aut. Instytut Kościuszki 09.02.2018

CYBERSEC FORUM: MUSIMY ZWIĘKSZYĆ INWESTYCJE W CYBERBEZPIECZEŃSTWO

Musimy zwiększyć inwestycje w cyberbezpieczeństwo – to numer 1 na liście 9 najważniejszych wyzwań dla bezpieczeństwa cyfrowego w 2018 roku, podkreśla Instytut Kościuszki w rekomendacjach CYBERSEC Forum 2017. Raport jest podsumowaniem dwudniowych debat ponad 150 światowej klasy ekspertów biorących udział w III Europejskim Forum Cyberbezpieczeństwa, które odbyło się pod hasłem „Dealing with Cyber Disruption". Wydawana corocznie publikacja zawiera najważniejsze zalecenia dla rządów, organizacji międzynarodowych i sektora prywatnego w 4 obszarach: Państwo, Obrona, Przyszłość i Biznes.

1. Większe inwestycje w cyberbezpieczeństwo i rozsądny plan wykorzystania środków przeznaczonych na ten cel. Rządy muszą przejąć inicjatywę w tej kwestii, aby dobry przykład rezonował na inne sektory. Prawo zamówień publicznych powinno nakładać obowiązek spełnienia określonych wymogów przez producentów, dostawców usług i rozwiązań teleinformatycznych, by tworzone przez nich rozwiązania uwzględniały zasadę security and privacy by design budującą cyberbezpieczeństwo i prywatność danych w całym łańcuchu wartości (ze szczególnym uwzględnieniem urządzeń końcowych). Taka zmiana przyczyni się do zwiększenia bezpieczeństwa m.in. w obrębie Internetu Rzeczy (Internet of Things), w tym dynamicznie rozwijających się Inteligentnych Miast (Smart Cities), do których już dziś podłączone są miliardy urządzeń na całym świecie.

2. Specjalny system sankcji i zachęt do implementacji sektorowych standardów cyberbezpieczeństwa oraz dobre zaprojektowanie systemu certyfikacji produktów i usług IT i ICT. Szczególnie operatorzy infrastruktury krytycznej powinni być zobowiązani do implementowania standardów cyberbezpieczeństwa. Wdrażanie obowiązkowych, dostosowanych do potrzeb krajów, sektorów i organizacji, standardów powinno być połączone z systemem zachęt dla biznesu do ich implementowania.

3. Współpraca sektora prywatnego i państwa w zakresie budowania zdolności do działania w cyberprzestrzeni, m.in. w zakresie atrybucji cyberataków, czyli ustaleniu sprawstwa oraz zaprojektowania efektywnej polityki ujawniania luk (coordinated vulnerability disclosure) w zabezpieczeniach i aktualizacji urządzeń podłączonych do sieci.

4. Walka informacyjna prowadzona w cyberprzestrzeni na pierwszym planie zagrożeń dla demokracji. Zabezpieczenie wyborów przed „hakowaniem" powinno się odbywać poprzez:
– kompleksową ocenę ryzyka (która wykracza poza technologie),
– stworzenie odpowiednich warunków legislacyjnych (np. włączenie infrastruktury wyborczej do infrastruktury krytycznej) oraz technicznych (monitoring ruchu, weryfikacja zliczania głosów),
– tworzenie analogowych kopii zapasowych oddanych głosów,
– budowanie świadomości w zakresie zabezpieczenia systemów IT wśród kandydujących polityków.

5. Zwiększone cyberbezpieczeństwo NATO: kluczowe jest zapewnienie bezpieczeństwa operacji wojskowych i wzmocnienie cyberobrony państw członkowskich. Zdolności NATO do działania w cyberprzestrzeni powinny być rozwijane na poziomie doktrynalnym, politycznym i organizacyjnym. Priorytetowe kwestie w tym obszarze to:
– tworzenie silnego zaplecza kompetencyjnego poprzez różnego rodzaju szkolenia i ćwiczenia cywilno-wojskowe,
– wspieranie państw członkowskich w rozwoju narodowego potencjału,
– zwiększanie innowacyjności NATO, np. w zakresie zaawansowanej analizy danych opartej na algorytmach i uczeniu maszynowym.
Sojusz podjął szereg kroków w kierunku zwiększenia poziomu cyberbezpieczeństwa. Należy kłaść nacisk na kontynuację tych działań i rozwijanie ścisłej współpracy państw członkowskich, zwłaszcza w zakresie atrybucji oraz zdolności i narzędzi ofensywnych.

6. Sztuczna inteligencja (Artificial Intelligence, AI) jednocześnie szansą i wyzwaniem. Obawy związane z jej zastosowaniem rosnąć będą tym bardziej, w im większym stopniu zależeć od niej będzie ludzkie życie i im bardziej ta technologia wymykać się będzie spod ludzkiej kontroli. Wśród największych zagrożeń wyróżnić należy:
– brak dostatecznej transparentności i zagrożenie „stronniczością" algorytmów AI,
– ryzyko fałszowania procesu decyzyjnego AI poprzez ingerencję w dane wejściowe,
– wysoce prawdopodobne wykorzystanie AI do prowadzenia kampanii dezinformacyjnych.
AI może również okazać się szansą, zwłaszcza w kontekście deficytu wykwalifikowanych ekspertów bezpieczeństwa ICT. Zaleca się zatem wsparcie innowacji w tym zakresie i unikanie nadmiernych regulacji tej technologii.

7. Efektywny system cyberubezpieczeń powinien być wdrażany w kulturę bezpieczeństwa opartą o zarządzanie cyber ryzykiem oraz partnerstwo z klientami w zakresie budowania ich zdolności, świadomości, organizacji i procedur. Cyberubezpieczenia, które odegrają ważną rolę w kontekście ustanowienia właściwych standardów cyberbezpieczeństwa oraz będą jedną z ekonomicznych zachęt do przemian sektora biznesu (komplementarną do proponowanych zmian w zamówieniach publicznych), powinny:
– być dostosowane do specyfiki danego podmiotu (zwłaszcza podmiotów z sektora infrastruktury krytycznej),
– opierać się na faktycznej ocenie ryzyka, uwzględniającej kompleksowy wgląd w organizację i jej uwarunkowania (wewnętrzne i zewnętrzne).

8. Dalszy rozwój bezpieczeństwa w sektorze biznesu:
– kompleksowe podejście do architektury sieci wewnętrznej i połączeń zewnętrznych,
– edukację użytkowników sieci IT w zakresie ryzyk i zagrożeń w sieci, Security Operations Center (SOC) z Security Information Management (SIM),
– analityką i gromadzeniem danych o zagrożeniach (SOC umożliwia przygotowanie się, wykrycie i kompleksową odpowiedź na atak),
– audyt procedur i bezpieczeństwa,
– budowanie zdolności atrybucyjnych,
– zabezpieczenie przed wewnętrznym zagrożeniem ze strony pracowników (insider threats) poprzez wdrażanie rozwiązań (przy zachowaniu zasad prywatności) bazujących na analityce zachowań i profilowaniu,
– implementacja rozwiązań chmurowych (może przynieść wiele pozytywnych efektów zwłaszcza w sektorze zdrowia).

9. Budowanie regionalnych centrów kompetencji oparte na silnej i efektywnej współpracy pomiędzy różnymi uczestnikami ekosystemu. Kluczowe w tym kontekście:
– rządowe wsparcie regionalnych projektów o największym potencjale edukacyjnym i innowacyjnym

poprzez odpowiednie fundusze,
– ścisła współpraca w skali globalnej – na przykład poprzez Globalną Platformę Innowacji dla Cyberbezpieczeństwa (Global EPIC), która została zainicjowana podczas CYBERSEC Forum 2017. Porozumienie podpisało 14 regionalnych centrów innowacji z 10 krajów, w tym jeden z Polski – CYBERSEC HUB prowadzony przez Instytut Kościuszki.

Rekomendacje zostaną przedyskutowane z najważniejszymi decydentami politycznymi, przedstawicielami sektora biznesu i środowisk eksperckich podczas brukselskiego podsumowania konferencji, które odbędzie się już 27 lutego 2018 r., pt. „Dealing with cyber disruption – Brussels leaders' foresight".

Pełna treść publikacji: Rekomendacje CYBERSEC 2017

Informacja: Instytut Kościuszki