Ireneusz Piecuch, Partner i Lider Praktyki Teleinformatycznej, Kancelaria CMS

Pierwszy krok na drodze do Cyberbezpieczeństwa

McAfee, amerykańska firma stanowiąca część grupy Intel, ocenia, że działalność cyberprzestępców kosztowała globalną gospodarkę w 2017 r. około 600 miliardów dolarów - czyli prawie 0.8% światowego PKB. Dwie na każde trzy osoby korzystające z internetu zostały bądź bezpośrednio okradzione, bądź ich dane zostały przejęte przez cyfrowych przestępców, których osiągnięcia tylko nieznacznie ustępują działaniom grup specjalizujących się w korupcji oraz w narkobiznesie. Kolejność ta może zresztą szybko się zmienić. Cyberprzestępcy są bowiem w czołówce „przedsiębiorców" korzystających z najnowszych rozwiązań cyfrowych.

Płatności cyfrowe w znakomity sposób pozwoliły im na minimalizację ryzyka związanego z pobieraniem haraczu za odblokowanie zainfekowanych złośliwym oprogramowaniem serwerów, a chmura obliczeniowa na wykorzystywanie nielimitowanych zasobów informatycznych. Setki milionów różnego rodzaju urządzeń przyłączanych do sieci w ramach internetu rzeczy (IoT), pozbawionych jakiejkolwiek ochrony przed przejęciem kontroli, stanowią niewyczerpane źródło urządzeń wykorzystywanych do ataków DDoS. Ciemna strona internetu tzw. Dark Net, zapewnia możliwość handlu skradzionymi danymi na niespotykaną wręcz skalę. Prawdziwe przestępcze Eldorado - i do tego cyfrowe. I jeszcze jedno udogodnienie: niska wykrywalność i jeszcze niższa skuteczność ścigania. Przestępczość cyfrowa to biznes z definicji globalny. Nie zna granic czy problemów językowych. To dlatego zwalczanie tego typu działalności wymaga działań ponad granicami. Taka też była geneza powstania regulacji europejskiej mającej tworzyć zręby dla powstania skutecznej ochrony gospodarki i obywateli UE w Cyfrowej Europie - sztandarowym projekcie wdrażanym przez Komisję Europejską.

Dyrektywa Parlamentu Europejskiego i Rady w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (tzw. dyrektywa NIS), została uchwalona 6 lipca 2016 r. Dyrektywa zobowiązała państwa członkowskie do przyjęcia krajowych strategii w zakresie bezpieczeństwa sieci i systemów informatycznych (w Polsce strategię taką na lata 2017-2022 przyjęto w dniu 27 kwietnia 2017 r.), utworzyła tzw. grupę współpracy składającą się z przedstawicieli państw członkowskich, komisji oraz Agencji Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji ENISA (do dnia dzisiejszego grupa ta opracowała już szereg niewiążących rekomendacji dotyczących poszczególnych zagadnień adresowanych przez dyrektywę) oraz zespołów reagowania na incydenty bezpieczeństwa komputerowego (tzw. CSIRT-y). Dyrektywa zobowiązała

także państwa członkowskie do wyznaczenia organów odpowiedzialnych za realizację celów w zakresie cyberbezpieczeństwa oraz ustanowiła wymogi dotyczące bezpieczeństwa oraz zgłaszania incydentów czyli zdarzeń mających niekorzystny wpływ na bezpieczeństwo sieci i systemów informatycznych. Do dnia 9 maja 2018 r., każdy członek UE miał dokonać implementacji postanowień dyrektywy do ustawodawstwa krajowego. W Polsce proces ten zakończył się niedawno, czyli w dniu 1 sierpnia 2018 r., kiedy to Prezydent podpisał ustawę z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. Ustawa weszła w życie po 14 dniach i przez kolejne lata stanowić będzie fundament systemu ochrony polskich obywateli, przedsiębiorstw oraz jednostek administracji państwowych i samorządowych przed jednym z głównych zagrożeń XXI wieku.

Zgodnie z wymogami dyrektywy NIS, polska ustawa definiuje organizacje krajowego systemu cyberbezpieczeństwa, zadania i obowiązki podmiotów wchodzących w skład tego systemu, sposób sprawowania nadzoru i kontroli w zakresie jej stosowania oraz zakres Strategii Cyberbezpieczństwa Rzeczypospolitej Polskiej.

W skład owego systemu wchodzi dwadzieścia podmiotów lub grup podmiotów, przy czym na potrzeby niniejszego artykułu warto wymienić operatorów usług kluczowych, dostawców usług cyfrowych, trzy CSIRT-y (MON, NASK i GOV) oraz sektorowe zespoły cyberbezpieczństwa.

Operatorem usługi kluczowej, czyli usługi mającej podstawowe znaczenie dla utrzymania krytycznej działalności społecznej lub gospodarczej są podmioty wymienione w załączniku do ustawy. W odniesieniu do rynku energetycznego są to m.in. przedsiębiorstwa z sektora energii, ciepła, ropy naftowej i gazu, posiadające koncesję na wykonywanie działalności gospodarczej w zakresie wytwarzania (bądź wydobycia), przesyłania, dystrybucji, obrotu lub magazynowania odpowiednio kopalin, energii elektrycznej, ciepła, ropy naftowej lub gazu. Ponadto, ustawa wymienia też inne grupy przedsiębiorstw z sektora transportu, bankowości i infrastruktury rynków finansowych, ochrony zdrowia, zaopatrzenia w wodę pitną i jej dystrybucji oraz sektora infrastruktury cyfrowej. Do dnia 9 listopada 2018 r., organy właściwe do spraw cyberbezpieczeństwa muszą, zgodnie z treścią ustawy, wydać stosowne decyzje o uznaniu danego przedsiębiorstwa za operatora usługi kluczowej, a następnie powiadomić o tym Ministra Cyfryzacji, który prowadzi wykaz takich podmiotów. Co ciekawe, decyzja ta będzie podlegać natychmiastowemu wykonaniu, niezależnie od ewentualnej ścieżki odwoławczej. Mając na uwadze fakt, że implementacja dyrektywy NIS, ma służyć także zbudowaniu ogólnoeuropejskiego systemu zapewniającego bezpieczeństwo krajów członkowskich w cyberprzestrzeni, w przypadku podmiotów świadczących usługę kluczową także w innych państwach UE, konieczne będą konsultacje międzynarodowe prowadzone przez Ministra Cyfryzacji (a w zasadzie przez prowadzony przezeń tzw. Pojedynczy Punkt Kontaktowy).

Dla niektórych podmiotów, uznanych za operatorów usługi kluczowej, może oznaczać to dodatkowe koszty, a czasami wręcz dodatkowe inwestycje związane z dostosowaniem organizacji wewnętrznej takiego operatora oraz procesów obowiązujących w jego przedsiębiorstwie do wymogów ustawy. Głównym obowiązkiem każdego operatora usługi kluczowej jest wdrożenie systemu zarządzania bezpieczeństwem w systemie informacyjnym wykorzystywanym do świadczenia usługi kluczowej. W ramach takiego systemu, operatorzy zobowiązani będą między innymi do prowadzenia systematycznego

szacowania ryzyka wystąpienia incydentu oraz zarządzania tym ryzykiem. Dyrektywa NIS wyraźnie zachęca w takim przypadku do stosowania europejskich lub uznanych międzynarodowych norm. Przykładem takiej normy jest chociażby norma ISO 27001. System taki winien zostać wdrożony w terminie trzech miesięcy od dnia doręczenia decyzji o uznaniu za operatora usługi kluczowej, a ustawa przewiduje możliwość nałożenia kary w wysokości 150 tysięcy zł na podmioty, które takiemu obowiązkowi uchybią. Jeśli uchybianie takie miałoby cechy uporczywości i spełnione zostałyby jeszcze dodatkowe warunki, kara mogłaby wynieść nawet 1 mln zł.

fot: Pixabay.com

Kolejnym obowiązkiem operatora usługi kluczowej (tym razem z terminem realizacji 6 miesięcy), również zagrożonym karą (w wysokości 100 tys. złotych), jest obowiązek polegający na wdrożeniu odpowiednich i proporcjonalnych do oszacowanego ryzyka środków technicznych i organizacyjnych, uwzględniających najnowszy stan wiedzy. Adekwatność i proporcjonalność to zasady określone w dyrektywie NIS, dość dobrze oddające relacje pomiędzy zagrożeniem, a koniecznymi inwestycjami. Polska ustawa idzie jednak dalej wymieniając szereg cech, którymi system zarządzania bezpieczeństwem musi się charakteryzować. Otóż wdrożone środki techniczne i organizacyjne muszą zapewniać utrzymanie i bezpieczną eksploatację systemu, bezpieczeństwo fizyczne i środowiskowe, bezpieczeństwo i ciągłość dostaw usług, od których zależy świadczenie usługi kluczowej, a także wdrażanie, dokumentowanie i utrzymywanie planów działania umożliwiających ciągłe i niezakłócone świadczenie usługi kluczowej, poufność, integralność, dostępność i autentyczność informacji oraz monitorowanie systemu w trybie ciągłym.

Ponadto, system zarządzania bezpieczeństwem winien zapewniać zbieranie informacji o zagrożeniach cyberbezpieczeństwa i podatnościach na incydenty, możliwość zarządzania tymi incydentami (m.in. możliwość usuwania przyczyn wystąpienia takich incydentów) oraz stosowanie środków zapobiegających i ograniczających wpływ incydentów na bezpieczeństwo systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej.

Praktyka stosowania ustawy o KSC pozwoli na lepsze zrozumienie na ile wymagania te traktowane będą literalnie, a na ile określają one wyłącznie kierunek pożądanych działań.

Pozostałe obowiązki operatora usługi kluczowej sprowadzają się do wyznaczenia osoby odpowiedzialnej za utrzymywanie kontaktów z innymi podmiotami krajowego systemu cyberbezpieczeństwa, utrzymywania stosownej dokumentacji oraz powołanie wewnętrznej struktury organizacyjnej odpowiedzialnej za cyberbezpieczeństwo lub zawarcie umowy z podmiotem świadczącym usługi z tego zakresu (podmioty takie także wchodzą w skład KSC). Operator usługi kluczowej ma także obowiązek (przynajmniej raz na dwa lata), przeprowadzenia audytu bezpieczeństwa przez podmiot lub audytorów do tego upoważnionych. Pierwszy taki audyt powinien się odbyć w terminie roku od dnia doręczenia decyzji o uznaniu za operatora usługi kluczowej. Wyjątek od tej zasady stanowią operatorzy, u których osoby spełniające warunki zdefiniowane w ustawie dla audytorów, przeprowadziły w danym roku audyt wewnętrzny w zakresie bezpieczeństwa informacji na podstawie ustawy z 17 lutego 2015 r. o informatyzacji podmiotów realizujących zadania publiczne.

Nieco inny reżim ustawowy stosować się będzie do dostawców usług cyfrowych. Określenie to obejmuje dostawców internetowych platform handlowych, usług przetwarzania w chmurze oraz dostawców wyszukiwarek internetowych. Dyrektywa NIS, podkreśla-

jąc niższy niż w przypadku operatorów usług kluczowych poziom ryzyka, nakazuje tu stosowanie łagodniejszych wymogów w zakresie bezpieczeństwa oraz pozostawienie dostawcom usług cyfrowych swobody w podejmowaniu środków, które uznają za odpowiednie do zarządzania ryzykiem, na jakie może być narażone bezpieczeństwo ich sieci i systemów informatycznych. Uznając potrzebę dalej idącej harmonizacji podejścia, Komisja wydała także 18 stycznia 2018 r. rozporządzenie wykonawcze w tym zakresie. Podążając za dyrektywą, ustawa o KSC nakazuje więc dostawcom usług cyfrowych podjęcie właściwych i proporcjonalnych środków technicznych i organizacyjnych określonych w rozporządzeniu wykonawczym oraz podjęcie środków zapobiegających i minimalizujących wpływ incydentów na usługę cyfrową.

Zarówno dostawcy usług kluczowych, jak i cyfrowych zobowiązani są (choć nieco w innym zakresie) do obsługi incydentów, ich klasyfikacji oraz zgłaszania ich do właściwego CSIRT. W przypadku operatorów usług kluczowych dotyczy to incydentów poważnych, czyli takich, które powodują lub mogą powodować poważne obniżenie jakości lub przerwanie ciągłości świadczenia usługi kluczowej. Dostawcy usług cyfrowych zgłaszać będą incydenty istotne - tj. incydenty, które mogą spowodować, iż usługa taka będzie niedostępna przez ponad 5 milionów użytkownikogodzin, które doprowadziły do utraty integralności lub poufności danych (lub powiązanych usług) co najmniej 100 tysięcy użytkowników w skali UE), incydenty powodujące ryzyko dla bezpieczeństwa publicznego lub ryzyko wystąpienia ofiar śmiertelnych a także incydenty, które wyrządziły, przynajmniej jednemu użytkownikowi UE stratę materialną wyższą niż milion euro. Każdy taki incydent winien być zgłoszony niezwłocznie, nie później jednak niż w ciągu 24 godzin od jego wykrycia, pod rygorem kary w wysokości 20 tys. zł za każdy przypadek braku zgłoszenia.

Kolejną po dostawcach usług kluczowych oraz dostawcach usług cyfrowych grupą podmiotów wchodzących w skład KSC są, zgodnie z wymogami dyrektywy NIS, organy krajowe do spraw bezpieczeństwa sieci i systemów informatycznych. Polska ustawa wdrażająca dyrektywę przewiduje dość rozbudowaną i skomplikowaną strukturę składającą się z trzech zdefiniowanych w ustawie CSIRT-ów (CSIRT GOV - prowadzony przez Szefa ABW, CSIRT MON - prowadzony przez Ministra Obrony Narodowej oraz CSIRT NASK - prowadzony przez Naukową i Akademicką Sieć Komputerową - Państwowy Instytut Badawczy), sektorowych zespołów cyberbezpieczeństwa, organów właściwych do spraw cyberbezpieczeństwa (przykładowo Minister Energetyki w odniesieniu do sektora energii), Pojedynczego Punktu Kontaktowego, Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa oraz Kolegium do Spraw Cyberbezpieczeństwa.

CSIRT-y współpracując na gruncie krajowym z pozostałymi wymienionymi tu podmiotami a na gruncie europejskim współpracując w ramach tzw. Sieci krajowych CSIRT, mają zapewnić spójny i kompletny system zarządzania ryzykiem na poziomie krajowym, realizując zadania na rzecz przeciwdziałania zagrożeniom cyberbezpieczeństwa o charakterze ponadsektorowym i transgranicznym, a także zapewniając koordynację obsługi zgłoszonych incydentów. Mogą też w niektórych przypadkach udzielać wsparcia w obsłudze incydentów. Najbardziej widocznym, zewnętrznym objawem działalności CSIRT-ów będą zapewne komunikaty o zidentyfikowanych zagrożeniach cyberbezpieczeństwa, ale uprawnienia tych podmiotów sięgają dużo dalej, łącznie z prowadzeniem badań urządzeń informatycznych i oprogramowania w celu identyfikacji podatności, której wykorzystanie może zagrozić w szczególności integralności, poufności, rozliczalności, autentyczności lub dostępności przetwarzania danych mogących mieć wpływ na bezpieczeństwo publiczne lub istotny interes bezpieczeństwa państwa. Badania takie mogą stanowić podstawę do wystąpienia do Pełnomocnika Rządu o wydanie rekomendacji dotyczących stosowania takich urządzeń lub oprogramowania. CSIRT-y mają także uprawnienia do wystąpienia do organu właściwego do spraw cyberbezpieczeństwa z wnioskiem o wezwanie operatora usługi kluczowej lub dostawcy usługi cyfrowej, aby w wyznaczonym terminie usunął podatności, które doprowadziły lub mogłyby doprowadzić do incydentu (nie usunięcie takiej podatności zagrożone jest sankcją w wysokości 20 tys. zł).

Koordynację działań i realizowanie polityki rządu w zakresie cyberbezpieczeństwa ustawa pozostawia w rękach Pełnomocnika (w randze Sekretarza lub Podsekretarza Stanu), podlegającego Radzie Ministrów i powoływanego i odwoływanego przez Prezesa Rady Ministrów. Pełnomocnik taki dokonywać ma między innymi analizy ocen funkcjonowania KSC, sprawować nadzór nad procesem zarządzania ryzykiem KSC, opiniować dokumenty rządowe mające wpływ na realizacje zadań z zakresu cyberbezpieczeństwa oraz wydawać rekomendacje dotyczące stosowania urządzeń informatycznych lub oprogramowania na wniosek CSIRT. W jego gestii pozostawać będzie także współpraca w zakresie cyberbezpieczeństwa z innymi państwami, wspieranie badań naukowych i rozwój technologii z zakresu cyberbezpieczeństwa oraz podejmowanie inicjatyw edukacyjnych w tym zakresie. Przy Radzie Ministrów powstanie także Kolegium, jako ciało opiniodawczo-doradcze a niezależnie od Pełnomocnika i Kolegium, Prezes Rady Ministrów, w celu koordynacji działań administracji rządowej w zakresie cyberbezpieczeństwa otrzymał uprawnienie wydawania wiążących wytycznych dotyczących zapewnienia cyberbezpieczeństwa na poziomie krajowym. Głównym narzędziem kształtowania polityki rządu będzie jednak Strategia przyjmowana przez Radę Ministrów w drodze uchwały.

Strategia taka zostanie przyjęta do dnia 31 października 2019 r.

Kończąc omawianie głównych wątków ustawy o KSC, warto także wspomnieć o tym, że do dnia 1 stycznia 2021 r. Minister Cyfryzacji zobowiązany będzie zapewnić rozwój i utrzymanie systemu teleinformatycznego wspierającego działania opisane w ustawie, w szczególności zgłaszanie i obsługę incydentów oraz ostrzeganie o zagrożeniach cyberbezpieczeństwa.

Niewątpliwie samo uchwalenie ustawy o KSC jest olbrzymim krokiem naprzód, bo choć wymuszona dyrektywą NIS, daje ona szanse na systematyczne i kompleksowe zaadresowanie problemu stanowiącego jedno z głównych wyzwań cyfryzacji życia prywatnego i publicznego. Jak zostało to już wspomniane, cyberprzestępczość to intratny biznes ale nie tylko. Wykorzystywanie złośliwego oprogramowania służyć może jako narzędzie wspomagające lub zastępujące działania militarne (możemy wspomnieć chociażby wirus Stuxnet, który sparaliżował na lata irański projekt jądrowy), narzędzie do szpiegostwa przemysłowego na olbrzymią skalę (wedle specjalistów wartość skradzionej w ten sposób własności intelektualnej liczy się w miliardach dolarów) a także narzędzie mogące wpłynąć na to, jakie będą wyniki kolejnych wyborów. Cyberzagrożenia to globalne wyzwanie cywilizacyjne o potencjalnych negatywnych skutkach nieporównywalnych ze skutkami naruszenia dóbr osobistych. Nic zatem dziwnego, że w niektórych krajach implementacja dyrektywy NIS wiąże się z sankcjami porównywalnymi z tymi, które przewiduje dziś inna regulacja europejska - RODO.

Wydaje się jednak, że oprócz niewątpliwych zalet, ustawa o KSC ma także poważne wady, które mogą znacznie utrudnić a być może uniemożliwić osiągniecie zakładanych celów. Po pierwsze, w proponowanym kształcie, ustawa ta tworzy niesłychanie skomplikowany system kilkudziesięciu organów mających nierzadko podobne cele i kompetencje, które powinny aktywnie ze sobą współpracować. Narzędzie mające zapewnić efektywność tej współpracy pojawi się jednak dopiero za ponad dwa lata. Oczywiście, specjalny system można zastąpić istniejącymi narzędziami informatycznymi, ale dużo trudniej będzie się zmierzyć z wyzwaniem pozyskania odpowiednio licznego grona specjalistów skłonnych do rozwijania swojej kariery w ramach służby publicznej.

Kolejnym problemem jest finansowanie. Jednym z głównych zarzutów Raportu NIK z 2015 r. weryfikującego działania ówczesnej administracji w obszarze cyberbezpieczeństwa, był brak stworzenia solidnych podstaw finansowych dla funkcjonowania systemu ochrony. Obecna regulacja nie zmienia tego stanu rzeczy w zasadniczy sposób. Co więcej, zgodnie z treścią ustawy o KSC, wyczerpanie wyjątkowo skąpych limitów budżetowych związanych z jej realizacją, oznaczać będzie ograniczenie działań przewidzianych tą ustawą (tj. zmniejszenie liczby kontroli, rezygnacja z ćwiczeń w zakresie cyberbezpieczeństwa etc.). To trochę tak, jakby straży pożarnej ustalić odgórne limity na zużycie paliwa a po ich wyczerpaniu zaprzestać wyjazdów do pożarów. W tym samym czasie budżet USA przeznaczany na zwalczanie cyberprzestępczości to ponad 14 miliardów dolarów rocznie.

Pomimo, że prace nad ustawą trwały bardzo długo, nie ustrzeżono się też licznych niejasności, które mogą w przyszłości powodować problemy interpretacyjne. Przykładowo, po wystąpieniu incydentu to operator usługi kluczowej zobowiązany jest do zapewnienia jego obsługi, „współpracując" w tej mierze z odpowiednim CSIRT-em. Na czym jednak polegać ma taka współpraca? Ustawa nakłada także na CSIRT-y obowiązek „reagowania" na zgłoszone incydenty, ale nie wyjaśnia na czym reakcja taka ma polegać. Jeszcze inny przepis tejże ustawy przewiduje, że w uzasadnionych przypadkach i wyłącznie na wniosek operatora usługi kluczowej, dostawcy usług kluczowych lub innych uprawnionych podmiotów, CSIRT może zapewnić wsparcie w obsłudze incydentów. Nie wiadomo jednak o jakich uzasadnionych przypadkach mowa i jakie będą kryteria udzielenia takiej pomocy. Na CSIRT-y nałożono także obowiązek przekazania operatorowi usługi kluczowej zgłaszającemu poważny incydent, informacji dotyczących działań podjętych po zgłoszeniu incydentu, które mogłyby pomóc w jego obsłudze… "jeżeli pozwalają na to okoliczności". Podobnych znaków zapytania jest więcej.

Wydaje się także, że ustawa w swoim obecnym kształcie, ma niewielkie szanse na stworzenie skutecznej platformy aktywnej współpracy pomiędzy podmiotami prywatnymi a podmiotami publicznymi. Jej tradycyjna, nakazowo-rozdzielcza konstrukcja wydaje się ignorować fakt, że to po stronie przedsiębiorców istnieją olbrzymie zasoby, które można byłoby wykorzystać dla osiągnięcia zakładanych celów. W końcu, wydaje się, że absolutnie słuszna idea przeprowadzania obowiązkowych audytów w zakresie cyberbezpieczeństwa, również może nie osiągnąć zakładanych celów, a to na skutek dość liberalnego podejścia do kompetencji audytorów przeprowadzających takie audyty.

Pomimo tych mankamentów, pierwszy krok na drodze do zwiększenia poziomu cyberbezpieczeństwa został dokonany. Ważne, aby kolejne działania związane z wdrożeniem tej ustawy w życie (w tym wydanie wszystkich aktów wykonawczych, zorganizowanie efektywnej pracy nowych organów oraz aktywne uczestniczenie Polski w pracach organów europejskich) pokazały, że jest to krok wystarczająco duży, aby pokonać pierwszą przeszkodę. Nie ma bowiem nic bardziej niebezpiecznego jak próba pokonania przepaści w kilku krokach.

□