https://www.bbn.gov.pl/pl/wydarzenia/4708,Szef-BBN-dla-PAP-Strategia-bezpieczenstwa-musi-uwzgledniac-cyber przestrzen.html
04.03.2024, 06:30

25.06.2013

Szef BBN dla PAP: Strategia bezpieczeństwa musi uwzględniać cyberprzestrzeń

Komentarz szefa BBN ministra Stanisława Kozieja na temat fałszywych alarmów bombowych, ogłoszonych 25 czerwca br.

***

Seria fałszywych alarmów bombowych pokazała, jak ważna stała się cyberprzestrzeń i że trzeba ją uwzględnić w strategii bezpieczeństwa narodowego – powiedział PAP we wtorek szef BBN Stanisław Koziej.

„Moim zdaniem dzisiejsze wydarzenia w spektakularny sposób pokazały, jak ważna staje się cyberprzestrzeń i jak uzależnieni jesteśmy od tego, co się w niej dzieje. Jednocześnie widać, jak jest delikatna, wrażliwa i podatna na zakłócenia, jak łatwo w niej dokonać prowokacji, przestępstwa. Stąd wniosek, że musimy uczyć się ją lepiej rozumieć, organizować się w niej, ubezpieczać” – powiedział Koziej PAP.

„To był odpowiednik nieodpowiedzialnych, głupich zachowań, jak rzucenie kamieniem czy sianie paniki w tłumie. Cyberprzestrzeń potęguje tego typu zachowania” – ocenił wtorkowe zdarzenia.

„Musimy pilnie zbudować fundamenty cyberbezpieczeństwa, by w sposób skoordynowany i bezpieczny reagować na ryzyka. Na szczęście ten alarm okazał się fałszywy, ale pokazał, co mogłoby się dziać, gdyby ktoś chciał nie tylko przesłać fałszywą wiadomość, ale np. spowodować jakąś awarię. To klarowny sygnał, że trzeba te zagrożenia traktować poważnie” – podkreślił.

Przypomniał, że bezpieczeństwo cybernetyczne jest w ocenie BBN jedną z najważniejszych dziedzin współczesnego bezpieczeństwa. „Uważamy, że potrzebna jest strategia cyberbezpieczeństwa, która będzie wskazywała priorytety, główne reguły, zasady. To nie mogą być dzikie pola pozostawione same sobie. Trudność tego zagospodarowania polega i na tym, że w cyberprzestrzeni nie ma tradycyjnej administracji, ministra, resortów; potrzebne jest myślenie i działanie ogólne, strategiczne ” – dodał. Zaznaczył, że wraz z pracami nad strategią bezpieczeństwa systemów przekazywania informacji trzeba prowadzić działania operacyjne i chronić systemy informatyczne przed zakłóceniami i włamaniami.

Szef BBN zwrócił uwagę, że system zarządzania kryzysowego w geoprzestrzeni jest dostosowany do reagowania na fizyczne zdarzenia, katastrofy, klęski żywiołowe, natomiast zagrożenia cybernetyczne są niewidoczne, trudne do szybkiej interpretacji i konieczny jest inny system reagowania niż na normalne katastrofy i zdarzenia, uwzględniający jednak styk świata fizycznego i cyberprzestrzeni.

Przypomniał, że na problemy bezpieczeństwa cybernetycznego zwrócili uwagę autorzy Strategicznego Przeglądu Bezpieczeństwa Narodowego. „Konsekwencje wysyłania informacji, dezinformacji, niejasnych sprzecznych

informacji na reagowanie kryzysowe jest ogromny”. Podkreślił, że problemy cyberbezpieczeństwa trzeba uwzględnić w nowej strategii bezpieczeństwa narodowego, którą w tym roku wyda prezydent na wniosek rządu.

Po fałszywych alarmach bombowych w kraju sprawdzono we wtorek 22 obiekty użyteczności publicznej – szpitale, sądy, budynki prokuratury i policji, a także centra handlowe. Ponad 2700 osób musiało opuścić budynki. Fałszywe ostrzeżenia wysyłano z serwerów w kraju i za granicą. Po południu zatrzymano pierwszego podejrzewanego w sprawie.

Źródło: PAP
