Krajowy System Cyberbezpieczeństwa – ustawa podpisana

Kategoria: Aktualności
Opublikowano: środa, 08, sierpień 2018 15:03
Alicja Cisowska
Odsłony: 1076

1 sierpnia 2018 roku Prezydent podpisał ustawę o krajowym systemie cyberbezpieczeństwa. Celem ustawy jest wykrywanie, zapobieganie i minimalizowanie skutków ataków naruszających bezpieczeństwo informatyczne kraju.

Nowe prawo wejdzie w życie po upływie 14 dni od dnia ogłoszenia.

Ustawa wdraża dyrektywę NIS i utworzy w Polsce krajowy system cyberbezpieczeństwa, w którego skład wejdą m.in. administracja rządowa i samorządowa oraz najwięksi przedsiębiorcy z wybranych sektorów gospodarki.

Ustawa nakłada obowiązki na operatorów usług, które mają kluczowe znaczenie dla utrzymania krytycznej działalności społecznej lub gospodarczej. Wśród operatorów znajdą się największe banki, firmy z sektora energetycznego, przewoźnicy lotniczy i kolejowi, armatorzy, szpitale i podmioty tworzące w Polsce infrastrukturę cyfrową.

Operatorzy usług kluczowych będą zobowiązani do wdrożenia skutecznych zabezpieczeń, szacowania ryzyka związanego z cyberbezpieczeństwem oraz przekazywania informacji o poważnych incydentach i ich obsługi we współpracy z jednym z trzech CSIRT (Zespołów Reagowania na Incydenty Bezpieczeństwa Komputerowego). Podmioty te będą zobowiązane do wyznaczenia osoby odpowiedzialnej za cyberbezpieczeństwo świadczonych usług, obsługi i zgłaszania incydentów oraz udostępniania wiedzy na temat cyberbezpieczeństwa.

Dostawcy usług cyfrowych, czyli internetowe platformy handlowe, usługi przetwarzania w chmurze i wyszukiwarki internetowe również zostaną objęte wymaganiami z zakresu cyberbezpieczeństwa. Z racji międzynarodowej specyfiki tych podmiotów, obowiązki dla dostawców usług cyfrowych będą objęte zharmonizowanym na poziomie UE reżimem regulacyjnym.

Cyberbezpieczeństwo dotyka wielu aspektów, zagrożeń zarówno cywilnych jak i wojskowych, potrzeby zaangażowania różnych organów administracji rządowej i służb. W związku z tym ustawa przewiduje różnorodne rozwiązania, określa zadania i wskazuje podmioty odpowiedzialne za ich realizację.

Do krajowego systemu cyberbezpieczeństwa, poza operatorami, będą włączone organy administracji publicznej, a także przedsiębiorcy telekomunikacyjni – w sposób zharmonizowany z istniejącymi uregulowaniami w tym zakresie.

System zarządzania cyberbezpieczeństwem w Polsce obejmie Zespół ds. Obsługi Incydentów Krytycznych, Pełnomocnik Rządu ds. Cyberbezpieczeństwa oraz Kolegium ds. Cyberbezpieczeństwa.

Ustawa wskazuje organy właściwe ds. cyberbezpieczeństwa odpowiedzialne za sprawowanie nadzoru wobec operatorów usług kluczowych i usług cyfrowych. Każdemu sektorowi określonemu w załączniku został przydzielony organ właściwy, zgodnie z działami administracji rządowej.

Zostanie utworzony również pojedynczy punktu kontaktowy ds. cyberbezpieczeństwa, prowadzony przez ministra właściwego do spraw informatyzacji, który ma odpowiadać za wymianę informacji na poziomie kraju, a także za współpracę na poziomie Unii Europejskiej.

Ustawa przyjęła federacyjny model obsługi incydentów, gdzie podmioty krajowego systemu będą

Phoca PDF

zgłaszały incydenty do właściwego CSIRT. Rolę CSIRT przyjęły na siebie Agencja Bezpieczeństwa Wewnętrznego (CSIRT GOV), Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy (CSIRT NASK) oraz resort obrony narodowej (CSIRT MON). Będą one współpracować ze sobą oraz z organami właściwymi do spraw cyberbezpieczeństwa, ministrem właściwym do spraw informatyzacji i Pełnomocnikiem Rządu ds. Cyberbezpieczeństwa. Razem zapewniać mają spójny i kompletny system zarządzania ryzykiem na poziomie krajowym, realizując zadania na rzecz przeciwdziałania zagrożeniom cyberbezpieczeństwa o charakterze ponadsektorowym i transgranicznym oraz koordynację obsługi zgłoszonych incydentów.

Źródło: Ministerstwo Cyfryzacji

Phoca PDF