https://www.bbn.gov.pl/pl/wydarzenia/6378,Szef-BBN-dla-Polski-Zbrojnej-Wirtualny-atak-jest-realny.html
19.04.2024, 21:05
29.01.2015

Szef BBN dla Polski Zbrojnej: Wirtualny atak jest realny

- Zagrożenia w przestrzeni wirtualnej są podobne do tych w geoprzestrzeni. Jeśli w realnym świecie wzrasta pospolita przestępczość, musimy być świadomi, że w cyberprzestrzeni złodzieje mogą kraść nasze dane czy pieniądze – mówił szef BBN minister Stanisław Koziej w rozmowie z red. Łukaszem Zalesińskim z Polski Zbrojnej. Zapraszamy do zapoznania się z rozmową.

Wyobraźmy sobie taką sytuację: atakuje nas nieprzyjaciel, wojna rozwija się w najlepsze, jednak przeciętny człowiek nawet nie wie, że ona trwa. Toczy się bowiem w przestrzeni wirtualnej. Realne?

Szef BBN Stanisław Koziej: W tej chwili raczej trudno wyobrazić sobie cyberwojnę na skalę tak dużą, że konieczne byłoby na przykład zaangażowanie naszych sojuszników z NATO. Z pewnością jednak wirtualny atak na elementy infrastruktury krytycznej i instytucje, czy to państwowe, czy prywatne, jest jak najbardziej realny. Przecież na świecie do takich sytuacji dochodzi.

I przed tym właśnie ma nas chronić spójna doktryna cyberbezpieczeństwa? Biuro Bezpieczeństwa Narodowego właśnie przygotowało poświęcony jej dokument…

„Doktryna Cyberbezpieczeństwa" nie jest dokumentem operacyjnym. Nie wskazuje konkretnych sposobów obrony przed atakiem cyfrowym. Naszą intencją było raczej stworzenie swego rodzaju wspólnej platformy porozumienia co do cyberbezpieczeństwa dla instytucji państwowych, ale też prywatnych. Każda z nich buduje swoją strategię radzenia sobie z tego typu zagrożeniami – począwszy od rządu, wojska, przez służby specjalne, instytucje publiczne, prywatne firmy, a skończywszy na pojedynczych obywatelach, którzy przecież zabezpieczają własne komputery przed włamaniem czy kradzieżą danych.

Mówiąc obrazowo – cyfrowa mapa Polski pełna jest wysp, które dbają o swoje bezpieczeństwo w wirtualnej przestrzeni. Nam zależy, by te wyspy scalić w jeden kontynent. Wypracować wspólny katalog zasad, według których można by postępować, tak aby działać najbardziej efektywnie. Przy czym na poziomie doktryny nie dajemy oczywiście gotowych recept. Wskazujemy na filozofię zwalczania zagrożeń, które mogą przyjść z bardzo różnych kierunków.

No właśnie – z jakich konkretnie?

Można powiedzieć, że zagrożenia w przestrzeni wirtualnej stanowią dokładną analogię zagrożeń w geoprzestrzeni. Można je tak samo podzielić na wewnętrzne i płynące z zewnątrz. Jeśli w realnym świecie rośnie zagrożenie pospolitą przestępczością, musimy być świadomi, że złodzieje mają teraz w cyberprzestrzeni możliwość kradzieży naszych danych czy pieniędzy. Gdy zwracamy uwagę na problem wynikający z różnego rodzaju ulicznych demonstracji, protestów społecznych, okupowania budynków użyteczności publicznej, musimy być gotowi na przykład na blokowanie rządowych stron internetowych. Przykłady można by mnożyć.

Jakie rozwiązania proponują twórcy doktryny?

Ważną sprawą jest samo uświadomienie sobie zagrożeń. Należy też stale monitorować sytuację w otaczającym nas świecie i uwzględniać w strategiach działania potencjalne zagrożenia. Przykład: każdy samorząd zobowiązany jest przygotować plan działania na wypadek wojny, ataku terrorystycznego czy niepokojów społecznych. Teraz powinien też uwzględniać zagrożenia w cyberprzestrzeni.

Doktryna mówi także o konieczności odpowiedniego przygotowania osób odpowiedzialnych za wirtualne bezpieczeństwo na różnych poziomach. Podpowiada, jakie kierunki powinny być w takich szkoleniach uwzględniane. Wskazujemy na potrzebę stworzenia odpowiedniej polityki kadrowej, kształcenia fachowców od bezpieczeństwa cybernetycznego na wyższych uczelniach, ale też wyławiania i włączania do systemu obywateli, którzy chcieliby się zaangażować w jego tworzenie i funkcjonowanie.

Z jakich narzędzi przy tym korzystać?

W doktrynie mówimy o konieczności rozwoju kryptologii i kryptografii, tworzeniu systemów służących do tajnej łączności, o zapewnianiu sobie pełnej kontroli nad kupowanym za granicą uzbrojeniem. Chodzi tutaj o dostęp do kodów źródłowych, tak by mieć pewność, że to my, a nie producent, w pełni panujemy nad tym sprzętem.

W dokumencie skazujemy również konieczność współpracy publiczno-prywatnej. Kraj może zostać zdestabilizowany także przez uderzenie w prywatne firmy czy koncerny. Dlatego do dbania o jego bezpieczeństwo musimy poczuwać się wszyscy.

***

Źrdódło: [polska-zbrojna.pl]
