku na turecki odcinek ropociągu Baku-Tbilisi-Ceyhan, który spowodował wybuch i poważny pożar, są na to dowodem. Ze względu na wysoki poziom uzależnienia technologicznego oraz stopień współzależności, **wśród najbardziej wrażliwych na cyberataki elementów infrastruktury krytycznej wymieniany jest także sektor finansowy**. Już teraz ponosi on największe straty z powodu ataków w cyberprzestrzeni. Jeszcze większą szkodę może wyrządzić spadające zaufanie klientów. Lista sektorów jest znacznie dłuższa.

Współpraca na linii państwo - biznes oraz na poziomie międzynarodowym

Wypracowanie podejścia do zapewnienia cyberbezpieczeństwa infrastruktury krytycznej **komplikuje fakt, że jej część (a w wielu krajach nawet zdecydowana większość) znajduje się w rękach prywatnych lub prywatne firmy są jej operatorami**. Oznacza to **konieczność współpracy państwa z podmiotami prywatnymi**. Jak taka współpraca powinna jednak wyglądać w szczegółach? Czy niezbędne jest nakładanie na prywatne firmy zobowiązań w dziedzinie cyberbezpieczeństwa, czy też lepsze efekty przynosi podejście dobrowolne? W tym pierwszym kierunku zmierzają przepisy unijnej **Dyrektywy w sprawie środków mających na celu zapewnienie wspólnego wysokiego poziomu bezpieczeństwa sieci i informacji w UE (Dyrektywa NIS)**. W jej projekcie na podmioty zaliczone do infrastruktury krytycznej został nałożony **obowiązek (pod groźbą sankcji) spełnienia określonych wymogów bezpieczeństwa**. Jednocześnie kontrowersje, a przez to opóźnienie przyjęcia regulacji wywołuje pytanie o to, czy do infrastruktury krytycznej włączyć dostawców usług świadczonych drogą elektroniczną, w tym np. portale społecznościowe i sprzedawców internetowych.

Jak operatorzy infrastruktury krytycznej powinni reagować na zagrożenia bezpieczeństwa cyfrowego?

Wciąż największym zagrożeniem dla bezpieczeństwa w sferze cybernetycznej jest

nieodpowiedzialna postawa pracowników, w tym ustawianie łatwych do złamania haseł. Być może stosunkowo prostym, ale efektywnym rozwiązaniem byłoby wprowadzenie zabezpieczeń biometrycznych (np. odciski palców)? Bardziej ofensywnym rozwiązaniem, mającym przeciwdziałać wykradaniu danych przez osoby „z wewnątrz”, jest tropienie anomalii w codziennych zachowaniach pracowników, których wykrycie mogłoby stanowić ostrzeżenie przed niebezpieczeństwem. Stawiający na pierwszym miejscu bezpieczeństwo nazwą to budowaniem systemu immunologicznego instytucji, obrońcy praw obywatelskich – niedopuszczalną inwigilacją.

Kolejnym wyzwaniem jest kwestia **dzielenia się przez firmy informacjami na temat zagrożeń płynących z cyberprzestrzeni – zarówno z instytucjami państwowymi, jak również między sobą**. Z powodu obaw przed stratami reputacyjnymi czy też negatywnym wpływem na kurs akcji, ale też nie chcąc dawać wskazówek odnośnie do słabszych elementów swoich systemów teleinformatycznych – **firmy niechętnie ujawniają informacje na ten temat, często bagatelizując skalę szkód**. Poważnym wyzwaniem jest więc przepływ informacji na temat rzeczywistych strat powodowanych przez cyberataki.

Wnioski i rekomendacje

Zarysowane dylematy posłużyły do dyskusji na temat cyberbezpieczeństwa infrastruktury krytycznej podczas tegorocznego Europejskiego Forum Nowych Idei w Sopocie. Z debaty – w której wzięli udział przedstawiciele administracji rządowej, prywatnych i państwowych operatorów infrastruktury krytycznej, a także firm informatycznych – wyłania się kilka kluczowych wniosków i rekomendacji:

1] Zapewnienie bezpieczeństwa infrastruktury krytycznej wymaga współpracy wielu podmiotów, w tym zarówno ze sfery państwowej, jak i prywatnej. Stąd rolą państwa powinno być zapewnienie przywództwa, ale próba wzięcia na siebie pełnej odpowiedzialności skazana jest na porażkę. Koordynacja i współpraca potrzebne są nie tylko na linii państwa – operatorzy infrastruktury krytycznej, lecz także wewnątrz poszczególnych sektorów, nie tylko na poziomie kraju, ale również międzynarodowym.
2] Poziom cyberbezpieczeństwa zależny jest od ogólnych kompetencji cyfrowych użytkowników. Oznacza to konieczność wprowadzania obowiązkowych procedur bezpieczeństwa,

które choć mają kluczowe znaczenie, spotykają się z oporem pracowników. Ważną kwestią jest także rozwijanie świadomości i kompetencji cyfrowych w społeczeństwach. Dostrzegają to instytucje europejskie – w obecnej perspektywie finansowej (na najbliższe 7 lat) na działania w tym zakresie przeznaczono 360 mln zł.

3] Kolejnym zadaniem dla twórców polityki zapewniania cyberbezpieczeństwa jest znalezienie balansu między wysokością nakładów a poziomem bezpieczeństwa. Biorąc pod uwagę wymienność tych dwóch wartości, dążenie do osiągnięcia 100 proc. bezpieczeństwa wymagałoby poniesienia nieskończonych nakładów finansowych. Z tego powodu tak ważne jest przeprowadzenie oceny zagrożenia (*risk assessment*). W ramach tej procedury należy odpowiedzieć na pytania o kluczowe punkty infrastruktury krytycznej, które państwo musi chronić, bieżącą sytuację geopolityczną, czynniki zwiększające zagrożenia, a także motywacje potencjalnych agresorów (ciekawość, zyski finansowe, interes narodowy).

4] W odniesieniu do cyberbezpieczeństwa infrastruktury krytycznej w Polsce pilnym zadaniem jest poprawa koordynacji działań instytucji i wyznaczenie jednej z nich jako wiodącej. Obecnie firmy składają raporty na temat incydentów w cyberprzestrzeni do trzech różnych podmiotów (Ministerstwa Administracji i Cyfryzacji, Urzędu Komunikacji Elektronicznej, Biura Bezpieczeństwa Narodowego), co rozmywa odpowiedzialność po stronie administracji publicznej i wprowadza dezorientację po stronie podmiotów prywatnych. Konieczne jest także zbudowanie mechanizmu wymiany danych i doświadczeń między podmiotami rządowymi i prywatnymi, w tym doprecyzowanie i standaryzacja form komunikacji.

Stopień zagrożenia i rozmiar potencjalnych szkód powinny skłaniać zainteresowane podmioty do szybkiego wdrażania rekomendacji przedstawianych przez ekspertów. O powadze kwestii cyberbezpieczeństwa, w tym infrastruktury krytycznej, świadczą wyniki badań Pew Research Center. Ośrodek ten zapytał ponad 1600 ekspertów, czy do 2025 roku przewidują potężny atak w cyberprzestrzeni, w wyniku którego może zginąć duża liczba ludzi lub który przyniesie straty materialne na poziomie dziesiątek miliardów dolarów. Ponad 60 proc. pytanych odpowiedziało twierdząco.

Opracował **Andrzej Turkowski**

CSM jest niezależnym, pozarządowym ośrodkiem analitycznym zajmującym się polską polityką zagraniczną i najważniejszymi problemami polityki międzynarodowej. Fundacja została zarejestrowana w 1996 r. CSM prowadzi działalność badawczą i edukacyjną, wydaje publikacje, organizuje konferencje i spotkania, uczestniczy w międzynarodowych projektach we współpracy z podobnymi instytucjami w wielu krajach. Tworzy forum debaty i wymiany idei w sprawach polityki zagranicznej, relacji między państwami oraz wyzwań globalnego świata. Działalność CSM jest adresowana przede wszystkim do samorządowców i przedsiębiorców, a także administracji centralnej, polityków, dyplomatów, politologów i mediów. Od 2009 r. CSM jest uznawany za jeden z najlepszych think tanków Europy Środkowo-Wschodniej w badaniu „The Leading Public Policy Research Organizations In The World" przeprowadzanym przez Uniwersytet Pensylwanii.

Centrum Stosunków Międzynarodowych ul. Mińska 25, 03-808 Warszawa t: +48 22 646 52 67
www.twitter.com/CIR_CSM www.facebook.com/CIR.CSM

CENTRUM
STOSUNKÓW
MIĘDZYNARODOWYCH