DMZ KANCELARIA

Stan realizacji wymogów ustawy o cyberbezpieczeństwie w Polsce

Ustawa o krajowym systemie cyberbezpieczeństwa (Ustawa o KSC) weszła w życie dnia 28 sierpnia 2018 r., aby w pełni wdrożyć Dyrektywę Parlamentu Europejskiego i Rady (UE) 2016/1148 w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dyrektywa NIS). Ustawa obchodzi w tym roku swoje dwulecie obowiązywania. Jakie istotne wydarzenia dla tego obszaru miały w tym czasie miejsce, jak do tej pory swoje zadania wypełniały podmioty tworzące krajowy system cyberbezpieczeństwa oraz jakie nowe wyzwania rysują się w przyszłości w tym obszarze?

Anna Dmochowska
DMZ Kancelaria Prawna, Adwokat. Współpracuje m.in. z grupami kapitałowymi, w tym podmiotami rynku finansowego w zakresie projektów dostosowania systemów ochrony danych osobowych do wymogów RODO. Audytor wiodący ISO 9001 oraz 22301. Prowadzi projekty wdrożenia Systemów Zarządzania ISO w organizacjach produkcyjnych jak i usługowych. Obsługuje organizacje w obszarze cyberbezpieczeństwa. Posiada doświadczenie w tworzeniu i negocjowaniu umów.

Raport CSIRT GOV o stanie bezpieczeństwa cyberprzestrzeni RP za 2019 r.

Ciekawe konkluzje dotykające cyberbezpieczeństwa w Polsce możemy znaleźć w raporcie o stanie bezpieczeństwa cyberprzestrzeni RP w 2019 r. autorstwa CSIRT GOV. W raporcie wskazano, iż miniony rok był rekordowy pod względem zgłoszeń dotyczących incydentów teleinformatycznych – było ich aż 226 914. Dla porównania, w roku 2018 odnotowano ich 31 865. Liczba zdarzeń, która została zarejestrowana jako faktyczny incydent wyniosła 12 405, co jest niemalże dwukrotnym wzrostem względem 2018 r., kiedy odnotowano 6 236 przypadków faktycznego naruszenia bezpieczeństwa teleinformatycznego. Zgodnie z raportem CSIRT GOV najczęściej występującą formą incydentu są zdarzenia określane jako „wirus", które stanowią ok. 58% wszystkich incydentów. W tej kategorii mieszczą się głównie zgłoszenia z systemu ARAKIS GOV. Dodatkowo jak wskazuje CSIRT GOV jednym z największych zagrożeń, z którymi zespół CSIRT GOV spotyka się najczęściej są kampanie phishingowe, które w większości są rozsyłane w sposób masowy.

Jak słusznie wskazano w przedmiotowym raporcie zwiększająca się liczba użytkowników sieci Internet, korzystających z coraz bardziej zaawansowanych technologii determinuje konieczność opracowywania oraz wdrażania coraz nowszych rozwiązań technicznych służących ochronie cyberprzestrzeni RP. Słusznie zwrócono uwagę na problem, iż atakujący stale zmieniają i udoskonalają profil prowadzonych działań oraz wykorzystują nowe metody służące do przeprowadzenia ataków. Z uwagi na to koniecznym staje się zintensyfikowanie prowadzonych działań prewencyjnych w sferze organizacyjnej oraz technicznej.

Nowe wytyczne w zakresie warunków technicznych i organizacyjnych

Aby w pełni wdrożyć Dyrektywę NIS w Polsce, potrzebne było przyjęcie dodatkowych rozporządzeń Rady Ministrów jako aktów wykonawczych. I tak w Polsce obowiązują następujące akty wykonawcze do Ustawy o KSC:

- Rozporządzenie Rady Ministrów w sprawie wykazu usług kluczowych oraz progów istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych;
- Rozporządzenie Rady Ministrów w sprawie rodzajów dokumentacji dotyczącej cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej;
- Rozporządzenie Rady Ministrów w sprawie progów uznania incydentu za poważny;
- Rozporządzenie Ministra Cyfryzacji w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu;
- Rozporządzenie Rady Ministrów w sprawie zakresu działania oraz trybu pracy Kolegium do Spraw Cyberbezpieczeństwa;
- Rozporządzenie Ministra Cyfryzacji w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo.

Istotna zmiana miała miejsce w przypadku ostatniego z wymienionych rozporządzeń. Pierwotna wersja z dnia 10 września 2018 r. została zastąpiona nowym rozporządzeniem o tej samej nazwie, które weszło w życie 7 stycznia 2020 r. Pierwotna wersja rozporządzenia spotkała się z krytyką m.in. z uwagi na wskazanie na sztywno warunków organizacyjnych i technicznych, jakie muszą spełnić operatorzy usług kluczowych. Postulowano przede wszystkim wprowadzenie wymogu zastosowania zabezpieczeń adekwatnych do oszacowanego ryzyka w danej instytucji.

I tak zgodnie z postulatami podmiotów będących uczestnikami Ustawy o KSC nowe rozporządzenie wprowadziło właśnie wymóg dostosowania zabezpieczeń adekwatnie do szacowanego ryzyka, tak aby zapewnić skuteczne:

- monitorowanie i wykrywanie incydentów bezpieczeństwa informacji;
- reagowanie na incydenty bezpieczeństwa;
- zapobieganie incydentom;
- zarządzanie jakością zabezpieczeń systemów, informacji i powierzonych aktywów;
- aktualizowanie ryzyk w przypadku zmiany struktury organizacyjnej, procesów i technologii, które mogą wpływać na reakcję na incydent.

Jest to zmiana na plus, ponieważ teraz organizacje mogą stosować zabezpieczenia techniczne i organizacyjne zgodnie z realiami w jakich funkcjonują.

Audyt zgodny z ustawą o KSC

Ustawa o KSC wprowadza obowiązek przeprowadzenia audytu bezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej raz na 2 lata, przy czym pierwszy audyt powinien zostać przeprowadzony w ciągu roku od dnia doręczenia decyzji o uznaniu podmiotu za operatora usługi kluczowej. Z uwagi na czas jaki upłynął od wejścia w życie Ustawy o KSC to większość podmiotów już jest po wyżej wskazanym audycie lub jest w trakcie jego organizowania.

Ciekawy materiał w tym zakresie możemy znaleźć m.in. na stronie ISSA Polska. Opublikowała ona bowiem szablon sprawozdania z audytu zgodnego z ustawą o KSC. Materiał został opracowany wraz z Ministerstwem Cyfryzacji oraz organami właściwymi, o których mowa w Ustawie o KSC. Jest to bardzo przydatny materiał podczas spełniania wyżej wskazanego obowiązku.

Szablon jest znakomitym punktem wyjścia dla członków zespołu audytu wewnętrznego organizacji. Jak wskazują na swoich stronach internetowych organy właściwe, o których mowa w Ustawie o KSC, poczytuje się za dobra praktykę korzystanie z przedmiotowego szablonu. Organy te zalecają również podmiotom zewnętrznych, które miałyby wykonać audyt na zlecenie organizacji, do przygotowania raportu właśnie zgodnie z przedmiotowym szablonem. W celu zachowania zgodności oraz porównywalności niedopuszczalne jest kasowanie i modyfikowanie struktury rozdziałów. Zalecane jest dodawanie podrozdziałów trzeciego poziomu zgodnie ze stanem faktycznym oraz wykonanymi pracami, jeżeli w opinii zespołu audytowego obecna struktura dokumentu nie jest kompletna. Jednakże nie należy usuwać żadnych rozdziałów z szablonu. Wszystkie niewypełnione rozdziały i podrozdziały powinny zostać oznaczone jako nieadekwatne z uzasadnieniem audytora.

Nadchodzą zmiany w Ustawie o KSC

Ministerstwo Cyfryzacji zapowiedziało projekt zmian w Ustawie o KSC oraz Ustawie – Prawo zamówień publicznych.

Według projektu przedsiębiorcy komunikacji elektronicznej mają stać się częścią krajowego systemu cyberbezpieczeństwa. W związku z powyższym ma zostać wprowadzona nowa kategoria incydentu tzw. incydent telekomunikacyjny. Projekt przewiduje powołanie odrębnego zespołu reagowania na incydenty bezpieczeństwa komputerowego, czyli CSIRT Telco. Przypomnijmy, że Ustawa o KSC usankcjonowała trzy podmioty na poziomie krajowym, które zajmują się reagowaniem na incydenty komputerowe wraz z ich zarządzaniem. Zgodnie z terminologią przyjętą w Dyrektywie NIS zostały one określone jako CSIRT (ang. Computer Security Incident Response Teams). W Polsce są to CSIRT GOV, CSIRT MON, CSIRT NASK. Ustawa wprowadza również pojęcie sektorowego zespołu cyberbezpieczeństwa, a więc zespołu ustanowionego przez organ właściwy dla danego sektora lub podsektora (wymienionego w załączniku do ustawy). Zespół ten odpowiedzialny jest za obsługę lub wsparcie obsługi incydentów w swoim sektorze lub podsektorze. Dotychczas powstał tylko jeden sektorowy zespół cyberbezpieczeństwa – Sektorowy Zespół Cyberbezpieczeństwa dla Sektora Bankowości i Infrastruktury Rynków Finansowych (CSIRT-KNF).

Zmiany umożliwią powstanie sektorowych CSIRT we wszystkich kluczowych dla społeczno-ekonomicznego bezpieczeństwa państwa i obywateli sektorach gospodarki.

Kolejną proponowaną zmianą jest przyznanie Kolegium ds. Cyberbezpieczeństwa kompetencji do oceny ryzyka dostawców sprzętu lub oprogramowania istotnego dla cyberbezpieczeństwa podmiotów krajowego systemu cyberbezpieczeństwa. Do tej pory obszar ten był niezagospodarowany a jest istotny z punktu widzenia bezpieczeństwa dostarczanych usług dla operatorów usług kluczowych. Wprowadzenie przez państwa członkowskie UE tego typu ocen ryzyka zostało uzgodnione z Komisją Europejską i ENISA[1], jako jeden ze środków strategicznych w dokumencie 5G Toolbox[2]. Planowane jest również wprowadzenie do krajowego systemu cyberbezpieczeństwa operacyjnych centrów bezpieczeństwa, czyli SOC a zgodnie z doniesieniami taką rolę mają pełnić już funkcjonujące w Polsce CSIRTy.

Wreszcie w propozycjach zmian znalazła się możliwość tworzenie ISAC, czyli specjalistycznych organizacji, dzięki którym podmioty krajowego systemu cyberbezpieczeństwa będą miały możliwość bieżącej wymiany informacji o incydentach, zagrożeniach, podatnościach oraz dobrych

[1] Europejska Agencja Bezpieczeństwa Sieci i Informacji

[2] Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów Bezpieczne Wprowadzanie sieci 5G w UE – wdrażanie unijnego zestawu narzędzi.

praktykach. ISAC usprawnią także współpracę podmiotów z zespołami CSIRT poziomu krajowego.

Jaki jest cel wprowadzania powyższych zmian? Usprawnienie krajowego systemu cyberbezpieczeństwa m.in. w takich obszarach jak:

- ujednolicenie na poziomie krajowym procedur zgłaszania incydentów, w tym także incydentów raportowanych przez przedsiębiorstwa telekomunikacyjne;
- zapewnienie warunków do utworzenia zespołów reagowania na incydenty komputerowe (CSIRT) w sektorach i podsektorach gospodarki o kluczowym znaczeniu dla społeczno-ekonomicznego bezpieczeństwa państwa (sektorowe CSIRT);
- wzmocnienie współpracy operatorów usług kluczowych z organami właściwymi oraz zespołami CSIRT poziomu krajowego w zakresie wymiany informacji o incydentach, podatnościach, zagrożeniach i dobrych praktykach;
- umożliwienie tworzenia centrów analizy i wymiany informacji (ISAC).

Realizacja „projektu S46" Ministerstwa Cyfryzacji

Zgodnie z wymogami ujętymi w Ustawie o KSC a konkretnie art. 46 KSC Minister właściwy do spraw informatyzacji (tj. Ministerstwo Cyfryzacji) zapewnia rozwój lub utrzymanie systemu teleinformatycznego wspierającego:

- współpracę podmiotów wchodzących w skład krajowego systemu cyberbezpieczeństwa,
- generowanie i przekazywanie rekomendacji dotyczących działań podnoszących poziom cyberbezpieczeństwa,
- zgłaszanie i obsługę incydentów,
- szacowanie ryzyka na poziomie krajowym,
- ostrzeganie o zagrożeniach cyberbezpieczeństwa.

Zadanie to realizowane jest w ramach aktualnie trwającego projektu S46 wykonywanego przez NASK PIB na zlecenie Ministerstwa Cyfryzacji. Od 2017 roku NASK PIB realizuje zadanie związane z opracowaniem kompleksowego, zintegrowanego systemu monitorowania, obrazowania i ostrzegania o zagrożeniach identyfikowanych w czasie zbliżonym do rzeczywistego w cyberprzestrzeni państwa.

Zgodnie z medialnymi informacjami część informatyczna systemu jest tworzona w ramach projektu pt. Narodowa Platforma Cyberbezpieczeństwa (NPC) współfinansowanego przez NCBR w ramach programu CyberSecIdent, a część sieciowa, w ramach projektu NPCnet realizowanego na zlecenie Ministerstwa Cyfryzacji. Z medialnych doniesień[3] wynika, że w dniu 28 maja 2020 r. miało miejsce ważne wydarzenie, wyznaczające rozpoczęcie końcowego etapu realizacji systemu. Został zainstalowany i podłączony pierwszy, zewnętrzny w stosunku do Grupy NASK, system brzegowy partnera – klienta Platformy. Należy podkreślić, że wcześniej został już zainstalowany i podłączony system brzegowy obsługujący NASK SA, a podłączanie kolejnych partnerów będzie miało miejsce w najbliższym czasie. Zgodnie z informacjami, zakończenie projektu ma nastąpić w drugim kwartale 2021 r.

W dniu 22 października 2019 r. Rada Ministrów podjęła uchwałę ws. Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024.

Przedmiotowa strategia była jednym z głównych wyzwań w zakresie budowania odporności na cyberzagrożenia oraz poziomu ochrony informacji w sektorach: publicznym, militarnym i prywatnym. Na lepszą ochronę informacji ma wpłynąć też promowanie wiedzy i dobrych praktyk wśród obywateli.

Strategia cyberbezpieczeństwa RP na lata 2019-2024

W dniu 22 października 2019 r. Rada Ministrów podjęła uchwałę ws. Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024.

Przedmiotowa strategia była jednym z głównych wyzwań w zakresie budowania odporności na cyberzagrożenia oraz poziomu ochrony informacji w sektorach: publicznym, militarnym i prywatnym. Na lepszą ochronę informacji ma wpłynąć też promowanie wiedzy i dobrych praktyk wśród obywateli.

Strategia określa strategiczne cele oraz odpowiednie środki polityczne i regulacyjne, które należy zrealizować, aby systemy informacyjne, operatorzy usług kluczowych, operatorzy infrastruktury krytycznej, dostawcy usług cyfrowych oraz administracja publiczna były odporne na cyberzagrożenia. Celem zasadniczym jest więc zwiększenie poziomu bezpieczeństwa narodowego. Strategia wymienia 5 szczegółowych celów. Cel szczegółowy 1 - rozwój krajowego systemu cyberbezpieczeństwa. Cel szczegółowy 2 - podniesienie poziomu odporności systemów informacyjnych administracji publicznej i sektora prywatnego oraz osiągnięcie zdolności do skutecznego zapobiegania i reagowania na incydenty zakłada się m.in. opracowanie Narodowych Standardów Cyberbezpieczeństwa. Cel szczegółowy 3 - zwiększenie potencjału narodowego w zakresie technologii cyberbezpieczeństwa. Cel szczegółowy 4 - budowanie świadomości i kompetencji społecznych w zakresie cyberbezpieczeństwa. Cel szczegółowy 5 - zbudowanie silnej pozycji międzynarodowej Rzeczypospolitej Polskiej w obszarze cyberbezpieczeństwa.

Za wypełnienie zapisów strategii odpowiada Minister właściwy ds. informatyzacji (tj. Ministerstwo Cyfryzacji), we współpracy z pozostałymi członkami Rady Ministrów. Ministerstwo zobowiązane jest również do przedkładania raportów do 30 marca każdego roku przedstawiających informację o realizacji strategii cyberbezpieczeństwa.

Głównym zastrzeżeniem jest fakt, że nie zapewniono funduszy na realizację zadań wynikających ze Strategii. Dokument ma być realizowany z budżetów poszczególnych jednostek oraz ze środków Narodowego Centrum Badań i Rozwoju, a także z funduszy europejskich.

[3] https://www.nask.pl/pl/aktualnosci/3859,NASK-realizuje-projekty-NPC-i-NPCnet.html