https://doi.org/10.31268/ZPBAS.2021.61 nr 3(71) 2021 ▪ s. 280–314 ZESZYTY PRAWNICZE BAS Biura Analiz Sejmowych Kancelarii Sejmu

Danuta Adamiec*, Justyna Branna**, Dobromir Dziewulak***, Natalia Firlej****, Kamila Groszkowska*****, Marta Karkowska******, Łukasz Żołądek*******

Informacja na temat legislacji dotyczącej systemu cyberbezpieczeństwa w wybranych państwach Unii Europejskiej (Belgia, Czechy, Estonia, Francja, Holandia, Niemcy, Szwecja)[1]

Legislation on the cybersecurity system in selected EU Member States (Belgium, Czech Republic, Estonia, France, Netherlands, Germany, Sweden)

The study presents information on the legislation on the cybersecurity system in selected European Union countries. The discussed laws in force in individual countries implement the NIS Directive concerning measures for a high common level of security of network and information systems across the Union. The NIS Directive specifies the institutions that should be established in all Member States; it regulates cooperation at the European level and imposes obligations in the field of network and information systems security, including the duty to adopt a national strategy on the security of network and information systems.

Keywords: security, digitalisation, internet, European Union

W opracowaniu przedstawiono informacje na temat legislacji dotyczącej systemu cyberbezpieczeństwa w wybranych państwach UE. Omówione przepisy obowiązujące w poszczególnych państwach implementują dyrektywę NIS w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii. Dyrektywa NIS określa instytucje, które powinny powstać we wszystkich państwach członkowskich; reguluje kwestie współpracy na poziomie europejskim oraz nakłada zobowiązania w zakresie bezpieczeństwa sieci i informacji, w tym m.in. obowiązek przyjęcia narodowej strategii bezpieczeństwa sieci i informacji.

Słowa kluczowe: bezpieczeństwo, cyfryzacja, Internet, Unia Europejska

* Doktor nauk prawnych, specjalista ds. międzynarodowych Biura Analiz Sejmowych ▪ Kancelaria Sejmu, Biuro Analiz Sejmowych, Wydział Analiz Prawa Międzynarodowego i Zagranicznych Systemów Prawnych, WARSZAWA, POLSKA ▪ danuta.adamiec@sejm.gov.pl ▪ https://orcid.org/0000-0002-6600-4309

** Specjalista ds. międzynarodowych Biura Analiz Sejmowych ▪ Kancelaria Sejmu, Biuro Analiz Sejmowych, Wydział Analiz Prawa Międzynarodowego i Zagranicznych Systemów Prawnych, WARSZAWA, POLSKA ▪ justyna.branna@sejm.gov.pl ▪ https://orcid.org/0000-0002-9653-9996

[1] *Informacja na temat legislacji dotyczącej systemu cyberbezpieczeństwa w wybranych państwach Unii Europejskiej (Belgia, Czechy, Estonia, Francja, Holandia, Niemcy, Szwecja)* sporządzona 22 stycznia 2021 r. na zlecenie posła Koalicyjnego Klubu Parlamentarnego Lewicy (Razem, Sojusz Lewicy Demokratycznej, Wiosna Roberta Biedronia); BAS-ZSP-2360/20.

*** Doktor nauk humanistycznych, adiunkt ▪
Uniwersytet Warszawski, Wydział Pedagogiczny, Katedra Dydaktyki i Pedeutologii, WARSZAWA, POLSKA ▪
dobromir.dziewulak@uw.edu.pl ▪ https://orcid.org/0000-0002-7974-8024

**** Specjalista ds. międzynarodowych Biura Analiz Sejmowych ▪
Kancelaria Sejmu, Biuro Analiz Sejmowych, Wydział Analiz Prawa Międzynarodowego i Zagranicznych Systemów Prawnych, WARSZAWA, POLSKA ▪
natalia.firlej@sejm.gov.pl ▪ https://orcid.org/0000-0002-9522-5522

***** Specjalista ds. międzynarodowych Biura Analiz Sejmowych ▪
Kancelaria Sejmu, Biuro Analiz Sejmowych, Wydział Analiz Prawa Międzynarodowego i Zagranicznych Systemów Prawnych, WARSZAWA, POLSKA ▪
kamila.groszkowska@sejm.gov.pl ▪ https://orcid.org/0000-0002-8618-1302

****** Doktor nauk humanistycznych, adiunkt ▪
Polska Akademia Nauk, Instytut Filozofii i Socjologii, WARSZAWA, POLSKA ▪
mkarkowska@ifispan.edu.pl ▪ https://orcid.org/0000-0003-0747-4332

******* Specjalista ds. międzynarodowych Biura Analiz Sejmowych ▪
Kancelaria Sejmu, Biuro Analiz Sejmowych, Wydział Analiz Prawa Międzynarodowego i Zagranicznych Systemów Prawnych, WARSZAWA, POLSKA ▪
lukasz.zoladek@sejm.gov.pl ▪ https://orcid.org/0000-0001-5247-6228

W przygotowaniu niniejszego opracowania wykorzystano obcojęzyczne akty prawne oraz obcojęzyczną i polską literaturę przedmiotu. Przeanalizowano informacje dostępne na stronach internetowych instytucji, organizacji i stowarzyszeń zajmujących się problematyką cyberbezpieczeństwa. Wykorzystano także materiały znajdujące się w bazie Europejskiego Centrum Badań i Dokumentacji Parlamentarnej (*European Centre for Parliamentary Research and Documentation*, ECPRD).

Wstęp

Pojęciem cyberbezpieczeństwa określa się ogół technik, procesów i praktyk realizowanych w celu ochrony sieci informatycznych, urządzeń, programów i danych przed atakami, uszkodzeniami lub nieautoryzowanym dostępem do cybernetycznej przestrzeni przetwarzania informacji np. w sieciach teleinformatycznych.

Pierwszym europejskim prawem w zakresie cyberbezpieczeństwa jest przyjęta w 2016 r. dyrektywa w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii[2] (nazywa-

[2] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii, Dz.Urz. UE L 194 z 19 lipca 2016 r., s. 1, https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32016L1148&from=PL.

na dyrektywą NIS lub NIS 1)[3]. Dyrektywa nakłada na państwa członkowskie wiele obowiązków, obliguje je między innymi do powołania konkretnych instytucji oraz wprowadzenia mechanizmów współpracy. Dyrektywa zobowiązuje wszystkie państwa członkowskie do zagwarantowania minimalnego poziomu krajowych zdolności w dziedzinie bezpieczeństwa teleinformatycznego. Jej przepisy umożliwiają stworzenie zarówno scentralizowanego systemu na poziomie krajowym, jak i podzielenie kompetencji między różne podmioty. Dokument stanowi jednak harmonizację minimalną, a zatem wyznacza pewne minimalne warunki, które należy spełniać. Nie ogranicza przy tym możliwości państw członkowskich do szerszego i bardziej szczegółowego regulowania tej problematyki[4].

Tekst dyrektywy koncentruje się na trzech filarach:

1. instytucjach, które powinny powstać we wszystkich państwach członkowskich,
2. współpracy na poziomie europejskim,
3. zobowiązaniach w zakresie bezpieczeństwa sieci i informacji.

Ad 1. Każde państwo członkowskie zostało zobligowane do ustanowienia organów właściwych ds. bezpieczeństwa sieci i informacji (*National Competent Authorities*). Funkcję tę mogą pełnić już istniejące instytucje. Zadaniem organu właściwego jest monitorowanie wdrożenia przepisów dyrektywy na poziomie krajowym we wszystkich sektorach objętych regulacją. Państwa mogą wyznaczyć jeden lub kilka organów. Jest to istotne zwłaszcza, jeśli istnieją regulatorzy sektorowi, wtedy to oni mogą odpowiadać za wdrożenie dyrektywy we właściwych sobie sektorach. Ponadto każde państwo członkowskie musi ustanowić Pojedynczy Punkt Kontaktowy (*Single Point of Contact*, PPK). Jego zadaniem jest wzmacnianie współpracy między państwami członkowskimi. Będzie również gromadził informacje o incydentach w skali kraju, a także wymieniał się informacjami o znaczących, międzynarodowych incydentach ze swoimi odpowiednikami z zagranicy. Kolejną instytucją wskazaną w dyrektywie jest CSIRT, czyli Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego (C*omputer Security Incident Response Team*). Kraje członkowskie mogą wyznaczyć jeden CSIRT narodowy dla całego kraju bądź zbudować sieć CSIRT-ów sektorowych, obejmujących sektory rynkowe.

Ad 2. Dyrektywa NIS wprowadziła mechanizmy współpracy na dwóch poziomach: technicznym i polityczno-strategicznym. W obszarze technicznym współpraca ma być zapewniona przez europejską sieć CISRT (*CSIRT network*) oraz stworzenie mechanizmów wymiany informacji o incydentach transgranicznych, a w obszarze polityczno-strategicznym ma być realizowana przez utworze-

---

[3] Trwają obecnie prace nad nowelizacją dyrektywy NIS.

[4] W prawie polskim dyrektywa została implementowana ustawą z 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz.U. 2020 poz. 1369) oraz uchwałą nr 125 Rady Ministrów z 22 października 2019 r. w sprawie „Strategii cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024" (M.P. poz. 1037).

nie Grupy Współpracy (*Cooperation Group*), która zajmie się wypracowaniem wspólnych koncepcji strategicznych oraz będzie przyjmowała między innymi roczne raporty od właściwych organów.

Ad 3. Wśród zobowiązań dyrektywa nakłada na państwa członkowskie także obowiązek przyjęcia narodowej strategii bezpieczeństwa sieci i informacji, w której określone zostaną między innymi: narodowe cele i priorytety cyberbezpieczeństwa, role i obowiązki organów administracji publicznej, zasady współpracy sektora publicznego i prywatnego, krajowa analiza ryzyka oraz zadania w zakresie edukacji.

W **Belgii** podstawowym aktem prawnym w zakresie cyberbezpieczeństwa jest ustawa implementująca do krajowego porządku prawnego dyrektywę NIS. Natomiast obowiązującym dokumentem określającym krajowy plan działania w zakresie cyberbezpieczeństwa jest „Narodowa strategia cyberbezpieczeństwa" z 23 listopada 2012 r.

W **Czechach** podstawowym aktem w zakresie bezpieczeństwa cybernetycznego jest ustawa nr 181/2014 z 23 lipca 2014 r. o bezpieczeństwie cybernetycznym, która implementuje dyrektywę NIS. Aktualna strategia państwa w zakresie bezpieczeństwa cybernetycznego zawarta jest w przyjętym przez rząd w listopadzie 2020 r. dokumencie zatytułowanym „Krajowa strategia bezpieczeństwa cybernetycznego Republiki Czeskiej na lata 2020–2025".

W **Estonii** podstawowym aktem obejmującym bezpieczeństwo cybernetyczne jest ustawa o bezpieczeństwie cybernetycznym z 2018 r., która wdraża do prawodawstwa estońskiego wymogi unijnej dyrektywy NIS. Oprócz ustawy podstawą podejmowanych działań związanych z cyberbezpieczeństwem są szczegółowe dokumenty strategiczne. Na lata 2019–2022 obowiązuje strategia, której głównym celem jest uznanie bezpieczeństwa cybernetycznego za priorytet dla społeczeństwa estońskiego.

We **Francji** transpozycję unijnej dyrektywy NIS dokonano za pomocą ustawy nr 2018-133 z 2018 r. i dekretu nr 2018-384 z 2018 r., ale już wcześniej, 16 października 2015 r., uchwalono strategię bezpieczeństwa cyfrowego. Została ona opracowana w związku z narastającym zagrożeniem terrorystycznym. Strategia ma na celu wspieranie cyfrowej transformacji francuskiego społeczeństwa i stawianie czoła nowym wyzwaniom związanym ze zmieniającymi się zastosowaniami technologii cyfrowych i związanymi z nimi zagrożeniami.

W **Holandii** implementacji unijnej dyrektywy NIS dokonano w ustawie o bezpieczeństwie sieci i systemów informacyjnych z 2018 r., na której przede wszystkim opiera się funkcjonowanie obowiązującego systemu cyberbezpieczeństwa. Jednakże system ten i instytucje właściwe w tym obszarze funkcjonowały przed wdrożeniem dyrektywy na podstawie krajowej strategii w zakresie cyberbezpieczeństwa z 2011 r. W konsekwencji implementacji dyrektywy NIS w 2018 r. przyjęto „Krajową strategię cyberbezpieczeństwa", która jako cel wyznaczyła między innymi ochronę bezpieczeństwa narodowego w przestrzeni cyfrowej.

W **Niemczech** na poziomie federalnym najważniejsze rozwiązania legislacyjne przewidziane w unijnej dyrektywie NIS już wcześniej zostały zawarte w ustawie o Federalnym Urzędzie Bezpieczeństwa Teleinformatycznego z 2009 r., a także w ustawie o zwiększeniu bezpieczeństwa systemów informatycznych z 2015 r. W związku z tym, po implementowaniu dyrektywy NIS do prawa federalnego, wprowadzono w nim stosunkowo niewielkie zmiany.

W **Szwecji** aktem implementującym dyrektywę NIS jest ustawa o bezpieczeństwie sieci i systemów informatycznych z 2018 r., która nakłada na operatorów usług kluczowych i dostawców usług cyfrowych obowiązek podjęcia środków prewencyjnych w celu zapewnienia bezpieczeństwa sieci i systemów informatycznych. Jednakże już w 2017 r. rząd przyjął narodową długofalową strategię cyberbezpieczeństwa, a w 2019 r. opublikował całościowy plan zawierający 77 działań w obszarze cyberbezpieczeństwa, których podjęcie przewidziano na lata 2019–2022.

Belgia

W Belgii obowiązującym dokumentem określającym krajowy plan działania w zakresie cyberbezpieczeństwa jest „Narodowa strategia cyberbezpieczeństwa" (*Stratégie Nationale de Cybersécurité*) z 23 listopada 2012 r.[5] (dalej: strategia). W strategii podkreślono, że społeczeństwo, gospodarka i ekonomia Belgii zależą w znacznym stopniu od wykorzystywanych technologii informacyjnych i komunikacyjnych. W strategii rozpoznano podstawowe czynniki zagrożenia dla cyberbezpieczeństwa krajowego jako: powszechny dostęp do Internetu; wykorzystywanie komercyjnych technologii w swoich systemach informatycznych przez instytucje publiczne; gromadzenie danych i korzystanie z możliwości przechowywania danych „w chmurze"; przechowywanie dużych ilości danych zagrażających prywatności obywateli; brak możliwości stosowania zaawansowanych systemów zabezpieczeń przez różne podmioty sektora publicznego; nieadekwatność współpracy międzynarodowej w zakresie cyberbezpieczeństwa. Zwrócono uwagę, że zagrożenia w cyberprzestrzeni są realne i w związku z gwałtownym rozwojem technologicznym stanowią coraz poważniejszy problem. Wśród głównych zagrożeń wymieniono między innymi cyberszpiegostwo, *cyberwarfare* (wykorzystywanie technologii do zakłócenia lub uniemożliwienia działania struktur państwa, w tym np. infrastruktury krytycznej) i cyberterroryzm.

W strategii określone zostały trzy cele:

- cyberprzestrzeń w Belgii ma być pewna i niezawodna, przy zachowaniu fundamentalnych praw i zasad nowoczesnego społeczeństwa,

[5] Https://ccb.belgium.be/sites/default/files/BE_NCSS_fr_0.pdf.

- Belgia zapewni ochronę i należyte bezpieczeństwo publicznym systemom informatycznym i infrastrukturze krytycznej, w szczególności ochronę przed cyberzagrożeniami i cyberatakami,
- Belgia będzie rozwijać swoje zdolności w zakresie cyberbezpieczeństwa.

W strategii wskazano, że do realizacji powyższych celów konieczne jest podejście zcentralizowane i zintegrowane, także we współpracy z partnerami międzynarodowymi. Uwzględniono też znaczenie świata nauki i środowiska akademickiego. Na podstawie strategii mają być opracowane ramy prawne, zakładające równowagę między zachowaniem prawa do prywatności obywateli a koniecznością wdrożenia systemów cyberzabezpieczeń, w tym aktualizacja kompetencji policji, sądów i innych organów do spraw bezpieczeństwa. Strategia zakłada także monitorowanie cyberzagrożeń i zwiększanie zdolności reagowania w przypadku wystąpienia incydentów i ataków na sieci informatyczne, przyjęcie szczególnych rozwiązań w zakresie cyberprzestępczości oraz rozwijanie technologii i współpraca ze środowiskiem naukowym.

Podstawowym aktem prawnym w zakresie cyberbezpieczeństwa jest ustawa z 7 kwietnia 2019 r. implementująca do krajowego porządku prawnego dyrektywę NIS, ustanawiająca ramy bezpieczeństwa sieci i systemów informatycznych użyteczności publicznej dla bezpieczeństwa publicznego[6] (dalej: ustawa). Zgodnie z art. 3 ustawy jej przepisy mają zastosowanie do operatorów usług kluczowych, prywatnych oraz publicznych, mających co najmniej jedno przedstawicielstwo na terytorium Belgii. Ustawa ma również zastosowanie do dostawców usług cyfrowych posiadających swoją siedzibę na terenie Belgii oraz do dostawców nie posiadających adresu swojej działalności (*établissement*) na terenie Unii Europejskiej, świadczących usługi na terytorium Belgii oraz posiadających w Belgii swojego przedstawiciela, dla celów dyrektywy NIS. Operatorzy usług kluczowych to wyznaczeni przez organy sektorowe dostawcy usług w sektorach energii, transportu, finansów, opieki zdrowotnej, wody pitnej i infrastruktury cyfrowej. Ustawa nakłada na operatorów usług kluczowych i dostawców usług cyfrowych obowiązek podjęcia określonych działań w zakresie cyberbezpieczeństwa. Operatorzy usług kluczowych muszą przyjąć niezbędne i proporcjonalne środki techniczne i organizacyjne, w celu zarządzania ryzykiem związanym z zagrożeniami bezpieczeństwa sieci i systemów informatycznych. Ponadto są zobowiązani do wyznaczenia inspektora ochrony danych i zapewnienia punktu kontaktowego do spraw bezpieczeństwa IT (techniki informacyjnej, ang. *information technology*) oraz zgłaszania zaistniałych incydentów. Za nieprzestrzeganie przepisów ustawy grożą sankcje karne i administracyjne.

Zgodnie z art. 7 ustawy król Belgii wyznacza organ krajowy odpowiedzialny za monitorowanie i koordynację wdrażania przepisów ustawy. Organ ten pełni

---

[6] *Loi de 7 Avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique*, http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&cn=2019040715&table_name=loi.

też rolę Pojedynczego Punktu Kontaktowego, wymaganego na podstawie art. 11 dyrektywy NIS oraz funkcję narodowego CSIRT. Organem krajowym jest Belgijskie Centrum Cyberbezpieczeństwa (*Centre pour la Cybersécurité Belgique*, CCB lub Centrum[7]). Ustawa nakłada także na organ krajowy (CCB) obowiązek utworzenia platformy internetowej, na której będzie można zgłaszać cyberincydenty (platforma NIS, www.nis-incident.be).

Aktem wykonawczym do ustawy jest dekret królewski wdrażający ustawę z 7 kwietnia 2019 r. ustanawiającą ramy bezpieczeństwa sieci i systemów informatycznych użyteczności publicznej dla bezpieczeństwa publicznego oraz ustawę z 1 lipca 2011 r. o bezpieczeństwie i ochronie infrastruktury krytycznej[8].

Belgijskie Centrum Cyberbezpieczeństwa zostało utworzone na podstawie dekretu królewskiego z 10 października 2014 r.[9] i podlega nadzorowi premiera. Swoje działania CCB realizuje przy wsparciu Kancelarii Prezesa Rady Ministrów. Jednym z głównych zadań Centrum jest opracowanie krajowej strategii bezpieczeństwa sieci i informacji. Ponadto zgodnie z art. 3 dekretu królewskiego Centrum jest odpowiedzialne za:

- monitorowanie, koordynowanie i nadzorowanie realizacji belgijskiej polityki w zakresie cyberbezpieczeństwa,
- zapewnienie koordynacji między odpowiednimi departamentami, organami administracji publicznej, podmiotami prywatnymi i sektorem naukowym,
- formułowanie propozycji mających na celu dostosowanie ram regulacyjnych w dziedzinie cyberbezpieczeństwa,
- zapewnienie zarządzania kryzysowego w przypadku incydentów dotyczących bezpieczeństwa sieci i systemów informatycznych, we współpracy z rządowym centrum zarządzania kryzysowego,
- przygotowywanie, rozpowszechnianie i nadzorowanie wdrażania wytycznych i standardów bezpieczeństwa dla różnych systemów informatycznych rządów i instytucji publicznych,
- reprezentowanie Belgii na forum międzynarodowym w dziedzinie cyberbezpieczeństwa, monitorowanie i nadzorowanie zobowiązań międzynarodowych,
- koordynowanie oceny bezpieczeństwa i certyfikacji systemów informatycznych i komunikacyjnych,

---

[7] *Centre pour la Cybersécurité Belgique*, https://ccb.belgium.be/en/organisation.

[8] *Arrêté royal portant exécution de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique, ainsi que de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques*, http://www.ejustice.just.fgov.be/eli/arrete/2019/07/12/2019041284/moniteur.

[9] *Arrêté royal de 10 Octobre 2014 portant création du Centre pour la Cybersécurité Belgique*, http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&cn=2014101008&table_name=loi.

- prowadzenie działalności edukacyjnej i podnoszenie świadomości użytkowników w zakresie systemów informatycznych i komunikacyjnych.

Obecnie CCB jest w trakcie prac nad znowelizowaniem obowiązującej od 2012 r. „Narodowej strategii cyberbezpieczeństwa".

Czechy

W Czechach aktualna strategia państwa w zakresie bezpieczeństwa cybernetycznego zawarta jest w przyjętym przez rząd w listopadzie 2020 r. dokumencie „Krajowa strategia bezpieczeństwa cybernetycznego Republiki Czeskiej na lata 2020–2025"[10] (dalej: strategia). Strategia będzie implementowana na podstawie planu działań, który ma zostać przyjęty do 30 czerwca 2021 r.[11].

Zgodnie z informacjami zawartymi w strategii podejście Czech do bezpieczeństwa cybernetycznego opiera się na współpracy podmiotów na poziomie krajowym i międzynarodowym, przy czym istotne znaczenie ma precyzyjne określenie zakresu kompetencji i uprawnień poszczególnych instytucji. Wskazuje się w niej na dynamicznie rozwijającą się sytuację w zakresie bezpieczeństwa, w tym na rosnące zjawisko zagrożenia szpiegostwem zarówno w odniesieniu do instytucji państwowych, jak i prywatnych przedsiębiorstw czy instytucji naukowych lub badawczych. W strategii podkreśla się także wzrost znaczenia operacji wojskowych w cyberprzestrzeni. W tym kontekście, jak wskazano w strategii, istotne jest nie tylko skupienie się na aktualnych zagrożeniach dla bezpieczeństwa cybernetycznego, ale także umiejętność adaptacji do nowych, nieustannie zmieniających się warunków w zakresie bezpieczeństwa.

W strategii wskazano cele w zakresie bezpieczeństwa cybernetycznego na lata 2020–2025. Podzielono je na trzy obszary:

- świadomość w cyberprzestrzeni (wspólne podejście do cyberbezpieczeństwa, wzmacnianie bezpieczeństwa infrastruktury, skuteczna strategia komunikacyjna, wymiana informacji itp.),
- silne i niezawodne sojusze (efektywna współpraca międzynarodowa, promowanie interesów państwa za granicą, eksport tzw. *know-how* itp.),
- prężne społeczeństwo 4.0 (bezpieczna e-administracja, edukacja, tworzenie bazy eksperckiej).

---

[10] *Národní strategie kybernetické bezpečnosti České republiky na období let 2020–2025*. Dokument ten nawiązuje do poprzedniej strategii bezpieczeństwa cybernetycznego (*Národní strategie kybernetické bezpečnosti České republiky na období let 2015–2020*). Dokumenty są dostępne na stronie: https://www.nukib.cz/cs/kyberneticka-bezpecnost/strategie-akcni-plan/.

[11] Plan działań do strategii na lata 2015–2020 jest dostępny na stronie https://www.nukib.cz/download/publikace/strategie_akcni_plany/akcni_plan_2015-2020.pdf.

Podstawowym aktem w zakresie bezpieczeństwa cybernetycznego jest ustawa nr 181/2014 z 23 lipca 2014 r. o bezpieczeństwie cybernetycznym oraz o zmianie niektórych ustaw[12] (dalej: ustawa). Ustawa ta implementuje dyrektywę NIS. W ustawie oraz wydanych na jej podstawie przepisach wykonawczych[13] określono kryteria identyfikacji operatorów usług kluczowych w sektorach energetyki, transportu, bankowości, infrastruktury rynków finansowych, służby zdrowia, gospodarki wodnej, infrastruktury cyfrowej oraz przemysłu chemicznego. Zasady zgłaszania incydentów dotyczących bezpieczeństwa cybernetycznego określono w § 8 ustawy. Incydenty, które mają istotny wpływ na ciągłość usług, operatorzy usług kluczowych zgłaszają niezwłocznie Krajowemu Urzędowi ds. Bezpieczeństwa Cybernetycznego i Informacyjnego (*Národní úřad pro kybernetickou a informační bezpečnost*, NÚKIB)[14], który pełni funkcję krajowego pojedynczego punktu kontaktowego ds. bezpieczeństwa sieci i systemów informatycznych (zgodnie z § 22 ustawy). Dostawcy usług cyfrowych zgłaszają incydenty do krajowego CERT (*národní CERT*[15]). NÚKIB prowadzi ewidencję incydentów, a zgromadzone w niej dane udostępnia organom administracji publicznej oraz innym podmiotom (zasady udostępniania określono w § 9 ustawy).

Krajowy Urząd ds. Bezpieczeństwa Cybernetycznego i Informacyjnego (NÚKIB) sprawuje kontrolę w zakresie bezpieczeństwa cybernetycznego. Za wykroczenia polegające na niewypełnieniu obowiązków nałożonych przepisami ustawy nr 181/2014 przewidziano grzywny w wysokości od 10 000 do 5 000 000 koron czeskich (a dla osób fizycznych w wysokości do 50 000 koron czeskich). NÚKIB prowadzi postępowanie w sprawie wykroczeń.

Jak wskazano w krajowej strategii bezpieczeństwa cybernetycznego z 2020 r., system zapewnienia bezpieczeństwa cybernetycznego w Czechach opiera się na wielu podmiotach, przy czym kluczową rolę w tym zakresie odgrywa rząd jako naczelny organ władzy wykonawczej. Odpowiada on za zapewnienie bezpieczeństwa oraz za sprawne funkcjonowanie całego systemu bezpieczeństwa

---

[12] *Zákon č. 181/2014 Sb. ze dne 23. července 2014 o kybernetické bezpečnosti a o změně souvisejících zákonů*, ze zm., tekst ujednolicony w jęz. czeskim dostępny: https://www.zakonyprolidi.cz/cs/2014-181.

[13] *Vyhláška č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby*, https://www.zakonyprolidi.cz/cs/2017-437; *Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti)*, https://www.zakonyprolidi.cz/cs/2018-82.

[14] Https://nukib.cz/en/about-nukib/.

[15] Krajowy CERT (*Computer Emergency Response Team*), zgodnie z § 17 ustawy nr 181/2014, zapewnia wymianę informacji z zakresu cyberbezpieczeństwa na poziomie krajowym i międzynarodowym oraz pełni funkcję Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego. Funkcję krajowego CERT Republiki Czeskiej pełni Zespół CSIRT.CZ, https://www.csirt.cz/cs/o-nas/.

kraju. Centralnym organem administracji ds. bezpieczeństwa cybernetycznego jest NÚKIB. Sekcją wykonawczą NÚKIB jest Krajowe Centrum Bezpieczeństwa Cybernetycznego (*Národní centrum kybernetické bezpečnosti*, NCKB)[16]. NÚKIB odpowiada między innymi za ochronę krytycznej infrastruktury informatycznej oraz innych istotnych systemów i sieci informacyjnych i komunikacyjnych. Dyrektor NÚKIB uczestniczy w posiedzeniach Rady Bezpieczeństwa Państwa (*Bezpečnostní rada státu*, BRS)[17] oraz jest członkiem Komitetu ds. Cyberbezpieczeństwa (*Výbor pro kybernetickou bezpečnost*)[18], który jest stałym organem roboczym BRS do spraw koordynacji planowania działań mających na celu zapewnienie bezpieczeństwa cybernetycznego Czech. Oprócz NÚKIB w systemie bezpieczeństwa cybernetycznego funkcjonuje krajowy CERT oraz rządowy CERT[19] (ich kompetencje określono odpowiednio w § 17 i 20 ustawy).

Politykę zagraniczną i stosunki międzynarodowe w zakresie cyberbezpieczeństwa z innymi krajami i organizacjami międzynarodowymi koordynuje Ministerstwo Spraw Zagranicznych we współpracy z NÚKIB. W systemie cyberbezpieczeństwa uczestniczą również służby wywiadowcze. Zgodnie ze swoimi kompetencjami w tym obszarze działają także: Informacyjna Służba Bezpieczeństwa (*Bezpečnostní informační služba*)[20], Wywiad Wojskowy (*Vojenské zpravodajství*)[21] oraz Urząd do Spraw Zagranicznych i Informacji (*Úřad pro zahraniční styky a informace*)[22], które gromadzą, przetwarzają i analizują informacje ważne dla bezpieczeństwa, w tym bezpieczeństwa cybernetycznego Republiki Czeskiej. Policja Republiki Czeskiej (*Policie České republiky*), a w jej ramach Krajowe Centrum ds. Przestępczości Zorganizowanej (*Národní centrála proti organizovanému zločinu*)[23] jest krajowym punktem kontaktowym do spraw cyberprzestępczości oraz krajowym punktem kontaktowym do spraw zgłaszania szkodliwych treści i działań w Internecie.

Zgodnie z informacjami zawartymi w strategii ważnym elementem systemu jest także zapewnienie skutecznej obrony cybernetycznej państwa w sytuacji poważnych zagrożeń bezpieczeństwa cybernetycznego, za którą odpowiedzialny jest w Czechach Wywiad Wojskowy. W obronie cybernetycznej uczestniczy również Armia Republiki Czeskiej (*Armáda ČR*), w szczególności Dowództwo Sił

16 Https://nukib.cz/cs/kyberneticka-bezpecnost/.

17 Rada jest stałym organem rządu do spraw koordynacji kwestii bezpieczeństwa państwa, https://www.vlada.cz/cz/pracovni-a-poradni-organy-vlady/brs/brs-uvod-3851/.

18 Https://www.vlada.cz/cz/ppov/brs/pracovni-vybory/kyberneticka_bezpecnost/vybor-pro-kybernetickou-bezpecnost-159932/ [dostęp 18 stycznia 2021 r.].

19 GovCERT.CZ, https://nukib.cz/en/cyber-security/government-cert/.

20 Https://www.bis.cz/en/.

21 Https://www.vzcr.cz/en.

22 Https://www.uzsi.cz/en/.

23 Https://www.policie.cz/clanek/narodni-centrala-proti-organizovanemu-zlocinu-skpv.aspx.

Cybernetycznych i Operacji Informacyjnych (*Velitelství kybernetických sil a informačních operací*), które działa niezależnie, wspólnie lub we współpracy z jednostkami sił lądowych, powietrznych i specjalnych. Podczas cybernetycznych operacji wojskowych ściśle współpracuje z Wywiadem Wojskowym.

Ponadto w ramach systemu bezpieczeństwa cybernetycznego istotną rolę, obok wyspecjalizowanych jednostek, odgrywają inne organy administracji, w tym Ministerstwo Przemysłu i Handlu (*Ministerstvo průmyslu a obchodu*), Ministerstwo Spraw Wewnętrznych (*Ministerstvo vnitra*) czy Czeski Urząd Telekomunikacji (*Český telekomunikační úřad*).

Estonia

Estonia w roku 2018 zajmowała piąte miejsce na świecie (i czwarte w Europie) w rankingu bezpieczeństwa cybernetycznego przygotowywanym przez Międzynarodowy Związek Telekomunikacyjny (*International Telecommunication Union*, ITU)[24], a także trzecie miejsce na świecie w rankingu bezpieczeństwa cybernetycznego przygotowywanym przez Estońską Akademię e-Governance we współpracy z estońskim Ministerstwem Spraw Zagranicznych. W Estonii swoją siedzibę mają Centrum Doskonalenia Cyberobrony NATO (*NATO Cooperative Cyber Defence Centre of Excellence*, CCDCOE) oraz Europejska Agencja ds. Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi w Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości (eu-LISA).

Podstawą prowadzenia działań w dziedzinie bezpieczeństwa cybernetycznego są w Estonii odpowiednie dokumenty strategiczne. Pierwszą strategię w zakresie cyberbezpieczeństwa przyjęto na lata 2008–2013 i był to jeden z pierwszych dokumentów tego typu na świecie[25]. Kolejna strategia, na lata 2014–2017, stanowiła podstawę dla zwiększenia ochrony infrastruktury krytycznej, walki z cyberprzestępczością czy poprawy zapewnienia bezpieczeństwa informacji. Na podstawie tej strategii przygotowano także środowisko legislacyjne potrzebne dla zapewnienia bezpieczeństwa cybernetycznego, współpracy międzynarodowej i rozwoju sektora bezpieczeństwa cybernetycznego w gospodarce.

Obowiązująca trzecia strategia cyberbezpieczeństwa na lata 2019–2022[26] powstała z wykorzystaniem poprzednich startegii, a jej ogólnym celem jest uznanie bezpieczeństwa cybernetycznego za priorytet dla społeczeństwa estońskiego oraz uzgodnienie i stworzenie warunków dla realizacji kompleksowej polityki sektorowej. W dokumencie zdefiniowano długoterminową wizję i cele działań

---

[24] *Global Cybersecurity Index 2018*, International Telecommunication Union (ITU), https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf.

[25] *Ibidem*, s. 48.

[26] Https://www.mkm.ee/sites/default/files/kyberturvalisuse_strateegia_2022_eng.pdf.

w zakresie cyberbezpieczeństwa, a także wskazano priorytetowe obszary i zadania w tym zakresie jako podstawę planowania działań i przydziału środków. Tak samo jak wcześniejsze strategie, również ta jest strategią horyzontalną i dotyczy wszystkich podmiotów: sektora publicznego (cywilnego i obronnego), głównych usługodawców, przedsiębiorców oraz środowiska akademickiego. W strategii podkreślono jednocześnie, że estońskie społeczeństwo nie jest jeszcze wystarczająco przygotowane, aby odpowiednio reagować na cyberzagrożenia, a w obliczu rozwoju technologii cyfrowych nie jest możliwe uwzględnienie wszystkich zagrożeń w jednym dokumencie strategicznym.

Według założenń przyjętych w strategii koncepcja bezpieczeństwa cybernetycznego jest realizowana zgodnie z czterema podstawowymi zasadami:

- ochrona i propagowanie podstawowych praw i wolności są tak samo istotne w cyberprzestrzeni jak i poza nią,
- bezpieczeństwo cybernetyczne jest czynnikiem stymulującym i wzmacniającym szybki rozwój cyfrowy Estonii, który stanowi podstawę jej wzrostu społeczno-gospodarczego; bezpieczeństwo i innowacyjność muszą się wzajemnie wspierać,
- zapewnienie bezpieczeństwa rozwiązań kryptograficznych jest fundamentem cyfrowego ekosystemu Estonii,
- zasada otwartej komunikacji: przejrzystość i zaufanie publiczne mają fundamentalne znaczenie dla cyfrowego społeczeństwa.

Przyjęto także cztery strategiczne cele, wskazując jednocześnie słabe strony oraz metody realizacji:

- zrównoważone społeczeństwo cyfrowe oparte na stabilnej podstawie technologicznej i przygotowane na ewentualne awarie,
- rozwój przemysłu bezpieczeństwa cybernetycznego, aby był silny, innowacyjny, ukierunkowany na badania naukowe i konkurencyjny w skali światowej,
- Estonia jako wiodący, kompetentny i wiarygodny partner na arenie międzynarodowej,
- „cyberpiśmienne" (*cyber-literate*) społeczeństwo oraz wystarczająca i wzrastająca podaż specjalistów.

W strategii na lata 2019–2022 przedstawiono ponadto zjawiska wpływające na poziom bezpieczeństwa cyfrowego w Estonii (takie jak zwiększenie wykorzystania nowoczesnych technologii, wzrost zależności cyfrowej oraz cyberprzestępczości czy globalna debata na temat cyberbezpieczeństwa), mocne strony Estonii w tej dziedzinie (między innymi bezpieczna infrastruktura społeczeństwa cyfrowego, wpływy na otoczenie międzynarodowe czy zaufanie odbiorcy końcowego do usług cyfrowego państwa) czy stojące przed nią wyzwania (np. ograniczone możliwości specjalizacji, potrzeba stworzenia zintegrowanego przywództwa w dziedzinie cyberbezpieczeństwa).

Strategia cyberbezpieczeństwa ma stworzyć odpowiednie ramy dla zapewnienia bezpieczeństwa cyfrowego oraz współpracy między wszystkimi zaangażowa-

nymi podmiotami. Zasady związane z bezpieczeństwem cybernetycznym są także częściowo wdrożone w ramach innych sektorowych planów, w tym między innymi: „Agendy Cyfrowej 2020”[27], „Planu rozwoju bezpieczeństwa wewnętrznego”[28], „Podstaw polityki kryminalnej do 2030 r.”[29], „Strategii polityki zagranicznej do 2030 r.”[30], „Strategii uczenia się przez całe życie”[31], „Strategii w dziedzinie badań i rozwoju”[32] czy „Estońskiej strategii rozwoju przedsiębiorstw”[33].

W 2018 r. weszła w życie estońska ustawa o bezpieczeństwie cybernetycznym[34], która wdraża do prawodawstwa estońskiego wymogi unijnej dyrektywy NIS, a także rozporządzenia (UE) 2016/679 o ochronie danych osobowych (RODO). W art. 1 określono wymogi dotyczące utrzymania sieci i systemów informatycznych niezbędnych do funkcjonowania społeczeństwa oraz sieci i systemów informatycznych władz państwowych i samorządowych. Ustawa tworzy także podstawy dla zapobiegania incydentom cybernetycznym oraz ich rozwiązywania. W ustawie wskazano obowiązki związane z zapewnieniem bezpieczeństwa cybernetycznego, jakie zostały nałożone na operatorów podstawowych usług (zdefiniowanych w art. 3 ustawy), dotyczące między innymi stosowania odpowiednich środków bezpieczeństwa (opisanych w rozporządzeniu ministra ds. przedsiębiorczości i technologii informacyjnych[35]), przygotowywania ocen ryzyka czy monitorowania systemu. Usługodawcy mają także obowiązek niezwłocznego powiadamiania odpowiednich organów państwowych o wskazanych w ustawie incydentach cybernetycznych. Za naruszenie wymogów związanych z obowiązkami usługodawcom grożą kary finansowe. W ustawie uregulowano również obowiązki organów państwowych i samorządowych oraz dostawców usług informatycznych. Zgodnie z art. 13 ustawy Organ ds. Systemu

---

27 *Digital Agenda 2020 for Estonia*, https://www.mkm.ee/sites/default/files/digitalagenda2020_final_final.pdf.

28 *Internal Security Development Plan* na lata 2015–2020 oraz 2021–2030.

29 *Kriminaalpoliitika põhialused aastani 2030*, dostępny w jęz. estońskim: https://www.just.ee/sites/www.just.ee/files/kriminaalpoliitika_pohialused_aastani_2030.pdf.

30 *Foreign Policy Strategy 2030*, https://vm.ee/sites/default/files/Estonia_for_UN/Rasmus/estonian_foreign_policy_strategy_2030_final.pdf.

31 *Lifelong Learning Strategy 2014–2020*, https://www.hm.ee/sites/default/files/estonian_lifelong_strategy.pdf.

32 *Knowledge-based Estonia, the RD&I Strategy for 2014–2020*, https://www.hm.ee/sites/default/files/estonian_rdi_strategy_2014-2020.pdf?_ga=1.101330693.584123060.1418315820.

33 *Estonian Enterpreneurship Growth Strategy 2014–2020*, https://kasvustrateegia.mkm.ee/index_eng.html.

34 Cybersecurity Act (*Küberturvalisuse seadus*), RT I, 22 maja 2018 r., 1, dostępna w jęz. angielskim: https://www.riigiteataja.ee/en/eli/523052018003/consolide.

35 Dostępne w jęz. estońskim: *Võrgu- ja infosüsteemide riskianalüüsi nõuded ning turvameetmete kirjeldus*, RT I, 10 lipca 2018, 6, https://www.riigiteataja.ee/akt/110072018006.

Informacyjnego (*Riigi infosüsteemi ameti*, RIA) odpowiada za rejestr incydentów cybernetycznych, do którego wprowadza się dane w celu tworzenia ewidencji incydentów cybernetycznych i ich analizowania pod kątem szukania rozwiązań, przekazywania ostrzeżeń i podejmowania działań nadzorczych. W rozdziale 4 ustawy określono obowiązki związane z nadzorem państwowym i administracyjnym, nałożone przede wszystkim na ISA.

Analizą i oceną sytuacji w zakresie bezpieczeństwa narodowego zajmuje się w Estonii rządowy Komitet Bezpieczeństwa (*Vabariigi Valitsuse julgeolekukomisjoni*), który koordynuje działania organów władzy wykonawczej w dziedzinie obrony narodowej[36]. Komitetowi przewodniczy premier, a w skład wchodzą wybrani ministrowie. W 2009 r. przy Komitecie Bezpieczeństwa utworzono Radę Bezpieczeństwa Cybernetycznego (*Küberjulgeoleku nõukogu*), która prowadzi nadzór nad realizacją celów strategii cyberbezpieczeństwa i współpracą między różnymi zaangażowanymi instytucjami. Przewodniczącym Rady jest sekretarz generalny Ministerstwa Spraw Gospodarczych i Komunikacji. W realizację polityki bezpieczeństwa cybernetycznego zaangażowana jest także Kancelaria Rządu Estonii (*Riigikantselei*), która zapewnia włączenie cyberbezpieczeństwa do dokumentów strategicznych obronności kraju.

Opracowaniem i koordynacją polityki bezpieczeństwa cybernetycznego oraz wdrażaniem strategii cyberbezpieczeństwa zajmuje się Ministerstwo Spraw Gospodarczych i Komunikacji. Ministerstwo odpowiada także za współpracę organów państwowych z pozostałymi zaangażowanymi stronami oraz społeczeństwem Estonii. Ponadto w realizację strategii są zaangażowane inne ministerstwa (ds. edukacji, sprawiedliwości, obrony, spraw wewnętrznych, spraw zagranicznych czy finansów) oraz rządowe agencje[37]:

- Urząd Nadzoru Technicznego (*Technical Surveillance Authority*, TJA) – odpowiedzialny za promowanie bezpieczeństwa i wiarygodności sprzętu łączności elektronicznej oraz nadzór nad dostawcami usług certyfikacyjnych i związanych z oznaczaniem czasu,
- Estońska Fundacja Internetowa (*Estonian Internet Foundation*, EIS) – reprezentująca estońską społeczność internetową i administrująca domeną ee,
- Państwowa Fundacja Infokomunikacyjna (*State Infocommunication Foundation*, RIKS) – zapewniająca jakość, ciągłość, bezpieczeństwo i efektywność kosztową komunikacji informacyjnej i usług infrastrukturalnych państwa (np. rządowej chmury),

---

[36] Informacja na podstawie: *National Cyber Security in practice*, e-Governance Academy, Tallinn 2020, https://ega.ee/wp-content/uploads/2020/05/Kuberturvalisuse_kasiraamat_ENG.pdf.

[37] Informacje na podstawie odpowiedzi udzielonej przez parlament estoński na pytanie zadane w ramach ECPRD: *Organization of cyber/information security*, ECPRD Request No. 4217, listopad 2019.

- *Enterprise Estonia* i *Startup Estonia* – przyczyniające się do rozwoju przedsiębiorczości i innowacyjności.

Za zarządzanie działaniami związanymi z zapewnieniem bezpieczeństwa informacji oraz z incydentami cybernetycznymi, które mają miejsce w estońskich sieciach komputerowych, odpowiada Organ ds. Systemu Informacyjnego. Jego zadaniem jest zwłaszcza zapewnienie bezpieczeństwa wszystkich sieci i systemów informatycznych niezbędnych do funkcjonowania państwa. W ramach RIA istnieje również dział ds. reagowania na incydenty związane z bezpieczeństwem cybernetycznym (CERT-EE), który stale monitoruje estońską cyberprzestrzeń i zajmuje się rozwiązywaniem incydentów cybernetycznych. Na stronie internetowej RIA publikowane są także roczne i kwartalne sprawozdania i oceny działań w dziedzinie cyberbezpieczeństwa Estonii[38].

Od 2018 r. działa Estońskie Stowarzyszenie Bezpieczeństwa Informacji (*Estonian Information Security Association*, EISA), które wspiera i stymuluje współpracę między sektorem prywatnym a środowiskiem akademickim oraz rządem (w tym w ramach partnerstwa publiczno-prywatnego) w zakresie bezpieczeństwa cybernetycznego[39].

Francja

Zgodnie z art. L111-1 francuskiego Kodeksu bezpieczeństwa wewnętrznego[40] państwo ma obowiązek zapewnić bezpieczeństwo, gwarantując na całym terytorium obronę instytucji i interesów narodowych, poszanowanie prawa, utrzymanie pokoju i porządku dla ochrony ludzi i mienia. Wymóg bezpieczeństwa rozciąga się również na cyberprzestrzeń, w której funkcjonuje całe społeczeństwo.

Ewolucja systemu bezpieczeństwa cybernetycznego we Francji została zapoczątkowana opracowaniem w 2008 r. białej księgi określającej podstawowe cele i założenia polityczne w obszarze cyberbezpieczeństwa. Późniejsze dokumenty programowe, takie jak: „Strategia Francji w zakresie ochrony i bezpieczeństwa systemów informacji" (2011)[41] czy „Krajowa strategia bezpieczeństwa cyfrowego" (2015)[42], doprowadziły do uporządkowania organizacyjnego i legislacyjnego

---

38 Dostępne także w jęz. angielskim na stronie RIA: https://www.ria.ee/en/information-system-authority/publications.html.

39 *Global Cybersecurity Index 2018*, *op. cit.*, s. 48.

40 *Code de la sécurité intérieure*, https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000025504921/.

41 *Défense et sécurité des systèmes d'information – Stratégie de la France*, www.ssi.gouv.fr/uploads/IMG/pdf/2011-02-15_Defense_et_securite_des_systemes_d_information_strategie_de_la_France.pdf.

42 *Stratégie nationale pour la sécurité du numérique*, https://www.ssi.gouv.fr/en/cybersecurity-in-france/.

systemu francuskiego cyberbezpieczeństwa. Rosnące współzależności między sferami gospodarki i informatyki sprawiły, że bezpieczeństwo sieci informatycznych jest jednym z narodowych priorytetów Francji.

Jednym z wymogów transpozycji dyrektywy NIS było uchwalenie strategii bezpieczeństwa cyfrowego. Taki dokument został we Francji przyjęty już wcześniej, 16 października 2015 r., i była to „Krajowa strategia bezpieczeństwa cyfrowego"[43]. Została ona opracowana w związku z narastającym zagrożeniem terrorystycznym. Strategia ma na celu wspieranie cyfrowej transformacji francuskiego społeczeństwa i stawianie czoła nowym wyzwaniom związanym ze zmieniającymi się zastosowaniami technologii cyfrowych i związanymi z nimi zagrożeniami[44]. Dokument koncentruje się na pięciu celach:

- zagwarantowanie suwerenności narodowej i zapewnienie bezpieczeństwa infrastruktury krytycznej w przypadku poważnego ataku cybernetycznego,
- reagowanie na akty cyberprzestępczości – działanie to ma celu uczynienie cyberprzestrzeni miejscem zaufania; w strategii deklaruje się podjęcie środków mających na celu ochronę obywateli w przestrzeni internetowej, w tym ich danych osobowych, które mogą być w niewłaściwy sposób wykorzystane,
- informowanie opinii publicznej; poczynając od edukacji szkolnej, zgodnie z celami przyjętymi w strategii, Francja będzie działała na rzecz budowania świadomości i kompetencji społecznych w zakresie cyberbezpieczeństwa,
- uczynienie z bezpieczeństwa cyfrowego przewagi konkurencyjnej dla firm; w tym celu deklaruje się pomoc dla francuskich firm w dostarczeniu najlepszych produktów i usług związanych z bezpieczeństwem cybernetycznym; ponadto w ramach tego działania będą prowadzone prace na rzecz zwiększenia odporności sektora prywatnego na potencjalne ataki cybernetyczne,
- wzmocnienie obecności Francji na arenie międzynarodowej w promowaniu bezpiecznej, stabilnej i otwartej cyberprzestrzeni; utworzenie europejskiej strategicznej autonomii cyfrowej we współpracy z innymi państwami.

Pozostałe przepisy dyrektywy w sprawie bezpieczeństwa sieci i informacji przyjętej przez Unię Europejską 6 lipca 2016 r. były już wcześniej uwzględnione w ustawie o programowaniu wojskowym nr 2013-1168 z 18 grudnia 2013 r.[45]. Zgodnie z tym aktem państwo ma obowiązek i jest odpowiedzialne za podjęcie odpowiednich środków w celu ochrony istotnych sektorów, które uznaje

[43] *La stratégie nationale pour la sécurité du numérique: une réponse aux nouveaux enjeux des usages numériques*, https://www.ssi.gouv.fr/actualite/la-strategie-nationale-pour-la-securite-du-numerique-une-reponse-aux-nouveaux-enjeux-des-usages-numeriques/.

[44] D. Altersitz, C. Bernier, F. Aza, *Cybersecurity in France*, https://www.lexology.com/library/detail.aspx?g=a412035f-b3af-4fd1-a6f2-17e7c97efd7f.

[45] *Loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale*.

się za mające kluczowe znaczenie dla przetrwania państwa, takich jak banki, szpitale i elektrownie jądrowe. W myśl ustawy premier określa główne kierunki polityczne i koordynuje działania rządu w zakresie bezpieczeństwa i obrony systemów informatycznych. Dekrety towarzyszące tej ustawie to dekret nr 2015-350 z 27 marca 2015 r. o kwalifikacji urządzeń bezpieczeństwa i dostawców usług zaufania na potrzeby bezpieczeństwa narodowego[46] i dekret 2015-351 z 27 marca 2015 r. o bezpieczeństwie systemów informatycznych operatorów o kluczowym znaczeniu[47].

Całościowo transpozycję dyrektywy NIS dokonano przez ustawę z 26 lutego 2018 r. nr 2018-133[48] i dekret nr 2018-384 opublikowany 23 maja 2018 r.[49].

Na mocy dekretów sektory, które uznaje się za mające podstawowe znaczenie dla przetrwania państwa (m.in. sądy, wojsko, przemysł spożywczy, elektroniczny, audiowizualny, kosmiczny i badawczy oraz sektor finansowy), są zobowiązane do:

- posiadania narzędzi do wykrywania zdarzeń zagrażających bezpieczeństwu cybernetycznemu w sieciach informatycznych,
- niezwłocznego powiadamiania właściwych organów o każdym naruszeniu bezpieczeństwa cybernetycznego,
- regularnych kontroli infrastruktury informatycznej,
- przyjęcia odpowiednich środków w celu ochrony na polecenie odpowiednich organów. Według ustawy o programowaniu wojskowym w przypadku naruszenia przepisów dotyczących bezpieczeństwa cybernetycznego przez operatorów o kluczowym znaczeniu (*opérateur d'importance vitale*, OIV), może grozić grzywna do wysokości 150 000 euro.

Przed wejściem w życie ogólnego rozporządzenia UE w sprawie ochrony danych w ustawie z 1978 r. o ochronie danych (zmienionej ustawą nr 2018-493 z 20 czerwca 2018 r.) uwzględniono bezpieczeństwo cybernetyczne, zapewniając, że w odniesieniu do danych osobowych administratorzy danych i podmioty je przetwarzające są zobowiązani do wdrożenia odpowiednich środków technicznych i organizacyjnych w celu zapewnienia odpowiedniego poziomu

---

[46] *Décret n° 2015-350 du 27 mars 2015 relatif à la qualification des produits de sécurité et des prestataires de service de confiance pour les besoins de la sécurité des systèmes d'information.*

[47] *Décret n° 2015-351 du 27 mars 2015 relatif à la sécurité des systèmes d'information des opérateurs d'importance vitale et pris pour l'application de la section 2 du chapitre II du titre III du livre III de la première partie de la partie législative du code de la defense*, https://www.legifrance.gouv.fr/loda/id/JORFTEXT000030405967/2021-01-14/.

[48] *Loi n° 2018-133 du 26 février 2018 portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité*, https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000036644772/.

[49] *Décret n° 2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique*, https://www.legifrance.gouv.fr/jorf/article_jo/JORFARTI000036940025?r=17Er4OuIVi.

bezpieczeństwa. Dostawcy usług cyfrowych (ISP) powinni zapewnić poziom bezpieczeństwa współmierny do stopnia ryzyka, na jakie narażone jest bezpieczeństwo świadczonych przez nich usług cyfrowych. Obejmują one ochronę przed nieautoryzowanym dostępem, zmianą lub kradzieżą. Ponadto dostawcy usług cyfrowych przetwarzający dane osobowe są zobowiązani do natychmiastowego poinformowania francuskiego Urzędu Ochrony Danych (CNIL) o przypadkach naruszenia. Dostawcy usług cyfrowych mają obowiązek prowadzenia rejestrów ataków cybernetycznych. Zgodnie z ogólnym rozporządzeniem UE o ochronie danych, mającym zastosowanie od 25 maja 2018 r., obowiązki te zostały rozszerzone na wszystkich administratorów danych i podmiotów przetwarzających dane zarówno prywatne, jak i publiczne. Od momentu wejścia w życie ogólnego rozporządzenia UE w sprawie ochrony danych administratorzy danych i osoby je przetwarzające w przypadku nieprzedstawienia sprawozdania i przyjęcia odpowiednich środków bezpieczeństwa zagrożeni są grzywną administracyjną w wysokości do 2% całkowitego rocznego obrotu lub 10 mln euro, w zależności od tego, która z tych kwot jest wyższa. Przepisy rozporządzenia UE w sprawie ochrony danych zostały transponowane do prawa francuskiego na mocy ustawy nr 2018-493 z 20 czerwca 2018 r.[50].

Zadania w zakresie cyberbezpieczeństwa są realizowane zarówno przez podmioty cywilne, jak i wojskowe. Zgodnie z wymogami dyrektywy NIS państwa członkowskie miały obowiązek wyznaczenia organów krajowych, którym powierzone zostaną zadania związane z cyberbezpieczeństwem. Funkcję tę we Francji spełnia powołana na mocy dekretu nr 2009-834 z 7 lipca 2009 r.[51] Narodowa Agencja Bezpieczeństwa Systemów Informatycznych (*Agence Nationale de la Sécurité des Systèmes d'Information*, ANSSI). Organ ten działa przy Sekretarzu Generalnym Obrony i Bezpieczeństwa Narodowego. ANSSI jest odpowiedzialna za podejmowanie działań w sytuacjach nadzwyczajnych w celu zapewnienia ochrony krytycznej infrastruktury teleinformatycznej oraz za wskazywanie środków, jakie operatorzy muszą wprowadzać w odpowiedzi na sytuację kryzysową. W tym celu przedkłada ona premierowi propozycje działań zmierzających do reagowania na sytuacje kryzysowe i zagrożenia bezpieczeństwa systemów wykorzystywanych przez organy publiczne, operatorów infrastruktury krytycznej, a także koordynuje, w ramach określonych przez premiera wytycznych, działania rządu w powyższym zakresie. Ponadto Agencja pełni funkcję głównego punktu kontaktowego dla operatorów o kluczowym znaczeniu, którzy są zobowiązani do zgłaszania jej

[50] *Loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles*, https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000037085952/ [dostęp 14 stycznia 2010 r.].

[51] *Décret n° 2009-834 du 7 juillet 2009 portant creation d'un service a competence nationale dénommé „Agence nationale de la sécurité des systèmes d'information"*, www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000020828212.

incydentów w zakresie bezpieczeństwa. Zadania w sferze cyberbezpieczeństwa realizowane są także przez Sztab Generalny Sił Zbrojnych (*État major des armées*, EMA), Generalną Dyrekcję Uzbrojenia (*Direction Générale de l'armement*, DGA) oraz w zakresie wywiadu elektronicznego – Generalną Dyrekcję Bezpieczeństwa Zewnętrznego (*Direction Générale de la Sécurité Extérieure*, DGSE).

Holandia

Obowiązujący w Holandii system cyberbezpieczeństwa opiera się przede wszystkim na aktach prawnych implementujących do prawa krajowego dyrektywę NIS. Jednak system cyberbezpieczeństwa i instytucje właściwe w tym zakresie funkcjonowały przed implementacją dyrektywy – na przykład pierwsza krajowa strategia w zakresie cyberbezpieczeństwa została przyjęta w 2011 r., zaś Krajowe Centrum Cyberbezpieczeństwa zostało utworzone w 2012 r. Implementacja dyrektywy NIS wprowadziła do holenderskiego systemu cyberbezpieczeństwa pewne nowe rozwiązania prawne, lecz zręby regulacyjne i instytucjonalne systemu powstały wcześniej.

Ustawa o bezpieczeństwie sieci i systemów informacyjnych z 17 października 2018 r. [*Wet van 17 oktober 2018, houdende regels ter implementatie van richtlijn (EU) 2016/1148, (Wet beveiliging netwerk- en informatiesystemen)*, WBNI][52] to akt prawny implementujący dyrektywę NIS do krajowego porządku prawnego[53]. Ustawa weszła w życie 9 listopada 2018 r.

Ustawa o bezpieczeństwie sieci i systemów informacyjnych nakłada na Ministra Sprawiedliwości i Bezpieczeństwa (*Ministerie van Justitie en Veiligheid*) obowiązek rozwoju i ochrony bezpieczeństwa sieci i systemów informacyjnych o kluczowym znaczeniu dla społeczeństwa, w tym systemów informacyjnych instytucji publicznych. Na podstawie zarządzenia (*Organisatiebesluit Ministerie van Justitie en Veiligheid van 02/05/2019*)[54] minister powierzył te zadania Krajowemu Centrum Cyberbezpieczeństwa (*Nationaal Cyber Security Centrum-Nederlanden*, NCSC-NL)[55]. NCSC-NL to główna krajowa instytucja w dziedzinie cyberbezpieczeństwa.

---

[52] Https://wetten.overheid.nl/BWBR0041515/2020-07-15.

[53] *Implementation of the NIS Directive in The Netherlands*, https://ec.europa.eu/digital-single-market/en/implementation-nis-directive-netherlands; *NIS Implementation Tracker*, https://www.digitaleurope.org/resources/nis-implementation-tracker/; *Cyber Security*, https://cms.law/en/int/publication/data-law-navigator/the-netherlands; *Cybersecurity Legislation in the Netherlands*, https://tedangevaare.nl/nl/.

[54] Https://wetten.overheid.nl/BWBR0040293/2019-05-02#Hoofdstuk9a.

[55] *NCSC-NL. Statutory task*, https://english.ncsc.nl/about-the-ncsc/statutory-task; *Operational Framework NCSC-NL*, https://english.ncsc.nl/publications/publications/2019/juli/02/operational-framework-and-rfc2350.

Zgodnie z art. 63h.1 i art. 63h. 2 rozporządzenia ministra, w celu ograniczenia i zapobiegania nieprawidłowościom w życiu społecznym spowodowanym przez zagrożenia bezpieczeństwa sieci oraz w celu poprawy odporności systemów informacyjnych, NCSC-NL odpowiada za:

- informowanie, doradzanie i wspieranie instytucji państwowych oraz operatorów usług kluczowych w przypadku incydentów dotyczących bezpieczeństwa sieci i systemów informacyjnych,
- informowanie innych podmiotów o incydentach dotyczących bezpieczeństwa sieci i systemów informacyjnych,
- prowadzenie analiz i dochodzeń technicznych dotyczących bezpieczeństwa sieci i systemów informacyjnych,
- upowszechnianie wiedzy uzyskanej dzięki przeprowadzonym analizom i dochodzeniom technicznym,
- realizację zadań pojedynczego punktu kontaktowego,
- promowanie partnerstwa publiczno-prywatnego w zakresie cyberbezpieczeństwa.

Struktura organizacyjna NCSC-NL zakłada funkcjonowanie czterech jednostek organizacyjnych: wydziału ds. operacyjnych; wydziału współpracy i wymiany informacji; wydziału działań informacyjnych i technologii; wydziału organizacyjnego.

Jak stanowi dyrektywa NIS, państwa członkowskie UE są obowiązane ustanowić Pojedynczy Punkt Kontaktowy (*Single Point of Contact*). Ustawa o bezpieczeństwie sieci i systemów informacyjnych stanowi, że właściwy w tym zakresie jest Minister Sprawiedliwości i Bezpieczeństwa, który może powierzyć te zadania właściwej instytucji. Na podstawie przywołanego wcześniej rozporządzenia minister powierzył te kompetencje NCSC-NL.

W dyrektywie NIS ustanowiono sieć CSIRT. Zgodnie z ustawą o bezpieczeństwie sieci i systemów informacyjnych funkcję CSIRT pełni Minister Sprawiedliwości i Bezpieczeństwa, który może powierzyć kompetencje właściwej instytucji. Na podstawie przywołanego wcześniej rozporządzenia Minister powierzył te zadania NCSC-NL.

Jeśli chodzi o zakres podmiotowy, ustawa o bezpieczeństwie sieci i systemów informacyjnych powtarza postanowienia dyrektywy NIS, wprowadzając kategorie operatorów usług kluczowych i dostawców usług cyfrowych. Operatorzy usług kluczowych (*aanbieders van essentiële diensten*) to podmioty sektora publicznego lub prywatnego, które dostarczają kluczowe usługi zależne od systemów informacyjnych, w przypadku których potencjalne zagrożenia bezpieczeństwa sieci mogą mieć istotny skutek zakłócający możliwość świadczenia usługi. Operatorzy usług kluczowych są obowiązani bezzwłocznie zgłaszać incydenty istotnie zagrażające ciągłości świadczenia przez nich usług do NCSC-NL oraz organu właściwego ds. bezpieczeństwa sieci i informacji. Zgodnie z postanowieniami dyrektywy NIS określono odrębne organy właściwe dla poszczególnych sektorów:

dla sektora bankowego jest to De Nederlandsche Bank, dla sektora energetycznego i cyfrowego – Agencja ds. Komunikacji Radiowej, jednostka organizacyjna Ministerstwa Gospodarki i Klimatu (Agentschap Telecom), dla zaopatrzenia w wodę – Ministerstwo Infrastruktury i Zasobów Wodnych. Na operatora usług kluczowych, który nie zgłosi incydentu, może zostać nałożona grzywna w wysokości do 1 mln euro. Odnośnie do dostawców usług cyfrowych organem właściwym ds. bezpieczeństwa sieci i informacji jest Agencja ds. Komunikacji Radiowej, jednostka organizacyjna Ministerstwa Gospodarki i Klimatu.

Dyrektywa NIS zobowiązuje państwa członkowskie UE do przyjęcia i wdrożenia krajowych strategii w zakresie bezpieczeństwa sieci i systemów informacyjnych. W Holandii obowiązuje „Krajowa strategia cyberbezpieczeństwa" z 2018 r.[56]. Ten dokument jako cele wyznacza możliwość korzystania w bezpieczny sposób z gospodarczych i społecznych korzyści cyfryzacji oraz ochronę bezpieczeństwa narodowego w przestrzeni cyfrowej. W związku z tym wyznaczono siedem kluczowych zagadnień:

- odpowiednie możliwości wykrywania, ograniczania i reagowania na zagrożenia,
- działanie na rzecz międzynarodowego pokoju i bezpieczeństwa w przestrzeni cyfrowej,
- zaangażowanie w rozwój bezpiecznego sprzętu i oprogramowania,
- tworzenie odpornej infrastruktury cyfrowej i procedur w przestrzeni cyfrowej,
- zwalczanie cyberprzestępczości,
- rozwój wiedzy w zakresie cyberbezpieczeństwa,
- współpraca sektora publicznego i prywatnego na rzecz cyberbezpieczeństwa.

Corocznie sporządza się „Przegląd strategii cyberbezpieczeństwa"[57]. Przegląd opracowuje NCSC-NL we współpracy z Krajowym Koordynatorem ds. Bezpieczeństwa i Zwalczania Terroryzmu[58] przy Ministrze Sprawiedliwości i Bezpieczeństwa. Przegląd zawiera analizę bieżących wyzwań w zakresie cyberbezpieczeństwa oraz rekomendacje, których wdrożenie ma przyczynić się do poprawy bezpieczeństwa i odporności sieci i systemów informacyjnych.

Niemcy

W Niemczech na poziomie federalnym najważniejsze rozwiązania legislacyjne przewidziane w dyrektywie NIS zostały zawarte w ustawie o zwiększeniu bezpie-

---

[56] *National Cyber Security Agenda. A cyber secure Netherlands*, https://www.enisa.europa.eu/news/member-states/CSAgenda_EN.pdf.

[57] *Cyber Security Assessment Netherlands 2020*, https://english.nctv.nl/documents/publications/2020/08/28/cyber-security-assessment-netherlands-2020.

[58] *National Coordinator for Security and Counterterrorism*, https://english.nctv.nl/organisation.

czeństwa systemów informatycznych IT (*Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme, ITSicherheitsgesetz*)[59], którą Bundestag uchwalił 17 lipca 2015 r., a także w uchwalonej 14 sierpnia 2009 r. ustawie o Federalnym Urzędzie Bezpieczeństwa Teleinformatycznego[60] (*Gesetz über das Bundesamt für Sicherheit in der Informationstechnik*, BSI-Gesetz)[61].

W związku z tym po przyjęciu dyrektywy NIS w Niemczech pojawiła się potrzeba stosunkowo niewielkich zmian w prawie federalnym[62]. Odpowiednie przepisy przyjęto na podstawie uchwalonej 27 kwietnia 2017 r. ustawy wdrażającej dyrektywę UE 2016/1148 w sprawie środków zapewniających wysoki poziom wspólnego bezpieczeństwa sieci i informacji w Unii (*Gesetz zur Umsetzung der EU-Richtlinie 2016/1148 „über Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der Union"*, NIS-RL)[63].

W wyniku przyjęcia ustawy NIS-RL zmianie uległy przepisy dotyczące Federalnego Urzędu Bezpieczeństwa Teleinformatycznego oraz niektórych gałęzi tzw. infrastruktury krytycznej (opisane w ustawach: AtG[64], EnWG[65], SGB V[66]),

---

[59] Https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl115s1324.pdf#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl115s1324.pdf%27%5D__1610974497797; https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/IT-Sicherheitsgesetz.pdf?__blob=publicationFile&v=7.

[60] Urząd ten jest właściwy do bezpieczeństwa informatycznego na poziomie federalnym. Podlega Federalnemu Ministerstwu właściwemu dla spraw wewnętrznych (BSIG, § 1); dalej: Urząd Federalny (*Bundesamt*). Więcej na temat zakresu zadań tego urzędu do 2017 r. w dokumentach BAS: A. Warchoł, *Cyberbezpieczeństwo w kontekście wojny informacyjnej – jakie są rozwiązania w Holandii i Niemczech?*, BAS-1424/19; D. Dziewulak, D. Łukasz, M. Mróz, *Informacja na temat informatyzacji państwa i cyberbezpieczeństwa we Francji i Niemczech*, BAS-ZSP-1713/17.

[61] Https://www.gesetze-im-internet.de/bsig_2009/BSIG.pdf.

[62] Kwestie te omówiono m.in. w następujących publikacjach: https://www.cr-online.de/blog/2017/05/14/it-sicherheit-bundestag-verabschiedet-nis-umsetzungsgesetz/; https://community.beck.de/2017/05/10/neue-europaeische-vorgaben-zur-cybersicherheit-der-bundestag-beschliesst-das-umsetzungsgesetz-zur-nis-rl-der.

[63] Https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&start=//*[@attr_id=%27bgbl117s1885.pdf%27]#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl117s1885.pdf%27%5D__1611137078166.

[64] Ustawa o pokojowym wykorzystaniu energii jądrowej i ochronie przed jej zagrożeniami (*Gesetz über die friedliche Verwendung der Kernenergie und den Schutz gegen ihre Gefahren*, AtG), https://www.gesetze-im-internet.de/atg.

[65] Ustawa o dostawach energii elektrycznej i gazu (*Gesetz über die Elektrizitäts- und Gasversorgung*, EnWG), https://www.gesetze-im-internet.de/enwg_2005.

[66] Kodeks cywilny (SGB) Księga Piąta (V) – Ustawowe ubezpieczenie zdrowotne (*Sozialgesetzbuch (SGB) Fünftes Buch (V) – Gesetzliche Krankenversicherung*, SGB V), https://www.gesetze-im-internet.de/sgb_5.

regulacje dotyczące CSIRT[67], a także specjalne regulacje dla dostawców usług cyfrowych zawarte w ustawie BSI-Gesetz czy ustawa o Służbie Kontrwywiadu Wojskowego[68].

Zgodnie z ustawą NIS-RL przede wszystkim poszerzono zakres działań Urzędu Federalnego. Obecnie urząd wspierać ma nie tylko organy ochrony konstytucji, ale także Służbę Kontrwywiadu Wojskowego (*Militärische Abschirmdienst*, MAGD) w zakresie cyberzagrożeń o podłożu terrorystycznym lub wywiadowczym, zwłaszcza w obszarze działalności niemieckiego ministerstwa odpowiedniego ds. obrony. W tym celu ustawą NIS-RL zmieniono odpowiednie przepisy między innymi w § 3 i § 5 BSI-Gesetz. Na ich podstawie rozpoczęto tworzenie rozszerzonych uprawnień do przesyłania danych osobowych (są one stosowane m.in. również w przypadku działań stanowiących zagrożenie dla bezpieczeństwa w obszarze biznesowym).

Zgodnie z dodanym ustawą NIS-RL § 5a BSI-Gesetz (*Przywracanie bezpieczeństwa lub funkcjonalności systemów informatycznych*), Urząd Federalny uzyskał nowe uprawnienia. Zgodnie z § 5a ust. (1) BSI-Gesetz w sytuacji naruszenia bezpieczeństwa lub funkcjonalności systemu informatycznego agencji federalnej lub operatora infrastruktury krytycznej, Urząd Federalny może na wniosek zainteresowanej agencji lub operatora (wnioskodawcy) podjąć działania niezbędne do przywrócenia bezpieczeństwa lub funkcjonalności danego systemu informatycznego[69]. Jeśli Urząd Federalny podejmie wstępne kroki w celu ograniczenia szkód i zapewnienia awaryjnego działania systemu na miejscu, za działalność Urzędu Federalnego nie będą naliczane żadne opłaty ani inne należności.

Zgodnie z § 5a ust. (3) BSI-Gesetz w przypadku środków przewidzianych w § 5a ust. (1) BSI-Gesetz Urząd Federalny może gromadzić i przetwarzać dane osobowe lub dane objęte tajemnicą telekomunikacyjną, o ile jest to konieczne i właściwe dla przywrócenia bezpieczeństwa lub funkcjonalności danego sy-

---

[67] Od 1 września 2001 r. zadania związane z bezpieczeństwem informatycznym w Niemczech zostały podjęte przez CERT-Bund, który został ustanowiony przez ówczesny Federalny Urząd Bezpieczeństwa Informacji. Bezpieczeństwo informatyczne administracji publicznej w Niemczech jest zorganizowane w ramach Stowarzyszenia Administracyjnego CERT (*Verwaltungs-CERT-Verbund*, VCV), zarówno na szczeblu federalnym, jak i krajowym (a w niektórych wypadkach też komunalnym). Urząd Federalny oferuje również odpowiednią usługę dla osób prywatnych z „Citizen CERT". Odpowiednie rozwiązania zastosowano też w sektorze bankowym, w związku z czym powołano m.in. S-CERT, CERT *Sparkassen-Finanzgruppe* (2001 r.).

[68] Ustawa o Służbie Kontrwywiadu Wojskowego (*Gesetz über den Militärischen Abschirmdienst*, MADG), https://www.gesetze-im-internet.de/madg.

[69] Na podstawie m.in. tych przepisów w Niemczech działają obecnie mobilne zespoły reagowania na incydenty (*Mobile Incident Response Teams*, MIRTs), https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2018.pdf?__blob=publicationFile&v=3.

stemu informatycznego. Dane należy natychmiast usunąć, gdy tylko przestaną być potrzebne do tych celów. Jeżeli dane zostały przekazane innemu organowi w przypadkach określonych w § 5a ust. (4) BSI-Gesetz w celu wykonania jego ustawowych zadań, Urząd Federalny może (w drodze wyjątku) dalej przetwarzać dane do czasu zakończenia wsparcia tych organów. Używanie do innych celów jest niedozwolone, a w innych przypadkach należy zastosować przepisy federalnej ustawy o ochronie danych (*Bundesdatenschutzgesetzes*, BDSG[70]). W praktyce oznacza to, że oprócz operatorów infrastruktury krytycznej (KRITIS)[71] także dostawcy usług cyfrowych (usług internetowych, wyszukiwarek internetowych i chmur, usług obliczeniowych) będą musieli zgłaszać do Urzędu Fedralnego[72] incydenty o istotnych skutkach dla bezpieczeństwa.

Zgodnie z § 5a ust. (4) BSI-Gesetz Urząd Federalny może przekazywać informacje wyłącznie za zgodą wnioskodawcy, chyba że dane te nie pozwalają na wyciągnięcie jakichkolwiek wniosków dotyczących tożsamości osób trzecich lub są zgodne z § 5 ust. (5) i (6) BSI-Gesetz. Dostęp do akt przechowywanych na podstawie § 5a ust. (1) BSI-Gesetz nie jest udzielany osobom trzecim.

Na podstawie § 5a ust. (5) BSI-Gesetz za zgodą wnioskodawcy Urząd Federalny może skorzystać z pomocy wykwalifikowanych osób trzecich w zakresie środków określonych w § 5a ust. (1) BSI-Gesetz, jeśli jest to konieczne do terminowego lub całkowitego przywrócenia bezpieczeństwa lub funkcjonalności danego systemu informatycznego. Osoba zgłaszająca wniosek ponosi wynikające z tego koszty. Urząd Federalny może również skierować wnioskodawcę do wykwalifikowanej osoby trzeciej. Urząd Federalny i osoby trzecie na zlecenie wnioskodawcy lub Urzędu Federalnego zgodnie z § 5a ust. (1) BSI-Gesetz mogą przekazywać sobie nawzajem dane w przypadku środków określonych w ust. (1) za zgodą wnioskodawcy.

Zgodnie z § 5a ust. (6) BSI-Gesetz w zakresie, w jakim jest to konieczne do przywrócenia bezpieczeństwa lub funkcjonalności systemu informatycznego, Urząd Federalny może zwrócić się do producenta systemu informatycznego o pomoc w przywróceniu bezpieczeństwa lub funkcjonalności tego systemu.

Na podstawie § 5a ust. (7) BSI-Gesetz, w uzasadnionych przypadkach indywidualnych, Urząd Federalny może również współpracować z innymi instytucjami niż wymienione w ust. (1), jeżeli jest to niezbędne i jeżeli jest to przypadek szczególny.

Zgodnie z § 5a ust. (8) BSI-Gesetz w przypadku instalacji lub działań, które wymagają zezwolenia na podstawie ustawy o energii atomowej, w przypadkach

---

70 Https://www.gesetze-im-internet.de/bdsg_2018/BJNR209710017.html.

71 Https://www.da-rz.de/de/glossary/betreiber-kritischer-infrastrukturen-kritis-betreiber/.

72 Https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2018.pdf?__blob=publicationFile&v=3.

określonych w § 5a ust. 1, 4, 5 i 7 BSI-Gesetz, przed podjęciem działań przez Urząd Federalny, należy powołać odpowiednie organy nadzoru jądrowego rządu federalnego i rządów landów.

W odniesieniu do operatorów usług kluczowych w ustawie BSI-Gesetz ustawą NIS-RL dodano § 8a, w którym zapisano, że Urząd Federalny może zażądać przedłożenia dokumentacji, na której oparto ocenę operatorów usług kluczowych. W przypadku braków w zakresie bezpieczeństwa Urząd Federalny może zażądać ich usunięcia w porozumieniu z odpowiedzialnym federalnym organem nadzorczym lub w porozumieniu z innym odpowiedzialnym organem nadzorczym. Zgodnie z § 8a ust. (4) BSI-Gesetz Urząd Federalny może sprawdzić, czy operator infrastruktury kluczowej spełnia wymagania § 8a ust. (1) BSI-Gesetz[73]. Operator infrastruktury kluczowej musi zezwolić urzędowi federalnemu i osobom działającym w jego imieniu na wejście do pomieszczeń biznesowych i operacyjnych w celu przeprowadzenia inspekcji w normalnych godzinach pracy oraz – na żądanie – na dostęp do odpowiednich zapisów, dokumentów i danych, udzielić informacji i zapewnić niezbędne wsparcie. Urząd Federalny obciąża danego operatora opłatami za infrastrukturę kluczową i wydatkami za przegląd tylko wtedy, gdy Urząd Federalny działał na podstawie przesłanek uzasadniających wątpliwości co do zgodności z wymogami określonymi w § 8a ust. (1) BSI-Gesetz.

Zgodnie z § 8b BSI-Gesetz operatorzy infrastruktury kluczowej (krytycznej)[74] muszą niezwłocznie zgłaszać do Urzędu Federalnego za pośrednictwem CSIRT następujące usterki:

- zakłócenia w dostępności, integralności, uwierzytelniania i poufności systemów, komponentów lub procesów informatycznych, które doprowadziły do awarii lub znacznego zakłócenia funkcjonalności infrastruktury krytycznej, którą obsługują,
- poważne zakłócenia w dostępności, integralności, uwierzytelnianiu i poufności systemów, komponentów lub procesów informatycznych, które mogą prowadzić do awarii lub znacznego zakłócenia funkcjonalności infrastruktury kluczowej.

W ustawie NIS-RL przyjęto też definicję[75] dostawców usług cyfrowych (*Anbieter digitaler Dienste*) oraz poszerzono ich obowiązki i uprawnienia, dodając do ustawy § 8c (*Wymagania specjalne wobec dostawców usług cyfrowych*). Zgodnie

[73] Zgodnie § 8a ust. (1) BSI-Gesetz Urząd Federalny określa minimalne standardy bezpieczeństwa federalnej technologii informatycznej.

[74] Dotyczy to też operatorów sieci energetycznych i takich systemów energetycznych, które zostały wyznaczone jako infrastruktura krytyczna, co pociągnęło za sobą konieczność zmian w ustawie o dostawach energii elektrycznej i gazu (EnWG). Podmioty te określane są jako *Betreiber Kritischer Infrastrukturen*.

[75] Przyjęto m.in. nową definicję dostawcy usług cyfrowych. „Dostawca usług cyfrowych w rozumieniu tej ustawy to osoba prawna oferująca usługę cyfrową" (art. 1 ust. 1 pkt 1 lit. b) NIS-RL).

z § 8c ust. (1) BSI-Gesetz dostawcy usług cyfrowych muszą podjąć odpowiednie i proporcjonalne środki techniczne i organizacyjne w celu zarządzania zagrożeniami dla bezpieczeństwa sieci i systemów informatycznych, których używają do świadczenia usług cyfrowych w Unii Europejskiej lub utrzymać skutki tych zagrożeń na jak najniższym poziomie.

Zgodnie z § 8c ust. (2) BSI-Gesetz środki mające na celu zapobieganie zagrożeniom dla bezpieczeństwa sieci i systemów informatycznych muszą, przy uwzględnieniu aktualnego stanu wiedzy, zapewniać poziom bezpieczeństwa sieci i systemów informatycznych, który jest odpowiedni do istniejącego ryzyka. Należy wziąć pod uwagę następujące aspekty:

- bezpieczeństwo systemów i obiektów,
- wykrywanie, analiza i powstrzymywanie incydentów,
- zarządzanie ciągłością działania,
- monitorowanie, przegląd i testowanie,
- zgodność z międzynarodowymi standardami.

Obowiązek zgłoszenia incydentu naruszającego ochronę nie ma zastosowania, jeżeli usługodawca nie ma wystarczającego dostępu do informacji wymaganych do oceny wpływu zdarzenia naruszającego bezpieczeństwo, przy czym Urząd Federalny może żądać od dostawcy usług cyfrowych między innymi informacji wymaganych do oceny bezpieczeństwa sieci i systemów informatycznych, w tym dowodów podjętych środków bezpieczeństwa[76].

Zaznaczyć należy, że jeżeli dostawca usług cyfrowych ma swoją główną siedzibę, przedstawiciela lub sieć i systemy informacyjne w innym państwie członkowskim Unii Europejskiej, Urząd Federalny współpracuje z właściwym organem tego państwa członkowskiego przy wykonywaniu zadań.

W ustawie NIS-RL zawarto też przepisy dotyczące raportowania do odpowiednich instytucji UE. Zgodnie z § 13 ust. (5) do 9 sierpnia 2018 r., a następnie corocznie Urząd Federalny przesyła podsumowujące sprawozdanie – zgodnie z art. 11 dyrektywy NIS. Raport zawiera liczbę zgłoszeń i rodzaj zgłoszonych incydentów bezpieczeństwa oraz opis przeprowadzonych pomiarów. Raport nie może zawierać żadnych informacji, które mogłyby prowadzić do identyfikacji poszczególnych zgłoszeń lub ujawnić poszczególnych operatorów lub dostawców.

W ustawie NIS-RL rozszerzono również środki zwiększające bezpieczeństwo techniki informatycznej. Obejmują one w szczególności rozszerzenie uprawnień dostawcy usług telekomunikacyjnych w zakresie wykrywania i obrony przed cyberatakami. W tym celu dostawcom przyznano nowe uprawnienia[77], na podsta-

---

[76] W sprawie oceny bezpieczeństwa infrastruktury telematycznej BSI działa we współpracy z instytucją o nazwie *Gesellschaft für Telematik* (Stowarzyszenie Telematyczne). W tym celu zmieniono przepisy Kodeksu cywilnego, Ks. V (SGB V).

[77] Zawarto je głównie w art. 5, dotyczącym zmian w prawie telekomunikacyjnym (*Telekommunikationsgesetzes*, TKG), https://www.gesetze-im-internet.de/tkg_2004/.

wie których będą oni mogli między innymi ograniczyć lub uniemożliwić przesyłanie danych do źródeł zakłóceń, ale też pozyskiwać dane o transmisji danych, które są przesyłane niezależnie od treści procesu komunikacyjnego. Proces ten musi odbywać się przy poszanowaniu komunikacji między odbiorcą a nadawcą.

Szwecja

W czerwcu 2017 r. rząd Szwecji przyjął narodową strategię cyberbezpieczeństwa[78]. Celem strategii jest pomoc w stworzeniu w długim okresie warunków dla różnych podmiotów w społeczeństwie do działań na rzecz zwiększenia cyberbezpieczeństwa oraz zwiększenia świadomości społecznej w tym zakresie. Strategia skierowana jest do władz centralnych, samorządowych, przedsiębiorstw, organizacji i osób fizycznych. Strategia została opracowana na podstawie narodowej strategii bezpieczeństwa[79] i narodowej strategii cyfryzacji[80], a także unijnej dyrektywy NIS.

W strategii określono sześć obszarów priorytetowych:

- zabezpieczenie systematycznego i całościowego podejścia w działaniach podejmowanych w zakresie cyberbezpieczeństwa,
- wzmocnienie bezpieczeństwa sieci, produktu i systemu w kontekście komunikacji elektronicznej,
- wzmocnienie zdolności do zapobiegania cyberatakom, wykrywania ich i zarządzania nimi,
- zwiększenie możliwości zapobiegania cyberprzestępczości,
- podnoszenie wiedzy i promowanie podejścia eksperckiego,
- wzmocnienie współpracy międzynarodowej.

W strategii podkreślono, że kwestie bezpieczeństwa informacyjnego są uregulowane w Szwecji w wielu aktach prawnych, w tym w ówczesnej ustawie o ochronie bezpieczeństwa z 1996 r.[81], rozporządzeniu w sprawie gotowości na sytuacje kryzysowe oraz środków stosowanych przez organy odpowiedzialne za nadzór

---

78 *A national cyber security strategy*, Skr. 2016/17:213, Ministry of Justice, 22/06/2017, https://www.government.se/4ada5d/contentassets/d87287e088834d9e8c08f28d0b9dda5b/a-national-cyber-security-strategy-skr.-201617213.

79 *National Security Strategy*, January 2017, https://www.government.se/4aa5de/contentassets/0e04164d7eed462aa511ab03c890372e/national-security-strategy.pdf.

80 *For sustainable digital transformation in Sweden – a Digital Strategy*, June 2017, https://www.government.se/49c292/contentassets/117aec2b9bf44d758564506c2d99e825/2017_digitaliseringsstrategin_faktablad_eng_webb-2.pdf.

81 *Säkerhetsskyddslag (1996:627)*, https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/sakerhetsskyddslag-1996627_sfs-1996-62, uchylona przez *Säkerhetsskyddslag (2018:585)*.

w przypadku podwyższonej gotowości[82], ustawie o archiwach[83], ustawie o ochronie danych osobowych[84] oraz ustawie o komunikacji elektronicznej[85]. Ponadto obowiązują sektorowe rozporządzenia odnoszące się do bezpieczeństwa informacyjnego.

W marcu 2019 r. opublikowano całościowy plan działania w zakresie cyberbezpieczeństwa[86]. Plan zawiera 77 działań, które mają być podjęte w latach 2019–2022 w celu realizacji sześciu obszarów priorytetowych określonych w narodowej strategii cyberbezpieczeństwa. Za realizację działań odpowiedzialne są:

- Szwedzka Agencja ds. Zagrożeń Cywilnych (szw. *Myndigheten för samhällsskydd och beredskap*, MSB; ang. *Swedish Civil Contingencies Agency*),
- Narodowy Instytut Obrony Radiołączności (szw. *Försvarets radioanstalt*, FRA; ang. *National Defence Radio Establishment*),
- Szwedzka Administracja Zaopatrzenia Sił Zbrojnych (szw. *Försvarets materielverk*, FMV; ang. *Swedish Defence Materiel Administration*),
- Szwedzkie Siły Zbrojne (szw. *Försvarsmakten*; ang. *Swedish Armed Forces*),
- Szwedzki Urząd ds. Poczty i Telekomunikacji (szw. *Post- och telestyrelsen*, PTS; ang. *Swedish Post and Telecom Authority*),
- szwedzka policja,
- Szwedzkie Służby Bezpieczeństwa (szw. *Säkerhetspolisen*, SÄPO; ang. *Swedish Security Service*).

Od czasu ogłoszenia narodowej strategii cyberbezpieczeństwa w Szwecji przyjęto dwie ustawy regulujące kwestie cyberbezpieczeństwa.

Pierwsza z nich to ustawa o ochronie bezpieczeństwa z 2018 r.[87] (zmieniona w 2020 r.), uchylająca wcześniejszą ustawę o ochronie bezpieczeństwa z 1996 r. Ustawa (wraz z rozporządzeniem[88]) znajduje zastosowanie do podmiotów, które

---

82 *Förordning (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap*, https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/forordning-20151052-om-krisberedskap-och_sfs-2015-1052.

83 *Arkivlag (1990:782)*, https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/arkivlag-1990782_sfs-1990-782.

84 *Lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning*, https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-2018218-med-kompletterande-bestammelser_sfs-2018-218.

85 *Lag (2003:389) om elektronisk kommunikation*, https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-2003389-om-elektronisk-kommunikation_sfs-2003-389.

86 *Comprehensive cyber security action plan 2019–2022*, March 2019, https://rib.msb.se/filer/pdf/28898.pdf.

87 *Säkerhetsskyddslag (2018:585)*, https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/sakerhetsskyddslag-2018585_sfs-2018-585.

88 *Säkerhetsskyddsförordning (2018:658)*, https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/sakerhetsskyddsforordning-2018658_sfs-2018-658.

prowadzą działalność ważną z punktu widzenia bezpieczeństwa Szwecji lub są objęte wiążącym zobowiązaniem międzynarodowym Szwecji w zakresie ochrony bezpieczeństwa (działalność wrażliwa z punktu widzenia bezpieczeństwa). Ustawa zawiera również przepisy odnoszące się do podmiotów zamierzających przenieść własność całości lub części swojej działalności wrażliwej z punktu widzenia bezpieczeństwa oraz przepisy w zakresie współpracy międzynarodowej w obszarze ochrony bezpieczeństwa.

Ochrona bezpieczeństwa zdefiniowana jest w ustawie o ochronie bezpieczeństwa z 2018 r. jako ochrona działalności wrażliwej z punktu widzenia bezpieczeństwa przed szpiegostwem, sabotażem, terroryzmem i innymi przestępstwami, które mogą zagrażać tej działalności, jak również ochronę w innych przypadkach informacji niejawnej, zgodnie z ustawą o publicznym dostępie do informacji i tajemnicy państwowej[89]. Podmioty, które prowadzą działalność ważną z punktu widzenia bezpieczeństwa, są zobowiązane do sporządzania stosownych analiz bezpieczeństwa oraz planowania i wdrażania wszelkich środków ochrony bezpieczeństwa (w zakresie bezpieczeństwa informacji bezpieczeństwa fizycznego i osobowego), które uznają za niezbędne w wyniku takiej analizy[90].

Druga ustawa przyjęta w ostatnich latach w obszarze cyberbezpieczeństwa, implementująca dyrektywę NIS, to ustawa o bezpieczeństwie sieci i systemów informatycznych[91] (wraz z rozporządzeniem[92]), która nakłada na operatorów usług kluczowych i dostawców usług cyfrowych obowiązek podjęcia środków prewencyjnych w celu zapewnienia bezpieczeństwa sieci i systemów informatycznych.

Zgodnie z ustawą Szwedzka Agencja ds. Zagrożeń Cywilnych[93] określiła kryteria identyfikacji operatorów usług kluczowych w sektorach energetyki,

---

89 *Offentlighets- och sekretesslag (2009:400)*, https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/offentlighets--och-sekretesslag-2009400_sfs-2009-400. Informacje o ustawie w jęz. angielskim: *Public access to information and secrecy. The legislation in brief*, Ministry of Justice, 2020, https://www.regeringen.se/4a76f3/contentassets/2c767a1ae4e8469fbfd0fc044998ab78/public-access-to--information-and-secrecy.pdf.

90 *The new Swedish Protective Security Act*, https://www.eversheds-sutherland.com/documents/global/Sweden/The-new-Swedish-Protective-Security-Act.pdf.

91 *Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster*, https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-20181174-om-informationssakerhet-for_sfs-2018-1174.

92 *Förordning (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster*, https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/forordning-20181175-om-informationssakerhet_sfs-2018-1175.

93 *MSBFS 2018:7 föreskrifter om anmälan och identifiering av leverantörer av samhällsviktiga tjänster*, https://www.msb.se/siteassets/dokument/regler/rs/0264c176-6b31-43c6-9fd8-807102df3844.pdf.

transportu, bankowości, infrastruktury rynków finansowych, służby zdrowia, zaopatrzenia w wodę pitną i jej dystrybucję oraz infrastruktury cyfrowej. Operatorzy usług kluczowych i dostawcy usług cyfrowych zgłaszają niezwłocznie incydenty, które mają odpowiednio istotny wpływ na ciągłość usług kluczowych lub na świadczenie usług cyfrowych Szwedzkiej Agencji ds. Zagrożeń Cywilnych. W przypadku niezgłoszenia incydentu organ właściwy może nałożyć na operatora lub dostawcę grzywnę w wysokości od 5000 koron szwedzkich do 10 000 000 koron szwedzkich[94] (497,15 euro – 994 300 euro)[95].

W Szwecji wyznaczono kilka organów właściwych ds. bezpieczeństwa sieci i informacji w rozumieniu dyrektywy NIS[96]. Dla dostawców usług cyfrowych funkcję tę pełni Szwedzki Urząd ds. Poczty i Telekomunikacji, a dla operatorów usług kluczowych w poszczególnych sektorach: Szwedzka Agencja Energii (szw. *Energimyndigheten*, STEM; ang. *Swedish Energy Agency*), Szwedzka Agencja Transportu (szw. *Transportstyrelsen*, TS; ang. *Swedish Transport Agency*), Szwedzki Urząd Nadzoru Finansowego (szw. *Finansinspektionen*, FI; ang. *Sweden's financial supervisory authority*), Inspektorat ds. Zdrowia i Opieki Społecznej (szw. *Inspektionen för vård och omsorg*, IVO; ang. *The Health and Social Care Inspectorate*), Szwedzka Agencja ds. Żywności (szw. *Livsmedelsverket*, SLV; ang. *The Swedish Food Agency*) oraz Szwedzki Urząd ds. Poczty i Telekomunikacji. Funkcję krajowego pojedynczego punktu kontaktowego ds. bezpieczeństwa sieci i systemów informatycznych pełni Szwedzka Agencja ds. Zagrożeń Cywilnych. W Szwecji wyznaczono jeden krajowy CSIRT, finansowany przez Szwedzką Agencję ds. Zagrożeń Cywilnych[97].

Bibliografia

Akty prawne

■ Unia Europejska

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii, Dz.Urz. UE L 194 z 19 lipca 2016 r.

---

94 *Developments on NIS Directive in EU Member States*, Bird & Bird, January 2020, https://www.twobirds.com/~/media/pdfs/developments-on-nis-directive-in-eu-member-states.pdf.

95 Wg kursu Europejskiego Banku Centralnego z 7 stycznia 2021 r.

96 *Implementation of the NIS Directive in Sweden*, https://ec.europa.eu/digital-single-market/en/implementation-nis-directive-sweden.

97 Https://www.cert.se.

■ Polska

Ustawa z 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, t.j. Dz.U. 2020, poz. 1369.

Uchwała nr 125 Rady Ministrów z 22 października 2019 r. w sprawie „Strategii cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024", M.P. poz. 1037.

■ Belgia

Ustawa z 7 kwietnia 2019 r. ustanawiająca ramy bezpieczeństwa sieci i systemów informatycznych użyteczności publicznej dla bezpieczeństwa publicznego [*Loi de 7 Avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique*].

Dekret królewski wdrażający ustawę z 7 kwietnia 2019 r. ustanawiającą ramy bezpieczeństwa sieci i systemów informatycznych o znaczeniu ogólnym dla bezpieczeństwa publicznego oraz ustawę z 1 lipca 2011 r. w sprawie bezpieczeństwa i ochrony infrastruktury krytycznej C–2019/41284 [*Arrêté royal portant exécution de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique, ainsi que de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques*].

Dekret królewski z 10 października 2014 r. ustanawiający Centrum Bezpieczeństwa Cybernetycznego Belgii [*Arrêté royal de 10 Octobre 2014 portant création du Centre pour la Cybersécurité Belgique*].

■ Czechy

Ustawa nr 181/2014 z 23 lipca 2014 r. o bezpieczeństwie cybernetycznym [*Zákon ze dne 23. července 2014 o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)*].

Rozporządzenie nr 437/2017 z 8 grudnia 2017 r. w sprawie kryteriów określania operatora usług kluczowych [*Vyhláška č. 437/2017 Sb. ze dne 8. prosince 2017, o kritériích pro určení provozovatele základní služby*].

Rozporządzenie nr 82/2018 z 21 maja 2018 r. o środkach bezpieczeństwa, incydentach w zakresie bezpieczeństwa cybernetycznego, środkach reaktywnych, wymogach dokumentacji w zakresie bezpieczeństwa cybernetycznego i usuwaniu danych (rozporządzenie o bezpieczeństwie cybernetycznym) [*Vyhláška č. 82/2018 Sb. ze dne 21. května 2018, o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti)*].

■ Estonia

Ustawa z 23 maja 2018 r. o bezpieczeństwie cybernetycznym [*Cybersecurity Act (Küberturvalisuse seadus) of 23rd May 2018*].

■ Francja

Ustawa nr 2013-1168 z 18 grudnia 2013 r. o programowaniu wojskowym na lata 2014–2019 oraz o różnych przepisach dotyczących obronności i bezpieczeństwa narodowego [*Loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale*].

Ustawa nr 2018-133 z 26 lutego 2018 r. o różnych przepisach w celu dostosowania do prawa Unii Europejskiej w dziedzinie bezpieczeństwa [*Loi n° 2018-133 du 26 février 2018 portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité*].

Ustawa nr 2018-493 z 20 czerwca 2018 r. o ochronie danych osobowych [*Loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles*].

Dekret nr 2009-834 z 7 lipca 2009 r. ustanawiający służbę krajową o nazwie „Krajowa Agencja ds. Bezpieczeństwa Systemów Informatycznych" [*Décret n° 2009-834 du 7 juillet 2009 portant creation d'un service a competence nationale dénommé "Agence nationale de la sécurité des systèmes d'information"*].

Dekret nr 2015-350 z 27 marca 2015 r. w sprawie kwalifikacji produktów bezpieczeństwa i dostawców usług zaufania do celów bezpieczeństwa systemów informacyjnych [*Décret n° 2015-350 du 27 mars 2015 relatif à la qualification des produits de sécurité et des prestataires de service de confiance pour les besoins de la sécurité des systèmes d'information*].

Dekret nr 2015-351 z 27 marca 2015 r. w sprawie bezpieczeństwa systemów informacyjnych ważnych operatorów i podjętych w celu zastosowania sekcji 2 rozdziału II tytułu III księgi III części I części legislacyjnej Kodeksu Obronnego [*Décret n° 2015-351 du 27 mars 2015 relatif à la sécurité des systèmes d'information des opérateurs d'importance vitale et pris pour l'application de la section 2 du chapitre II du titre III du livre III de la première partie de la partie législative du code de la defense*].

Dekret nr 2018-384 z 23 maja 2018 r. w sprawie bezpieczeństwa sieci i systemów informatycznych operatorów usług podstawowych i dostawców usług cyfrowych [*Décret n° 2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique*].

Kodeks bezpieczeństwa wewnętrznego [*Code de la sécurité intérieure*, https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000025504921/.

■ Holandia

Decyzja organizacyjna Ministerstwa Sprawiedliwości i Bezpieczeństwa z 2 maja 2019 r. [*Organisatiebesluit Ministerie van Justitie en Veiligheid van 02-05-2019*].

■ Niemcy

Federalna ustawa z 30 czerwca 2017 r. o ochronie danych, Federalny Dziennik Ustaw I, s. 2097 [*Bundesdatenschutzgesetz*, BGBl. I, s. 2097].

Ustawa z 20 grudnia 1990 r. o Służbie Kontrwywiadu Wojskowego, Federalny Dziennik Ustaw I, s. 2954, 2977 [*Gesetz über den Militärischen Abschirmdienst, MADG*].

Ustawa z 14 sierpnia 2009 r. o Federalnym Urzędzie ds. Bezpieczeństwa Informacji, Federalny Dziennik Ustaw I, s. 2821 [*Gesetz über das Bundesamt für Sicherheit in derInformationstechnik*, BGBl. I, s. 2821].

Ustawa z 17 lipca 2015 r. o zwiększeniu bezpieczeństwa systemów informatycznych (ustawa o bezpieczeństwie informatycznym) [*Gesetzzur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) Vom 17. Juli 2015*].

Ustawa wdrażająca dyrektywę Parlamentu Europejskiego i Rady (UE) 2016/1148 z 6 lipca 2016 r. w sprawie środków zapewniających wysoki wspólny poziom bezpieczeństwa sieci i systemów informatycznych w Unii [*Gesetzzur Umsetzung der Richtlinie (EU) 2016/1148des Europäischen Parlaments und des Rates vom 6. Juli 2016über Maßnahmen zur Gewährleistung eines hohen gemeinsamenSicherheitsniveaus von Netz- und Informationssystemen in der Union*].

■ Szwecja

Ustawa (1990:782) z 7 czerwca 1990 r. o archiwach [*Arkivlag (1990:782) av den 7 juni 1990*].

Ustawa (1996:627) z 8 lutego 1996 r. o ochronie bezpieczeństwa [*Säkerhetsskyddslag (1996:627) av den 8 februari 1996*].

Ustawa (2003:389) z 12 czerwca 2003 r. o łączności elektronicznej [*Lag (2003:389) om elektronisk kommunikation av den 12 juni 2003*].

Ustawa (2009:400) z 20 maja 2009 r. o publicznym dostępie do informacji i zachowaniu tajemnicy [*Offentlighets- och sekretesslag (2009:400) av den 20 maj 2009*].

Ustawa (2018:218) z 19 kwietnia 2018 r. z dodatkowymi przepisami do unijnego rozporządzenia o ochronie danych osobowych [*Lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning av den 19 april 2018*].

Ustawa (2018:585) z 24 maja 2018 r. o ochronie bezpieczeństwa [*Säkerhetsskyddslag (2018:585) av den 24 maj 2018*].

Ustawa (2018:1174) z 20 czerwca 2020 r. o bezpieczeństwie informacji dla usług społecznie ważnych i cyfrowych [*Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster av den 20 juni 2020*].

Rozporządzenie (2015:1052) z 17 grudnia 2015 r. w sprawie gotowości na wypadek sytuacji kryzysowej oraz środków podejmowanych przez organy odpowiedzialne za bezpieczeństwo w przypadku wystąpienia sytuacji kryzysowej [*Förordning (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap av den 17 december 2015*].

Rozporządzenie (2018:658) z 31 maja 2018 r. o ochronie bezpieczeństwa [*Säkerhetsskyddsförordning (2018:658) av den 31 maj 2018*].

Rozporządzenie (2018:1175) z 20 czerwca 2020 r. w sprawie bezpieczeństwa informacji dla usług społecznie ważnych i cyfrowych [*Förordning (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster av den 20 juni 2020*].

Literatura

Dziewulak D., Łukasz D., Mróz M., *Informacja na temat informatyzacji państwa i cyberbezpieczeństwa we Francji i Niemczech*, opinia BAS-ZSP-1713/17.

Warchoł A., *Cyberbezpieczeństwo w kontekście wojny informacyjnej – jakie są rozwiązania w Holandii i Niemczech?*, opinia BAS-1424/19.

Inne

Agenda cyfrowa 2020 dla Estonii [*Digital Agenda 2020 for Estonia*], https://www.mkm.ee/sites/default/files/digitalagenda2020_final_final.pdf.

A national cyber security strategy, Skr. 2016/17:213, Ministry of Justice, 22/06/2017, https://www.government.se/4ada5d/contentassets/d87287e088834d9e8c08f28d0b9dda5b/a-national-cyber-security-strategy-skr.-201617213.

Comprehensive cyber security action plan 2019–2022, March 2019, https://rib.msb.se/filer/pdf/28898.pdf.

Cybersecurity Legislation in the Netherlands, https://tedangevaare.nl/nl/.

Cyber Security, https://cms.law/en/int/publication/data-law-navigator/the-netherlands.

Cyber Security Assessment Netherlands 2020, https://english.nctv.nl/documents/publications/2020/08/28/cyber-security-assessment-netherlands-2020.

Das IT-Sicherheitsgesetz. Kritische Infrastrukturen schützen, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/IT-Sicherheitsgesetz.pdf?__blob=publicationFile&v=7.

Developments on NIS Directive in EU Member States, Bird & Bird, January 2020, https://www.twobirds.com/~/media/pdfs/developments-on-nis-directive-in-eu-member-states.pdf.

Digital Strategy, June 2017, https://www.government.se/49c292/contentassets/117aec2b9bf44d758564506c2d99e825/2017_digitaliseringsstrategin_faktablad_eng_webb-2.pdf.

Estonian Enterpreneurship Growth Strategy 2014–2020, https://kasvustrateegia.mkm.ee/index_eng.html.

Foreign Policy Strategy 2030, https://vm.ee/sites/default/files/Estonia_for_UN/Rasmus/estonian_foreign_policy_strategy_2030_final.pdf.

Globalny indeks bezpieczeństwa cybernetycznego 2018, Międzynarodowy Związek Telekomunikacyjny (ITU) [*Global Cybersecurity Index 2018, International Telecommunication Union (ITU)*], https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf.

Implementation of the NIS Directive in The Netherlands, https://ec.europa.eu/digital-single-market/en/implementation-nis-directive-netherlands.

Knowledge-based Estonia, the RD&I Strategy for 2014–2020, https://www.hm.ee/sites/default/files/estonian_rdi_strategy_20142020.pdf?_ga=1.101330693.

Krajowa strategia bezpieczeństwa cyfrowego, 2015 [*La stratégie nationale pour la sécurité du numérique: une réponse aux nouveaux enjeux des usages numériques*, 2015] https://

www.ssi.gouv.fr/actualite/la-strategie-nationale-pour-la-securite-du-numerique-une-reponse-aux-nouveaux-enjeux-des-usages-numeriques/.

Krajowa strategia bezpieczeństwa cybernetycznego Republiki Czeskiej na lata 2020–2025 [*Národní strategie kybernetické bezpečnosti České republiky na období let 2020–2025*].

Lifelong Learning Strategy 2014–2020, https://www.hm.ee/sites/default/files/estonian_lifelong_strategy.pdf.

National Cyber Security Agenda. A cyber secure Netherlands, https://www.enisa.europa.eu/news/member-states/CSAgenda_EN.pdf.

National Cyber Security in practice, e-Governance Academy, Tallinn 2020, https://ega.ee/wp-content/uploads/2020/05/Kuberturvalisuse_kasiraamat_ENG.pdf.

National Security Strategy, January 2017, https://www.government.se/4aa5de/contentassets/0e04164d7eed462aa511ab03c890372e/national-security-strategy.pdf.

NCSC-NL. Statutory task, https://english.ncsc.nl/about-the-ncsc/statutory-task.

NIS Implementation Tracker, https://www.digitaleurope.org/resources/nis-implementation-tracker/.

Public access to information and secrecy. The legislation in brief. Government Offices in Sweden. Ministry of Justice, 2020, https://www.regeringen.se/4a76f3/contentassets/2c767a1ae4e8469fbfd0fc044998ab78/public-access-to-information-and-secrecy.pdf.

Strategia Francji w zakresie ochrony i bezpieczeństwa systemów informacji, 2011 [*Défense et sécurité des systèmes d'information – Stratégie de la France*, 2011] www.ssi.gouv.fr/uploads/IMG/pdf/20110215_Defense_et_securite_des_systemes_d_information_strategie_de_la_France.pdf.

The new Swedish Protective Security Act, https://www.eversheds-sutherland.com/documents/global/Sweden/The-new-Swedish-Protective-Security-Act.pdf.

The State of IT Security in Germany 2018, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2018.pdf?__blob=publicationFile&v=3.