MC: W KWIETNIU DO SEJMU TRAFI PROJEKT USTAWY O CYBERBEZPIECZEŃSTWIE

W kwietniu przyszłego roku do Sejmu trafi projekt ustawy o krajowym systemie cyberbezpieczeństwa - poinformowała w środę w Sejmie minister cyfryzacji Anna Streżyńska. Jak dodała, projektem ustawy rząd zajmie się w marcu 2017 r.

Posłowie Komisji Cyfryzacji, Innowacyjności i Nowoczesnych Technologii wysłuchali w środę informacji o pracach nad rządowym projektem ustawy o krajowym systemie cyberbezpieczeństwa, będącej wdrożeniem dyrektywy NIS oraz informacji o Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2016-2020.

-Jeśli chodzi o projekt ustawy (o krajowym systemie cyberbezpieczeństwa) to trafi on do Sejmu w kwietniu przyszłego roku. Przewidujemy w marcu skierować go na posiedzenie Rady Ministrów(...) przy zachowaniu wszystkich pozytywnych wiatrów - powiedziała Streżyńska.

Włodzimierz Nowak z Departamentu Cyberbezpieczeństwa Ministerstwa Cyfryzacji poinformował, że w sprawie stanu zabezpieczeń państwowych systemów teleinformatycznych, resort przekazał premier Beacie Szydło niejawną notatkę. - Skala problemu jest tutaj na tyle wysoka, że Ministerstwo Cyfryzacji musiało nawet napisać do pani premier niejawną notatkę opisującą stan faktyczny tych rejestrów, w jaki sposób są zabezpieczone - a raczej, w jaki sposób nie są zabezpieczone - powiedział Nowak.

Jak wskazał podstawą projektu ustawy jest strategia cyberbezpieczeństwa, nad którą pracuje obecnie resort. Celem "Strategii Cyberbezpieczeństwa RP na lata 2016–2020" 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.

"... w listopadzie chcielibyśmy przeprowadzić strategię przez wszystkie szczeble uzgodnień(...), tak żeby koniec listopada, początek grudnia strategia znalazła się w Radzie Ministrów. Nie można opóźniać wdrożenia tej strategii, sytuacja jest obecnie na tyle zła,(...)że należy jak najszybciej wiele rzeczy - na zasadzie gaszenia pożaru - poprawić" - powiedział Nowak.

- Wdrożenie strategii pomoże nam uzupełnić te braki, które są w wielu systemach i pozwoli przyjąć pewne założenia na przyszłość - dodał. Zaznaczył, że strategia nie jest czymś, co jest "dane raz na zawsze" można ją modyfikować".

Nowak powiedział, że w projekcie ustawy o krajowym systemie cyberbezpieczeństwa znajdą się elementy wymagane przez dyrektywę NIS(dyrektywa PE o bezpieczeństwie sieci i informacji). W ustawie mają znaleźć się także zasady zarządzania istotnymi incydentami teleinformatycznymi. - Ponieważ dzisiaj te zasady nie są jednoznaczne i nie wszystkie służby, nie wszystkie sektory działają w sposób jednoznaczny, a powinny działać - dodał.

Resort chce też zapisać w ustawie zasady tworzenia "efektywnych programów edukacyjnych". - Począwszy od szkolenia akademickiego, kursów dla menedżerów, szkolenia na poziomie podstawowym dla obywateli i dla dzieci w wieku szkolnym. Jak również zasady uczestnictwa ośrodków naukowych w pracach badawczo-rozwojowych i w rozwiązywaniu problemów istotnych z punktu widzenia cyberbezpieczeństwa - powiedział Nowak.

Poinformował, że resort powołał grupę pracującą nad ustawą o krajowym systemie cyberbezpieczeństwa. - Ta grupa prawie od dwóch miesięcy już pracuje. Odbyły się spotkania z przedstawicielami sektorów, przewidziane są kolejne kroki, spotkania z przedstawicielami służb państwowych - dodał.

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: Streżyńska: Rząd przyjmie Strategię Cyberbezpieczeństwa w połowie listopada