Ustawa o krajowym systemie cyberbezpieczeństwa – nowe obowiązki dla operatorów usług kluczowych oraz dostawców usług cyfrowych

Przedsiębiorcy z sektora energetyki, transportu, bankowości, usług płatniczych, ochrony zdrowia, dostawcy i dystrybutorzy wody pitnej, czy zaopatrzenia w infrastrukturę cyfrową - stanowiący tzw. operatorów usług kluczowych oraz dostawcy usług cyfrowych, muszą przygotować się na konieczność sprostania kolejnym wyzwaniom, tym razem w zakresie cyberbezpieczeństwa.

3 sierpnia 2018 r. Prezydent podpisał ustawę o krajowym systemie cyberbezpieczeństwa, implementującą dyrektywę NIS (*Network and Information Systems Directive)*. Obok rozporządzenia o ochronie danych osobowych, dyrektywa jest jednym z kluczowych elementów realizowanej przez Unię Europejską strategii Jednolitego Rynku Cyfrowego. Głównym założeniem nowej regulacji jest zapewnienie jednolitego modelu bezpieczeństwa i odporności, w tym skutecznego i spójnego systemu reagowania na ataki i zagrożenia cybernetyczne.

Kogo dotyczą nowe obowiązki?

1) Operatorów usług kluczowych

Zaliczają się do nich przedsiębiorcy świadczący usługi z zakresu **bankowości, infrastruktury rynków finansowych, energetyki, transportu, czy ochrony zdrowia**, tj. takie których bezpieczeństwo jest kluczowe dla społeczeństwa i gospodarki.

Decyzje o uznaniu za operatorów usług kluczowych powinny zostać wydane **do 9 listopada 2018 r.** Wyznaczone podmioty będą miały bardzo **krótki czas na dostosowanie się do obowiązków wynikających z ustawy, zasadniczo będzie to 3 do 6 miesięcy** od doręczenia im decyzji.

2) Dostawców usług cyfrowych

Przez dostawców usługi cyfrowej należy rozumieć **internetowe platformy handlowe, dostawców usług przetwarzania w chmurze oraz wyszukiwarek internetowych**.

Jakie obowiązki przewiduje ustawa?

Ustawa skupia się na zapewnieniu bezpieczeństwa systemów informacyjnych u kluczowych przedsiębiorców, poprzez zapewnienie poufności, dostępności, integralności i autentyczności przetwarzanych w nich danych oraz usług oferowanych przez systemy.

Operatorzy usług kluczowych będą zobowiązani m.in. do:

- **Wdrożenia systemu zarządzania bezpieczeństwem w systemie operacyjnym**

System będzie polegał na wdrożeniu odpowiednich środków organizacyjnych (polityki, procedury, procesy) i technicznych, które pozwolą zapewnić bezpieczeństwo w obszarze IT, zapewnią systematyczne zarządzanie ryzykami, zbieranie i analizę informacji o zagrożeniach, identyfikację podatności oraz zarządzanie incydentami.

- **Wdrożenia procedur obsługi oraz zgłaszania incydentów bezpieczeństwa od właściwego organu**

Zgłoszenie powinno nastąpić maksymalnie w ciągu 24 godzin od wykrycia incydentu i powinno zawierać m.in. opis incydentu, jego wpływ na świadczenie usług kluczowych również przez innych operatorów, przyczynę i przebieg incydentu, a także informacje o podjętych działaniach zapobiegawczych i naprawczych. Informacje dotyczące obsługi incydentu powinny być dostarczane

organowi nadzoru na bieżąco. Przedsiębiorcy muszą liczyć się z tym, że konieczne może okazać się przekazanie nadzorcy informacji stanowiących tajemnice prawnie chronione, w tym tajemnicę przedsiębiorstwa.

Organ nadzoru może zdecydować o upublicznieniu informacji o incydencie.

Wdrożenia procedury klasyfikacji incydentów jako poważne lub istotne –progi skutków incydentu dla usługi kluczowej zostaną określone rozporządzeniem Rady Ministrów,

- natomiast w stosunku do dostawców usług cyfrowych zostały on określone w rozporządzeniu wykonawczym 2018/151/.
- **Powołania wewnętrznych struktur odpowiedzialnych za cyberbezpieczeństwo** (co może oznaczać powołanie odrębnej komórki lub przypisanie nowych zadań pracownikom, należy mieć jednak na uwadze, że komórki te będą miały charakter interdyscyplinarny) lub zawarcia umowy z podmiotem świadczącym usługi z zakresu cyberbezpieczeństwa.
- **Współpracy z organami nadzoru.**
- **Przeprowadzenia audytu bezpieczeństwa** systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej (co najmniej raz na 2 lata).
- Zapewnienia użytkownikom odpowiednich informacji pozwalających na zrozumienie zagrożeń cyberbezpieczeństwa oraz informacji dotyczących odpowiednich zabezpieczeń.

Podobne obowiązki nałożone zostały na dostawców usług cyfrowych. Ponadto, jeśli świadczą oni usługi na rzecz operatorów usług kluczowych, będą zobowiązani do przekazywania im informacji dotyczących incydentów.

Ustawa o krajowym systemie cyberbezpieczeństwa będzie wyzwaniem dla podmiotów obowiązanych do jej stosowania, zarówno pod względem zapewnienia odpowiednich środków organizacyjnych (strategia działania, informacja zarządcza, procesy zarządzania ryzykiem operacyjnym), wdrożenia i właściwego funkcjonowanie środków prewencyjnych, wykrywania i reagowania, jak również zapewnienia ciągłego budowania świadomości u pracowników, testowania organizacji pod kątem bezpieczeństwa a także zapewnienia środków gotowości odpowiedzi na zagrożenia, właściwej reakcji na incydenty – w tym efektywnej współpracy i komunikacji w tym zakresie, zebrania i analizy materiału dowodowego, i działań powłamaniowych.

Na operatorów usług kluczowych oraz dostawców usług kluczowych, którzy nie spełnią obowiązków nałożonych ustawą może zostać nałożona kara do 200 000 zł (a w wyjątkowych przypadkach do 1 mln zł).

Dodatkowo, w maju Europejski Bank Centralny (EBC) opublikował ogólnounijne zasady ramowe dotyczące przeprowadzania etycznych testów bezpieczeństwa typu red teaming – czyli symulowanych cyberataków na własną organizację na podstawie analizy informacji o zagrożeniach (Threat Intelligence Based Ethical Red Teaming, w skrócie TIBER-EU), które również wspierają sektor finansowy oraz operatorów usług kluczowych w prowadzeniu testów bezpieczeństwa.