Wprowadzenie

Statystki CERT Polska działającego przy NASK jednoznacznie wskazują, iż z roku na rok rośnie liczba cyberataków. W 2018 r. liczba zarejestrowanych incydentów była o 17,5% większa w stosunku do 2017 r., a w 2016 r. aż o 32% większa niż w 2015 r. (https://www.cert.pl/tag/statystyki/, https://www.nask.pl/pl/aktualnosci/wydarzenia/wydarzenia-2017/613,Raport-CERT-Polska-wiecej-groznych-incydentow-i-nowe-zagrozenia.html, dostęp: 20.5.2019 r.). Zgodnie z informacjami prasowymi, które pojawiły się w połowie 2018 r., średnio 700 razy na godzinę podejmowane są próby cyberataków na Polskę (https://antyweb.pl/polska-cyberataki-dane/, dostęp: 20.5.2019 r.).

Odpowiedzią na coraz większą liczbę zagrożeń w Internecie są inicjatywy prawodawcze z zakresu cyberbezpieczeństwa w ramach Unii Europejskiej, takie jak uchwalona 6.7.2016 r. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii, zwana Dyrektywą NIS (ang. *Directive on security of network and information systems, NIS Directive*). Przyjmując Dyrektywę NIS, UE nie powiedziała ostatniego słowa w zakresie ram prawnych cyberbezpieczeństwa. We wrześniu 2017 r. został przedstawiony tzw. pakiet cyberbezpieczeństwa, elementem którego był Komunikat KE „Odporność, prewencja i obrona: Budowa solidnego bezpieczeństwa cybernetycznego Unii Europejskiej" oraz projekt Cybersecurity Act. Cybersecurity Act składa się z dwóch części: nowego, permanentnego mandatu dla Europejskiej Agencji Bezpieczeństwa Sieci i Informacji (ENISA), której rola została znacznie wzmocniona, a także rozporządzenia tworzącego europejskie ramy certyfikacji cyberbezpieczeństwa dla produktów i usług ICT. Będzie to druga, po dyrektywie NIS, regulacja prawna w zakresie cyberbezpieczeństwa na poziomie europejskim.

Ustawa z 5.7.2018 r. o krajowym systemie cyberbezpieczeństwa implementuje dyrektywę NIS i ma charakter przełomowy, gdyż po raz pierwszy tworzy w Polsce całościowy prewencyjny system cyberbezpieczeństwa, obejmujący m.in.: operatorów usług kluczowych, dostawców usług cyfrowych, podmioty publiczne, podmioty świadczące usługi z zakresu cyberbezpieczeństwa, organy właściwe ds. cyberbezpieczeństwa, trzy zespoły Reagowania na Incydenty Bezpieczeństwa Komputerowego działające na poziomie krajowym (CSIRT GOV, CSIRT NASK i CSIRT MON) oraz sektorowe zespoły cyberbezpieczeństwa. Ustawa powołuje do życia Pojedynczy Punkt Kontaktowy, Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa oraz Kolegium do Spraw Cyberbezpieczeństwa. Implementując dyrektywę NIS, zobowiązuje Radę Ministrów do przyjęcia krajowej strategii w zakresie bezpieczeństwa sieci i systemów informatycznych określającej cele strategiczne oraz odpowiednie środki polityczne i regulacyjne, mające na celu osiągnięcie i utrzymanie wysokiego poziomu cyberbezpieczeństwa. Przepisy dotyczące kar pieniężnych zamykają ustawę.

Oddawany do rąk Czytelników komentarz przybliża adresatów nowych obowiązków z zakresu cyberbezpieczeństwa, opisując kryteria uznania za operatorów usług kluczowych oraz dostawców usług cyfrowych, i wskazuje na szeroką grupę podmiotów publicznych, objętych przepisami ustawy. Precyzyjnie prezentując obowiązki z zakresu cyberbezpieczeństwa spoczywające na

poszczególnych podmiotach, może służyć jako przewodnik w implementacji wymogów wynikających z ustawy i rozporządzeń wykonawczych. Przedstawia dobre praktyki w zakresie cyberbezpieczeństwa, wynikające z norm europejskich oraz wytycznych ENISA, w takich obszarach jak zarządzanie incydentami czy kwalifikacja środków organizacyjnych i technicznych pod kątem najnowszego stanu wiedzy i adekwatności, które pozwalają lepiej zrozumieć wymogi stawiane przez dyrektywę NIS i implementującą ją ustawę.

Komentarz prezentuje interdyscyplinarne podejście do tematu; wśród autorów komentarza są prawnicy (legislatorzy i praktycy) oraz specjaliści zajmujący się technicznymi aspektami cyberbezpieczeństwa. Atutem książki jest w szczególności udział w zespole autorskim ekspertów IT, którzy w komentarzu dzielą się wiedzą techniczną i udzielają praktycznych wskazówek w zakresie technologii służących cyberbezpieczeństwu.

Warszawa, 20 maja 2019 r.

Agnieszka Besiekierska