Przemysław Mazurczak
Koło Naukowe Doktorantów Nauk o Bezpieczeństwie
Uniwersytet Przyrodniczo-Humanistyczny w Siedlcach

Podmioty prywatne w polskim systemie cyberbezpieczeństwa

Streszczenie: *Z początkiem sierpnia 2018 r. zaczął funkcjonować krajowy system cyberbezpieczeństwa jako nowoczesna linia obrony przed cyberzagrożeniami. Składa się on z operatorów usług kluczowych i dostawców usług cyfrowych, w tym przedsiębiorców państwowych oraz prywatnych, którzy świadczą usługi na rzecz cyberbezpieczeństwa. Ustawa o krajowym systemie cyberbezpieczeństwa nakłada na podmioty wiele obowiązków, przez co stają się oni kluczowym ogniwem przeciwdziałania incydentom komputerowym.*

Wstęp

W artykule zaprezentowano zasadnicze uwarunkowania oraz budowę i funkcjonowanie polskiego systemu cyberberbezpieczeństwa z uwzględnieniem wkładu interesariuszy spoza administracji publicznej w budowę i funkcjonowanie tego systemu. Istotnym uwarunkowaniem dla funkcjonowania podmiotów prywatnych w systemie bezpieczeństwa jest *Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa*[1]. Określa ona organizację krajowego systemu cyberbezpieczeństwa oraz zadania i obowiązki podmiotów wchodzących w skład tego systemu, a także zakres Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej.[2] W ustawie zawarto kategorie podmiotów wchodzących w skład systemu, wśród których znaleźli się operatorzy usług kluczowych i dostawcy usług cyfrowych, a także instytuty badawcze, spółki prawa handlowego oraz podmioty świadczące usługi w zakresie cyberbezpieczeństwa.

Krajowy system cyberbezpieczeństwa ma na celu zapewnienie bezpieczeństwa teleinformatycznego na poziomie krajowym, w szczególności niezakłóconego świadczenia usług kluczowych i usług cyfrowych oraz osiągnięcie odpowiednio wysokiego poziomu bezpieczeństwa systemów informatycznych służących do świadczenia tych usług.

[1] *Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa* (Dz.U. 2018, poz. 1560), s. 1.
[2] Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022, Ministerstwo Cyfryzacji, Warszawa 2017, https://www.gov.pl/documents/31305/0/strategia_cyberbezpieczenstwa_rzeczypospolitej_polskiej_na_lata_2017_-_2022.pdf/f249b627-4050-a6f4-5cd3-351aa025be09, 07.07.2019.

Budowa i funkcjonowanie Polskiego systemu cyberbezpieczeństwa

Polski system cyberbezpieczeństwa składa się z operatorów usług kluczowych podzielonych na sektory; energetyczny, transportowy, zdrowotny i bankowy oraz dostawców usług cyfrowych, zespoły CSIRT[3] poziomu krajowego, sektorowe zespoły cyberbezpieczeństwa, podmioty świadczące usługi z zakresu cyberbezpieczeństwa, organy właściwe do spraw cyberbezpieczeństwa oraz pojedynczy punkt kontaktowy do komunikacji w ramach współpracy w Unii Europejskiej w dziedzinie spraw cyberbezpieczeństwa[4]. Operatorzy usług kluczowych są zobowiązani do wdrożenia skutecznych zabezpieczeń i szacowania ryzyka związanego z cyberbezpieczeństwem. Mają oni za zadanie przekazywanie informacji o poważnych incydentach oraz ich obsługę we współpracy z administracją poziomu krajowego. Obowiązkami z zakresu cyberbezpieczeństwa zostali także objęci dostawcy usług cyfrowych, czyli internetowe platformy handlowe, usługi przetwarzania w chmurze i wyszukiwarki internetowe.

Lista podmiotów wchodzących w skład systemu nie jest jawna. Od wejścia w życie ustawy każdy podmiot osobno otrzymuje informację od Ministerstwa Cyfryzacji i ma trzy miesiące na przygotowanie infrastruktury, oszacowanie ryzyka i wyznaczenie osoby koordynującej incydenty. Przez kolejne sześć miesięcy podmiot ma obowiązek wdrożyć środki techniczne i procedury zgodnie z przyjętym poziomem ryzyka. Po roku czasu podmioty są zobowiązane zgodnie z ustawą przygotować audyt ze swojej działalności[5].

Wprowadzenie ustawy o krajowym systemie cyberbezpieczeństwa jest dostosowaniem prawa do wymogów Dyrektywy Parlamentu Europejskiego i Rady Unii Europejskiej 2016/1148 w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii Europejskiej[6] W związku z dyrektywą utworzono krajowy system obsługi incydentów wraz z koordynacją na szczeblu europejskim, a także ogłoszono szczegółowe rozporządzenia, określające wymagania w zakresie warunków organizacyjnych i technicznych, dokumentacji, audytowania oraz bezpieczeństwa systemu informacyjnego wybranych podmiotów. Nadzór nad działalnością tego systemu sprawuje administracja publiczna, co będzie wiązało się z częstymi kontrolami i przyczyni się do zwiększenia poziomu polskiego cyberbezpieczeństwa.

---

[3] Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego, Ministerstwo Cyfryzacji, https://www.gov.pl/web/cyfryzacja/zespol-reagowania-na-incydenty-bezpieczenstwa-komputerowego-csirt, 23.07.2019.

[4] Krajowy system cyberbezpieczeństwa. Ustawa o krajowym systemie cyberbezpieczeństwa, Ministerstwo Cyfryzacji, https://www.gov.pl/web/cyfryzacja/krajowy-system-cyberbezpieczenstwa-, dostęp 07.07.2019 r.

[5] Co powinieneś wiedzieć o Krajowym Systemie Cyberbezpieczeństwa, EXATEL, https://exatel.pl/krajowy-system-cyberbezpieczenstwa-ksc-exatel, dostęp 07.07.2019 r.

[6] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r., https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A32016L1148, dostęp 07.07.2019r.

Operatorzy usług kluczowych

Operatorzy usług kluczowych to podmioty określone przez ustawę z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa prowadzący swoją działalność na terenie Polski. Do ich obowiązków należy szacowanie ryzyka wystąpienia zagrożeń, utrzymywanie i eksploatacja systemu informacyjnego oraz dbanie o bezpieczeństwo fizyczne i środowiskowe posiadanych systemów[7]. Ponadto, operatorzy mają obowiązek zbierać informację o zagrożeniach i podatnościach na incydenty w obrębie własnych obszarów oraz przekazywać te dane do centrum obsługi incydentów prowadzonym przez zespoły CSIRT. Incydenty posiadają priorytet ważności pod którym są obsługiwane. W ustawie zdefiniowano incydenty istotne, poważne i krytyczne.[8]

Lista podmiotów włączonych w system nie jest jawna, ale ustawodawca sklasyfikował je w kategorie. Wśród nich znajduje się wiele prywatnych przedsiębiorców, są nimi w odpowiednich sektorach firmy energetyczne, prowadzące wydobycie paliw oraz dostawcy usług dla sektora energii. W sektorze transportu znajdują się firmy transportowe obsługujące transport lotniczy, kolejowy, morski i drogowy. W sektorze bankowości i rynków finansowych wymienione zostały banki oraz niektóre instytucje kredytowe. Sektor ochrony zdrowia charakteryzuje się obecnością firm farmaceutycznych i usług medycznych. Przy sektorze cyfrowym wyszczególniono podmioty prowadzące rejestry domen i punkty wymiany ruchu internetowego.[9] Wszystkie podmioty objęte ustawą mają takie same obowiązki i wymogi bezpieczeństwa. Ujednolicenie to ma na celu stworzenie wysokiej jakości ochrony przed cyberprzestępczością.

Dostawcy usług cyfrowych

Drugą grupą podmiotów zobligowaną do ochrony zasobów cyberprzestrzeni są dostawcy usług cyfrowych, czyli przedsiębiorcy z wyjątkiem małych firm, którzy świadczą usługi cyfrowe. Rynek tych usług jest bardzo szeroki i może dotyczyć zarówno teleoperatorów, jak i dostawców rozwiązań bezpieczeństwa teleinformatycznego. Dostawcy będąc częścią systemu cyberbezpieczeństwa są zobowiązani zachować wysoki stopień bezpieczeństwa swoich systemów. Mają oni za zadanie zgłaszać incydenty oraz prowadzić bieżący monitoring i audyt na swoim obszarze funkcjonowania. Podobnie jak podmioty kluczowe, dostawcy są

[7] *Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa* (Dz.U. 2018, poz. 1560), s. 4.
[8] Tamże, s. 5.
[9] Krajowy system cyberbezpieczeństwa. Ustawa o krajowym systemie cyberbezpieczeństwa, Ministerstwo Cyfryzacji, https://www.gov.pl/web/cyfryzacja/krajowy-system-cyberbezpieczenstwa, dostęp 07.07.2019r.

zobowiązani do współpracy związanej z obsługą bieżących incydentów i przekazywaniu informacji odpowiednim organom nadzorczym, czyli zespołom CSIRT. Dostawcy usług cyfrowych powinni zapewnić wysoki poziom bezpieczeństwa współmierny do stopnia ryzyka na jakie narażone jest bezpieczeństwo świadczonych przez nich usług.

System cyberbezpieczeństwa RP określa trzy rodzaje usług cyfrowych, są to: internetowe platformy handlowe, usługi przetwarzania w chmurze oraz wyszukiwarki internetowe. Wśród dużych podmiotów zajmujących się e-handlem można wyróżnić np.: firmę Allegro, która należy do nieformalnej organizacji zrzeszającej podmioty działające na rzecz ochrony polskiej cyberprzestrzeni. Tą organizacją jest „Abuse Forum", która posiada własne centrum bezpieczeństwa[10]. Wśród firm zajmujących się udostępnianiem usług przetwarzania w chmurze należy wskazać podmioty udostępniające swoje serwery np.: do przechowywania plików. Przykładem tego jest polski serwis chomikuj.pl. Na liście znalazły się także wyszukiwarki internetowe. Ich właściciele, czasem międzynarodowe korporacje typu Google przetwarzają dużą ilość danych i są zobligowane do odpowiedniego zabezpieczenia tego procesu.

Wnioski

- Polski system cyberbezpieczeństwa sformalizował i ujednolicił obowiązki podmiotów świadczących usługi na rzecz cyberbezpieczeństwa.
- W budowę systemu zaangażowano zarówno podmioty administracyjne, jak i prywatne przedsiębiorstwa.
- Podział podmiotów na operatorów usług kluczowych oraz dostawców usług cyfrowych umożliwił włączenie do systemu prywatne przedsiębiorstwa.
- Brak jawnej listy podmiotów wchodzących w skład polskiego systemu cyberbezpieczeństwa ma na celu ochronę tego systemu przed obcym wywiadem.
- Wprowadzenie w życie krajowego systemu cyberbezpieczeństwa jest dostosowaniem prawa do wymogów Dyrektywy Parlamentu Europejskiego i Rady Unii Europejskiej 2016/1148 w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii Europejskiej.
- Operatorzy usług kluczowych stanowią podstawę systemu cyberbezpieczeństwa. Ich obowiązkiem jest szacowanie ryzyka wystąpienia zagrożeń,

[10] Abuse Forum Polska, https://www.abuse-forum.pl, dostęp 07.07.2019 r.

utrzymywanie i eksploatacja systemu informacyjnego oraz dbanie o bezpieczeństwo fizyczne i środowiskowe posiadanych systemów.
- Dostawcy usług cyfrowych są grupą podmiotów uzupełniających system. Ich obowiązki skupiają się na ochronie własnych systemów informatycznych, wymianie informacji oraz dostosowywaniu tworzonej technologii do wymaganych warunków bezpieczeństwa.

Podsumowanie

Pojawiające się coraz częściej i coraz bardziej wyrafinowane ataki cyberprzestępców na sieci informatyczne mogą pociągać za sobą ogromne straty związane z utratą reputacji, własności intelektualnej czy ograniczeniem zdolności do świadczenia usług. W celu ograniczenia działalności przestępców Parlament Europejski wprowadził w sierpniu 2016 r. Dyrektywę 2016/1148[11] dotyczącą zwiększenia ochrony zasobów informatycznych podmiotów świadczących usługi cyfrowe. Dyrektywa spowodowała wprowadzenie w Polsce ustawy o krajowym systemie cyberbezpieczeństwa. Wprowadzenie tej ustawy nałożyło na przedsiębiorców nowe obowiązki. Firmy muszą spełnić unijne standardy dotyczące odporności ich systemów na ataki hakerów. Przepisy zawarte w dyrektywie odnoszą się do dwóch grup podmiotów: operatorów usług kluczowych i dostawców usług cyfrowych.

Ustanowienie wspólnych standardów cyberbezpieczeństwa oraz poprawa współpracy między krajami UE ma pomóc przedsiębiorstwom skuteczniej stawiać czoła hakerom, a także pomóc w zapobieganiu atakom na infrastrukturę cyfrową. Ustawa wprowadza kompleksowe zarządzanie zdarzeniami, mającymi negatywny wpływ na cyberbezpieczeństwo, czyli wskazuje sposoby na obsługę incydentów przez podmioty do tego wyznaczone. Wprowadzenie nowych przepisów umożliwia zarządzanie cyberbezpieczeństwem z poziomu krajowego.

Nowy system cyberbezpieczeństwa jest czymś czego w Polsce brakowało od wielu lat. Wcześniej pojawiały się koncepcje związane z budową i organizacją tego systemu, jednak pozostały one jedynie rekomendacjami administracji. Obecny system funkcjonuje w oparciu o przepisy Unii Europejskiej. Skuteczność jego działania możliwa będzie do oceny dopiero po kilku latach, na podstawie przeprowadzenia oceny corocznych audytów dotyczących obsługi incydentów przez podmioty objęte obowiązkiem składania takich sprawozdań. Dzięki wprowadzonym zmianom, w Polsce cyberbezpieczeństwo zacznie być traktowane priorytetowo i jego poziom w najbliższych latach będzie się zbliżał do europejskich standardów.

[11] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r., https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A32016L1148, 07.07.2019r.

Literatura

Abuse Forum Polska, https://www.abuse-forum.pl, dostęp 07.07.2019 r.

Co powinieneś wiedzieć o Krajowym Systemie Cyberbezpieczeństwa, EXATEL, https://exatel.pl/krajowy-system-cyberbezpieczenstwa-ksc-exatel, dostęp 07.07.2019 r.

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r., https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A32016L1148, dostęp 07.07.2019r.

Krajowy system cyberbezpieczeństwa. Ustawa o krajowym systemie cyberbezpieczeństwa, Ministerstwo Cyfryzacji, https://www.gov.pl/web/cyfryzacja/krajowy-system-cyberbezpieczenstwa-, dostęp 07.07.2019 r.

Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022, Ministerstwo Cyfryzacji, Warszawa 2017, https://www.gov.pl/documents/31305/0/strategia_cyberbezpieczenstwa_rzeczypospolitej_polskiej_na_lata_2017_-_2022.pdf/f249b627-4050-a6f4-5cd3-351aa025be09, 24.07.2019.

Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. (Dz.U 2018, poz. 1560).

Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego, Ministerstwo Cyfryzacji, https://www.gov.pl/web/cyfryzacja/zespol-reagowania-na-incydenty-bezpieczenstwa-komputerowego-csirt, 23.07.2019.

Private entities in the cybersecurity Polish system

Summary: At the beginning of August 2018, the National Cyber Security System has started working. The system is a modern line of defense against cyber threats and consists of operators of key services and digital service providers, including state-owned and private enterprises that provide services for cybersecurity. The Act on the National Cybersecurity System imposes many obligations on entities, which makes them a key link to counteracting computer incidents.
Keywords: cybersecurity system, public administration, security solutions providers, social media