aut. Adam Lelonek 12.10.2017

GEN. NOWAK: „CYBERBEZPIECZEŃSTWO W BIZNESIE TO KONIECZNOŚĆ, A NIE OPCJA” (CYBERSEC 2017)

10 października w Krakowie podczas III Europejskiego Forum Cyberbezpieczeństwa – CYBERSEC 2017 wystąpił Włodzimierz Nowak, generał w stanie spoczynku, członek zarządu ds. Prawnych, Bezpieczeństwa i Zarządzania Zgodnością T-Mobile Polska S.A. Tytuł jego wystąpienia to „Cyberbezpieczeństwo w biznesie to konieczność, a nie opcja”.

Infrastruktura krytyczna jest całkiem dobrze uregulowana prawnie, lecz inne obszary nie. W związku z tym potrzeba więcej działań w systemie cyberbezpieczeństwa. Można albo redukować liczbę strat finansowych lub inwestować w zabezpieczenia. Kiedy większość ludzi nie przestrzega reguł, wzrasta liczba płaszczyzn do ataku, to też ważna informacja dla biznesu. Co więcej, jak mówił ekspert, kluczowa jest osobista odpowiedzialność za bezpieczeństwo – jeżeli sami o nie nie zadbamy, to jesteśmy podatni na atak. Trzeba zdiagnozować swoje słabe punkty.

W opinii generała cyberprzestrzeń jest złożona, a wszystko co jest w niej dostępne musi być zabezpieczone. Do celów cyberataków zaliczył on:

- zatrzymanie przepływu informacji,
- zakłócenie przepływu informacji,
- modyfikację informacji,
- kradzieże danych lub informacji,
- dyskredytacja osób (w tym przedstawicieli rządu, biznesu, osób publicznych, itd).

51% firm zostało ofiarami cyberataków, 93% dużych przedsiębiorstw zostało zaatakowanych tylko w 2016 roku. Jak poinformował ekspert, straty z tym związane szacowane są łącznie na 200 mld euro w Europie, a w skali świata na 450 mld euro. Jak mówił Nowak, w 2017 r. straty związane z atakami cybernetycznymi szacowana jest na ok. 7 mld euro. Obecnie mają one odpowiednie proporcje:

- infrastruktura krytyczna - 10%,
- biznes - 20%,
- indywidualni użytkownicy - 60%,
- Internet Rzeczy (IoT) - 10%.

Ekspert zaznaczył jednak, że będzie ona ewoluować. Według szacunków, wysokość strat spowodowanych przez ataki osiągnie poziom 50 mln euro rocznie, a ich cele również się zmienią:

- infrastruktura krytyczna - 10%,
- biznes - 10%,
- indywidualni użytkownicy - 30%,
- Internet Rzeczy (IoT) - 50%.

Nie da się indywidualnie zapewnić bezpieczeństwa w cyberprzestrzeni. Potrzebne są ponadnarodowe i krajowe regulacje, porozumienia firm telekomunikacyjnych, współpraca międzysektorowa, zwiększanie odpowiedzialności instytucjonalnej i indywidualnych podmiotów (rządy, firmy, itp.), a wreszcie indywidualna odpowiedzialność każdego użytkownika.

Odpowiedzialność w cyberprzestreni ma dwa poziomy: regulacje narodowe oraz państwowy system cyberobrony. W skład tego pierwszego wchodzą: infrastruktura krytyczna, ministerstwa, służby specjalne oraz inne podmioty państwowe. Do drugiego zaliczyć można: kwestie organizacyjne, edukację, świadomość i rozwój.

Niezwykle istotne jest, aby firmy telekomunikacyjne i dostawcy usług dążyli do wprowadzania porównywalnych poziomów bezpieczeństwa i współpracowali ze sobą. W ocenie eksperta reagowanie i podnoszenie zabezpieczeń tylko przez część podmiotów lub grupy dostawców, a nie wszystkich sprawia, iż taka selektywna odpowiedź nie jest realnie skuteczna. Podobnie w biznesie czy we współpracy międzynarodowej – należy myśleć o innych użytkownikach i podmiotach oraz dążyć do podnoszenia standardów i wspólnego dbania o bezpieczeństwo.

Dla zobrazowania tego ekspert podał konkretny przykład: „Czy są jakieś mechanizmy bezpieczeństwa w telewizorze? Nie. Czy podłącza się telewizor do Internetu? Tak. Czy jest to problemem? Tak. To jest działanie dla inżynierów, trzeba zmienić podejście do projektowania i produkowania sprzętu. Telewizor może obserwować nas. Trzeba przyjrzeć się architekturze, nie możemy się koncentrować wyłącznie na poziomie aplikacji”.

Punktem wyjścia jest przeanalizowanie architektury wewnętrznych sieci oraz zewnętrznych połączeń. Nowak przedstawił to z wykorzystaniem tzw. „Helicopter View” – grafiki obrazującej skąd pochodzi największy ruch, gdzie jest najwięcej powiązań. Dalej praca z Modelem OSI (Open Systems Interconnection model) czyli łączeniem systemów otwartych i ich standaryzacją, a w dalszej kolejności zarządzanie incydentami w matrixie cyberbezpieczeństwa: wykrycie, reakcja, naprawa, ochrona. Sam matrix składa się zarówno z ludzi, jak i procedur czy technologii.

Zdaniem Nowaka problemy związane z cyberbezpieczeństwem będą istnieć tak długo jak:

- ludzie nie będą poinformowani i świadomi zagrożeń,

- dzieci nie będą uczone w szkołach o dobrych praktykach i jak zachowywać się w sieci,
- inżynierowie będą produkować urządzenia, w tym IoT, z myślą jedynie o funkcjonalności,
- twórcy sieci będą myśleć jedynie o efektywności i parametrach,
- menadżerowie odpowiadający za bezpieczeństwo będą rozwiązywać problemy jedynie z wykorzystaniem technologii.

Ekspert zalecił również, aby „nie próbować bronić obecnego status quo, gdyż nic nie trwa wiecznie. Początkowym etapem w aspekcie bezpieczeństwa jest kompleksowa analiza, nie można omijać aspektów sieci globalnej, modelu OSI, matrixu cyberbezpieczeństwa oraz cyklu życia systemu. Należy próbować powstrzymywać ataki tak wcześnie i na tak dużej odległości jak to możliwe. Trzeba zmienić wszystko w taki sposób, aby można było być bardziej bezpiecznym”.