STREŻYŃSKA: POLSKA INFRASTRUKTURA KRYTYCZNA ATAKOWANA PRZEZ HAKERÓW

Na instytucje finansowe oraz infrastrukturę krytyczną w Polsce przypuszczane są ataki hakerskie spoza naszego kraju; eksperci potrafią na nie dobrze reagować, usprawnienia wymaga ich przewidywanie - oceniła w poniedziałek minister cyfryzacji Anna Streżyńska.

"Są oczywiście ataki spoza Polski, jak najbardziej, hakerskie. (...) Wiadomo, jakie są najczulsze punkty rzeczywistości teleinformatycznej - to są z reguły instytucje finansowe oraz infrastruktura krytyczna, czyli ta, na której tkanka państwa się rozpina - transportowa czy paliwowa, czy energetyczna i takie ataki są przypuszczane" - powiedziała minister w porannej audycji Radia Zet, pytana o cyberataki spoza Polski.

Jak dodała, ministerstwo cyfryzacji obserwuje kierunek ataków, a nie ich źródło. "Widać kierunek, można się spodziewać inspiracji po tych kierunkach, ale trudno jest to stwierdzić z całą pewnością, bo takimi rzeczami zajmują się raczej agencje wywiadu niż ministerstwo cyfryzacji" - powiedziała. Minister była pytana o swoje stwierdzenia z połowy października, że koszt najpilniejszych wydatków związanych z cyberbezpieczeństwem w 2017 r. szacuje się na 60 mln zł, ale środki te nie zostały jeszcze w całości zagwarantowane na przyszły rok. Pytanie dotyczyło tego, co jest lepsze - wydanie milionów na cyberbezpieczeństwo czy miliardów na Wojska Obrony Terytorialnej.

"Obrona terytorialna jest bardzo ważna, ale jest dość dobrze finansowana przez państwo. Natomiast to, do czego my próbujemy doprowadzić to, żeby infrastruktury teleinformatyczne były bardziej bezpieczne" - powiedziała. Minister cyfryzacji podkreśliła, że Polska bardzo dobrze wypada w międzynarodowych ocenach bezpieczeństwa. "Zawsze jest mowa, że jesteśmy doskonali, jeśli chodzi o odparcie ataku, jeśli on się odbędzie; gorzej jest z przewidywaniem jego kierunku i samego ataku, czasem bywamy zaskoczeni, ale nasi analitycy są coraz lepsi w przewidywaniu również" - wskazała.

W połowie października Streżyńska informowała, że w połowie listopada rząd powinien przyjąć "Strategię Cyberbezpieczeństwa RP na lata 2016–2020". Jej celem jest m.in. zwiększenie poziomu bezpieczeństwa infrastruktury teleinformatycznej państwa, zwiększenie zdolności do zapobiegania i zwalczania zagrożeń ze strony cyberprzestrzeni, a także zmniejszenie skutków incydentów godzących w bezpieczeństwo cyberprzestrzeni.

Zgodnie z zapowiedziami minister, w kwietniu przyszłego roku do Sejmu trafi projekt ustawy o krajowym systemie cyberbezpieczeństwa. Rząd ma się nim zająć w marcu 2017 r. MC chce, by w projekcie ustawy o krajowym systemie cyberbezpieczeństwa znalazły się elementy wymagane przez dyrektywę NIS (dyrektywa PE o bezpieczeństwie sieci i informacji). W ustawie mają znaleźć się także zasady zarządzania istotnymi incydentami teleinformatycznymi. Resort chce też zapisać m.in. zasady tworzenia "efektywnych programów edukacyjnych".

W lipcu Parlament Europejski przyjął dyrektywę o bezpieczeństwie sieci i informacji (NIS), która

zawiera listę tzw. krytycznych sektorów. Przedsiębiorstwa i administracja publiczna w tych sektorach będą mieć obowiązek oceny zagrożeń dla bezpieczeństwa sieci teleinformatycznych, przeciwdziałania im oraz zgłaszania poważnych incydentów. Lista obejmuje energetykę, transport, bankowość, infrastrukturę rynków finansowych (np. giełdy papierów wartościowych), służbę zdrowia, wodociągi oraz infrastrukturę cyfrową.

Władze państw unijnych mają ustalić szczegółową listę "operatorów kluczowych usług", biorąc pod uwagę znaczenie tych usług dla społeczeństwa i gospodarki czy bezpieczeństwa publicznego. Podmioty z tej listy będą objęte wymogami dyrektywy dotyczącymi zapewnienia bezpieczeństwa swych sieci informatycznych.

Państwa unijne będą musiały powołać instytucje ds. bezpieczeństwa sieci telekomunikacyjnych, które będą nadzorować wypełnianie dyrektywy, oraz zespoły reagowania na incydenty komputerowe (Computer Security Incident Response Teams - CSIRTs). Państwa mają też przyjąć własne strategie i plany współpracy w zakresie bezpieczeństwa sieci telekomunikacyjnych i informacji. Powstanie unijna sieć zespołów reagowania na incydenty komputerowe, której sekretariat będzie mieścić się przy Europejskiej Agencji Bezpieczeństwa Sieci i Informacji (ENISA).

Czytaj też: MC: w kwietniu do Sejmu trafi projekt ustawy o cyberbezpieczeństwie