SENAT: BEZ POPRAWEK DO USTAWY O KRAJOWYM SYSTEMIE CYBERBEZPIECZEŃSTWA

Powstanie Krajowego Systemu Cyberbezpieczeństwa (KSC), który będzie zapobiegał, wykrywał oraz minimalizował skutki ataków naruszających bezpieczeństwo informatyczne kraju - to cel ustawy o KSC, którą w piątek bez poprawek przegłosował Senat. Teraz nowe przepisy trafią do prezydenta.

Za ustawą głosowało 71 senatorów, nikt nie był przeciw. Ośmiu senatorów wstrzymało się od głosu. Autorem projektu jest Ministerstwo Cyfryzacji.

Przepisy wdrażają dyrektywę Unii Europejskiej. Dyrektywa ta zobowiązuje państwa UE do przyjęcia krajowych strategii cyberbezpieczeństwa, do wskazania lub ustanowienia organów właściwych do spraw cyberbezpieczeństwa oraz powołania tzw. zespołów reagowania na incydenty komputerowe (CSIRT). Dyrektywa zobowiązuje też do zapewnienia cyberbezpieczeństwa systemów informacyjnych w sektorach usług tzw. kluczowych - m.in. w energetyce, transporcie, bankowości czy ochronie zdrowia.

Już w połowie kwietnia wiceminister cyfryzacji Karol Okoński dał do zrozumienia, że terminu wdrożenia dyrektywy, wyznaczony na 9 maja, nie da się dotrzymać. Według kwietniowej wypowiedzi wiceministra, przy optymistycznym założeniu podpis prezydenta pod ustawą mógłby zostać złożony w połowie czerwca.

Podczas prac sejmowych Komisji Cyfryzacji, Innowacyjności i Nowoczesnych Technologii oraz Komisji Obrony Narodowej wprowadzono kilka zmian do ustawy. Dodano n.in. nowe uprawnienia dla Agencji Bezpieczeństwa Wewnętrznego dot. koordynowania systemu wczesnego ostrzegania o zagrożeniach występujących w Internecie.

Sejm zaakceptował też poprawki dotyczące m.in. zwiększenia budżetu dla ABW w związku z nadaniem tej instytucji dodatkowych obowiązków.

Dzięki proponowanym zmianom w prawie, działania w skali kraju, które mają na celu zapobieganie atakom cybernetycznym, zostaną skoordynowane.

Celem ustawy jest organizacja oraz określenie sposobu funkcjonowania krajowego systemu cyberbezpieczeństwa (KSC). W przepisach wskazano sektory gospodarki narodowej, dla których zastosowanie będą miały przepisy ustawy oraz określono, kim są dostawcy usług cyfrowych oraz operatorzy usług kluczowych, z punktu widzenia cyberbezpieczeństwa.

Zarówno operatorzy usług kluczowych, jak i same usługi zostaną określone w drodze rozporządzenia Ministra Cyfryzacji. Obecnie projekt takiego rozporządzenia znajduje się w konsultacjach publicznych. Przedsiębiorstwa, które będą nosić miano operatorów usług kluczowych, będą wyłaniani w drodze decyzji administracyjnych. Według szacunków MC zostanie wyznaczonych ok. 335 operatorów usług

kluczowych.

Operatorzy będą zobowiązani do wdrożenia systemu zarządzania cyberbezpieczeństwem. Będą musieli systematycznie szacować ryzyka wystąpienia incydentu, który może mieć wpływ na cyberbezpieczeństwo. Ich zadaniem będzie też zbieranie informacji o zagrożeniach cyberbezpieczeństwa oraz stosowanie środków im zapobiegających. Będą także zobowiązani do prowadzenia odpowiedniej dokumentacji, którą w drodze rozporządzenia określi Rada Ministrów.

Zadaniem operatora będzie obsługa i sklasyfikowanie występującego incydentu. W ciągu 24 godzin od momentu wykrycia incydentu operator będzie miał obowiązek zgłoszenia go do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV. CSIRT MON prowadzony jest przez ministra obrony narodowej, CSIRT NASK prowadzi Naukowa i Akademicka Sień Komputerowa, a CSIRT GOV - szef Agencji Bezpieczeństwa Wewnętrznego. Są to zespoły reagowania na incydenty bezpieczeństwa komputerowego, działające na poziomie krajowym. Przekazują one sobie informacje dotyczące m.in. operatorów czy incydentów.

CSIRT-y wraz z Rządowym Centrum Bezpieczeństwa będą tworzyć Zespół ds. Incydentów Krytycznych, którego zadaniem będzie obsługa incydentów, które wykraczają poza kompetencje jednego CSIRT-u.

Z kolei dostawcy usług cyfrowych będą odpowiedzialni za zapewnienie bezpieczeństwa świadczonych przez nich usług. Będą musieli określić i podejmować odpowiednie środki techniczne w celu zarządzania ryzykami. Proponowane przepisy nakładają na nich także obowiązek podjęcia odpowiednich środków zapobiegających i minimalizujących wpływ zaistniałych incydentów.

Dostawcy usług cyfrowych będą powiadamiać o istotnych incydentach odpowiednie CSIRT-y, również o tych transgranicznych. Przewiduje się także, iż za niedopełnienie swoich obowiązków zarówno operatorzy usług kluczowych, jak i dostawcy usług cyfrowych poniosą kary.

Przepisy określają też kompetencje poszczególnych ministrów w zakresie cyberbezpieczeństwa. Przykładowo minister właściwy ds. informatyzacji odpowiedzialny będzie za opracowanie Strategii Cyberbezpieczeństwa, informowanie na temat krajowego systemu, sprawozdawczość wobec instytucji unijnych oraz uruchomienie z początkiem 2021 r. systemu teleinformatycznego, umożliwiającego zautomatyzowane zgłaszanie i obsługę incydentów, szacowanie ryzyka teleinformatycznego oraz ostrzeganie o zagrożeniach. Przewiduje się też, że premier powoła pełnomocnika ds. cyberbezpieczeństwa, do zadań którego będzie należało koordynowanie i realizowanie polityki rządu w zakresie zapewnienia cyberbezpieczeństwa kraju.

Ustawa ma wejść w życie 14 dni po ogłoszeniu w Dzienniku Ustaw.

MK/PAP