**Cybersecurity and Law**

2025 Nr 1(13)

**DOI: 10.35467/cal/214599**

# System of cybersecurity authorities in Germany

# System organów cyberbezpieczeństwa w Niemczech

**Agnieszka BRZOSTEK**
Akademia Sztuki Wojennej
ORCID: 0000-0002-7444-0186
e-mail: a.brzostek@akademia.mil.pl

## Abstract

Increasing the level of resilience and security of networks and information systems in the EU was the reason for the adoption by the European Parliament and the Council on 14 December 2022 of Directive EU 2022/2555, known as the NIS 2 Directive. The implementation of the directive forced Member States to adapt their national frameworks to new cybersecurity management standards. In Germany, this process led to the development of the draft IT-Sicherheitsgesetz 3.0 act and an amendment to the Act on the Federal Office for Information Security (BSI).

## *Keywords*

*cybersecurity system, cybersecurity authorities, NIS Directive 2*

## Streszczenie

W celu zwiększenie poziomu odporności i bezpieczeństwa sieci i systemów informatycznych w UE przyjęto przez Parlament Europejski i Radę 14 grudnia 2022 r. dyrektywę UE 2022/2555, znaną jako dyrektywa NIS 2. Wdrożenie dyrektywy zmusiło państwa członkowskie do dostosowania krajowych ram prawnych do nowych standardów zarządzania cyberbezpieczeństwem. W Niemczech proces ten doprowadził do opracowania projektu ustawy IT-Sicherheitsgesetz 3.0 oraz nowelizacji ustawy o Federalnym Urzędzie ds. Bezpieczeństwa Informacji (BSI).

***Słowa kluczowe***
*system cyberbezpieczeństwa, organy właściwe w zakresie cyberbezpieczeństwa, Dyrektywa NIS 2*

## Uwagi ogólne

Rozwiązania przyjęte przez Dyrektywę NIS z 2016 r. okazały się być niewystarczające skuteczne na rosnące ataki w cyberprzestrzeni przez takie jak ataki *ransomware*, sabotaże dotyczące coraz szerszej grupy podmiotów. Przyjęta przez Parlament Europejski i Radę w dniu 14 grudnia 2022 r. Dyrektywa UE 2022/2555 znana jako dyrektywa NIS 2 miała za zadanie usunąć wszystkie powstałe luki i stworzyć bardziej jednolity system ochrony cyberprzestrzeni poprzez wprowadzenie minimalnych wymogów bezpieczeństwa, obowiązek zarządzania ryzykiem i zgłaszania incydentów, surowsze kary administracyjne oraz wzmocnienie współpracy europejskiej. Implementacja dyrektywy wymusiła na państwach członkowskich dostosowanie krajowych ram do nowych standardów zarządzania cyberbezpezpieczeństwem, Efektywne wdrożenie dyrektywy wymaga przyjęcia rozwiązań prawnych i organizacyjnych. W Niemczech ten proces ten doprowadził do opracowania projektu ustawy IT-Sicherheitsgesetz 3.0 oraz nowelizacji ustawy o federalnym Urzędzie ds. Bezpieczeństwa Informacji (BSI). Stąd celem artykułu jest analiza prawnych i administracyjnych form działania systemu federalnych organów powołanych do realizacji zadań w zakresie cyberbezpieczeństwa.

Niemcy były jednym z pierwszych krajów, który zareagowały na zagrożenie cybernetyczne w Europie. Już w 2005 r. wskazano, że bezpieczeństwo cybernetyczne musi być częścią bezpieczeństwa narodowego. W 2009 r. uchwalono pierwszą ustawę dotyczącą bezpieczeństwa w zakresie cyberbezpieczeństwa była to ustawa o wzmocnieniu federalnego bezpieczeństwa technologii informatycznych[1]. Ustawa określiła zadania BSI jako centralnego biura raportowania w zakresie bezpieczeństwa IT, upoważniając go do gromadzenia, przetwarzania danych w celu skutecznego wykrycia zagrożeń i opracowywania jednolitych standardów dla administracji federalnej. W 2011 r. rząd przyjął pierwszą strategię bezpieczeństwa cybernetycznego[2]. Według C. Guitton Niemcy przyjęły strategią bezpieczeństwa cybernetycznego jako formę polityki prewencyjnej, nie popartej żadnymi incydentami dotyczące krytycznej infrastruktury informatycznej. Duży wpływ na poziom zagrożenia miały nie weryfikowalne dane dostarczone przez dostawców cyberbezpieczeństwa i wpływ, jakie na nich wywarły wydarzenia mające miejsce w innych krajach, np.

[1] Gesetz über das Bundesamt für Sicherheit in derInformationstechnik, BSI-Gesetz vom 14. August 2009. (BGBl. i S. 2821)/ Dalej jako ustawa o BSI.
[2] Strategia cybernetyczna Niemiec 2011 (niem. Cyber Sicheritstrategie fur Deutschland 2011, s. 3-4).

w USA[3]. Przyjęcie strategii skutkowało utworzeniem Krajowej Rady Bezpieczeństwa Cybernetycznego, której zadaniem było sprawowanie ogólnej kontroli nad realizacją wdrożenia celów strategii, a w razie potrzeby mogła dostosować strategie i środki do określonych wymagań i warunków ramowych wynikających ze Strategii[4]. W 2011 r. Ministerstwo Spraw Wewnętrznych RFN powołało Narodowe Centrum Przeciwdziałania Zagrożeniom dla Cyberprzestrzeni (*Nationale Cyber-Abwehrzentrum* – NCAZ), które miało stać się pierwszym ogniwem walki z zagrożeniami cybernetycznymi i stanowić platformę współpracy właściwych rzeczowo organów niemieckiej administracji. Niemcy nie zdecydowali się na instytucjonalizację prac Centrum ze względu na obowiązujący w RFN nakaz rozdziału (*Trennungsgebot*) służb specjalnych od służb policyjnych[5].

Ustawa o bezpieczeństwie sieci teleinformatycznych uchwalona w 2015 r.[6]zobowiązała operatów infrastruktury krytyczej do regularnego raportowania do BSI ( Federalnego Urzędu ds. Bezpieczeństwa Informacji) oraz do utrzymania zgodności ze standardami bezpieczeństwa. Ustawa podtrzymała regulacje poprzedniej ustawy, wskazując na szczególna rolę BSI w systemie organów administracji publicznej w zakresie cyberbezpieczeństwa. BSI pełniło funkcję centralnego organu nadzorującego bezpieczeństwo systemów informatycznych, analizując zgłoszenia o incydentach i koordynując działania naprawcze. Ponadto urząd opracowywał minimalne standardy bezpieczeństwa dla administracji federalnej i wspiera instytucje rządowe w ich wdrażaniu.

Następna strategia cyberbezpieczeństwa Niemiec w 2016 r. wskazała na konieczność budowy zrównoważanego systemu bezpieczeństwa cybernetycznego[7]. Narodowego Centrum Przeciwdziałania Zagrożeniom dla Cyberprzestrzeni (NCAZ) zorganizowało swoją strukturę na szczeblu federalnym w sposób umożliwiający współpracę poszczególnych podmiotów w zakresie swoich działań. Istotnym założeniem było zintensyfikowanie współpracy z landami. W ramach działania NCAZ, władze federalne odpowiedzialne za kwestie bezpieczeństwa cybernetycznego wymieniały informacje o incydentach cybernetycznych w Cyber-AZ oraz udostępniały swoje oceny i analizy[8].

Do implementacji Dyrektywy NIS z 2016 r. w Niemczech konieczne było wprowadzenie zmian w ustawodawstwie. Ustawa implementacyjna do Dyrektywy NIS z czerwca 2017 r. stworzyła podstawę do powołania mobilnych zespołów reagowania na incydenty MIRT w BSI. Natomiast w prawie telekomunikacyjnym

[3] C. Guitton, Cyber insecurity as a national threat: overreaction from Germany, France and the UK?, „European Security" 2013, no. 22(1), s. 22.
[4] Strategia cyberbezpieczeństwa Niemiec z 2011, s. 7.
[5] K. Sacewicz, Niemiecka strategia ochrony cyberprzestrzeni, „Przegląd Bezpieczeństwa Wewnętrznego" 2021, t. 4, nr 7, s. 129-130.
[6] Zweite Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0 z 23 kwietnia 2021 r.
[7] Strategia cyberbezpieczeństwa Niemiec z 2016, (niem. Cyber- Sicherheitsstrategie für Deutschland 2016), s. 9.
[8] Ibidem, s. 27-28.

rozszerzono opcje wykrywania i blokowania cyberataków. W BSI powoływane zostały mobilne zespoły reagowania na incydenty (MIRT), które dokonywały analizy, i miały uprawnienia do usuwania incydentów cybernetycznych w instytucjach. Na żądanie MIRT, BSI miał zapewnić wsparcie organom konstytucyjnym, władzom federalnym i operatorom infrastruktury krytycznej oraz podobnie ważnych obiektów lokalnych w celu tego wsparcia jest szybkie przywrócenie sprawności technicznej danego obiektu[9]. Strategia cyberbezpieczeństwa przyjęta przez rząd federalny w dniu 8 września 2021 r. Punktem wyjścia strategii jest analiza sytuacji zagrożenia. Wskazuje na to znaczny wzrost jakościowy i ilościowy cyberataków, rosnąca powierzchnia ataków i nowe rodzaje scenariuszy zagrożeń. Krajobraz cyberbezpieczeństwa obejmuje społeczeństwo obywatelskie, inicjatywy i podmioty naukowe, gospodarcze i rządowe. Cele strategii wskazano w 4 obszarach:

- Cyberbezpieczeństwo jako wspólne zadanie państwa, biznesu, nauki i udziału społeczeństwa;
- Wzmocnienie cyfrowej suwerenności państwa, biznesu, nauki i społeczeństwa;
- Zapewnienie bezpieczne cyfryzację;
- Uczyń cele mierzalne i przejrzyste[10].

Przedstawione cele strategii wskazują na zapewnieniu bezpieczeństwa obywateli jako głównych użytkowników sieci IT. W tym celu cele strategiczne przewidują uwrażliwienie obywateli i zwiększenie ich kompetencji cybernetycznych. Następny cel ma zostać osiągnięty poprzez wzmocnienie cyberbezpieczeństwa w całej gospodarce i skupienie się na ochronie infrastruktury krytycznej, a w szczególności na działaniu małych i średnich przedsiębiorców. Istotny jest tu rozwój suwerenności cyfrowej i konkurencyjności firm w obszarze cyberbezpieczeństwa. W ramach kolejnego celu można wyodrębnić trzy główne obszary działania: 1. Podział kompetencji i współpracy pomiędzy władzami, 2. Dalszy rozwój umiejętności i uprawnień władz, 3. Nowe wyzwania dla państwowych podmiotów w zakresie cyberprzestrzeni. Ostatni cel, rząd federalny zamierza osiągnąć poprzez „aktywne pozycjonowanie Niemiec w europejskiej i międzynarodowej polityce cyberbezpieczeństwa" oraz poprzez zaangażowanie Niemiec w Unii Europejskiej (UE) oraz w Pakt Północnoatlantycki (NATO)[11].

Strategia cyberbezpieczeństwa 2021 r. opiera się na rozwoju wskazanych wyżej strategii z 2011 r. i 2016 r. a przede wszystkim na podstawach działania Krajowej Rady Cyberbezpieczeństwa (NCSR), Narodowego Centrum Cyberobrony (NCAZ, Cyber A-Z) czy Centralnego Biura Informatyki w Sektorze Bezpieczeństwa (ZITiS). Realizacja specyfikacji i celów strategicznych odbywa

[9] Strategia cyberbepieczństwa Niemiec 2016, (niem. Cyber- Sicherheitsstrategie für Deutschland 2016), s. 29.
[10] Strategia cyberbezpieczeństwa Niemiec 2021, (Cybersicherheitsstrategie für Deutschland 2021), s. 6.
[11] Ibidem, s. 6-7.

się w szczególności przez organy wydziałowe Kancelarii Federalnej i ministerstwa. Działania federalne dzielą się na dwa poziomy działania: strategiczny i operacyjny.

## Krajowy system cyberbezpieczeństwa Republiki Federalnej Niemiec

Krajowy system cyberbezpieczeństwa Republiki Federalnej Niemiec opiera się na modelu współpracy między organami cywilnymi, policyjnymi wywiadowczymi i wojskowymi działającymi pod ogólną koordynacją Federalnego Ministerstwa Spraw Wewnętrznych i Ojczyzny (BMI). System ten stanowi złożoną strukturę instytucjonalną, której celem jest zapewnienie bezpieczeństwa infrastruktury cyfrowej państwa., obywateli oraz gospodarki, a także realizacja zobowiązań wynikających z prawa Unii Europejskiej, w tym dyrektywy NIS2.

Federalny Urząd ds. Bezpieczeństwa Informacji (*Bundesamt fur Sicherheit* -BSI) stanowi centralny organ administracji Federalnej właściwy w zakresie bezpieczeństwa informatycznego w Niemczech, pełniący funkcje narodowego organu właściwego ds. cyberbezpieczeństwa oraz punktu kontaktowego. Na mocy ustawy z dnia 14 sierpnia 2009 r.[12] BSI realizuje zadania w zakresie ochrony systemów teleinformatycznych administracji publicznej oraz koordynuje działania na rzecz zapewnienia bezpieczeństwa cybernetycznego. Do głównych kompetencji urzędu należy gromadzenie, analiza i ocena informacji o zagrożeniach, incydentach oraz ich podatność w systemach informatycznych, a także opracowywanie standardów bezpieczeństwa dla organów administracji federalnej. BSI pełni funkcję centralnego punktu raportowania i dokonuje wymiany informacji o incydentach cyberbezpieczeństwa[13]. Ponadto BSI uczestniczy w tworzeniu jednolitych standardów technicznych i organizacyjnych. Dla administracji publicznej oraz sprawuje nadzór nad zgodnością wykorzystywanych rozwiązań z obowiązującymi normami bezpieczeństwa.

W ramach unijnego systemu współpracy, BSI pełni także funkcję krajowego punktu kontaktowego w sieci CSIRT ustanowionego w dyrektywie NIS 2, zapewniający koordynację wymiany informacji i współpracy z Europejską agencją ds. cyberbezpieczeństwa (ENISA). BSI jest więc kluczowym elementem systemu organów cyberbezpieczeństwa Niemiec, łącząc funkcje regulacyjne, analityczne i operacyjne, a jego działalność stanowi podstawę dla zapewnienia cyfrowej suwerenności państwa i ochronę infrastruktury o znaczeniu krytycznym. Specyficzną cechą niemieckich rozwiązań jest powierzenie BSI kontroli nad sposobem wdrożenia szczegółowych procedur ochronnych w tych działach infrastruktury krytycznej, które decydują o sposobie funkcjonowania społeczeństwa. Za takie uznano systemy: bankowy, energetyczny, wodociągowy

[12] BSI -Gesetz vom 14. August 2009 ( BGBl i S. 2821), das zuletzt durch Artikel 12 des Gesetzes vom 23. Juni 2021 ( BGBl (Dz. U.F.Z.I s.2821), ustawa o BSI.
[13] § 8a-8b ustawy o BSI.

(dostaw wody pitnej), wyżywienia, telekomunikacyjny oraz technologii informatycznych. z racji tego, że zadania odnoszą się one do operatorów sieci teleinformatycznych i instytucji je wykorzystujących w zakresie ochrony danych, form zabezpieczenia w przypadku ich digitalizacji oraz prób włamania do osobistych kont w systemie, zdecydowano o takim rozdziale kompetencji instytucji federalnych. BSI jest uprawniona do wdrażania procedur dotyczących sposobu wykorzystywania przez elementy infrastruktury krytycznej systemów informatycznych, odnoszących się zarówno do sposobu ich wykorzystywania, jak i wprowadzanych zmian i inwestycji dokonywanych w celu zabezpieczenia ich funkcjonalności[14].

Koordynacji polityczną i strategiczną sprawuje BMI, które wyznacza kierunki polityki bezpieczeństwa cyfrowego i nadzoruje działania innych instytucji. Federalne Ministerstwo Spraw Wewnętrznych i Ojczyzny (Bundesministerium des Innerm und fur Heimat -BMI) pełni centralną rolę w systemie instytucjonalnym cyberbezpieczeństwa. Jako organ nadrzędny wobec BSI, BMI odpowiada za kształtowanie i koordynację strategii państwowej w zakresie bezpieczeństwa informatycznego, polityki cyfrowej oraz ochrony infrastruktury krytycznej. Podstawową kompetencją BMI w tym obszarze są przepisy ustawy o federalnym urzędzie do spraw bezpieczeństwa, informacji, a także strategia cyberbezpieczeństwa dla Niemiec 2021 roku. BMI określa cele, priorytety oraz instrumenty polityki rządowej dotyczącej ochrony cyfrowej. Ministerstwo koordynuje także działania międzyresortowe oraz współpracę między strukturami federalnymi, landami i prywatnymi instytucjami zapewniające spójność i efektywność działań w obszarze cyberbezpieczeństwa[15]. BMI posiada również kompetencje w zakresie nadzoru nad BSI, zatwierdzenia minimalnych standardów bezpieczeństwa informatycznego dla administracji Federalnej oraz podejmowania decyzji w sytuacjach kryzysowych dotyczących cyberataków o znaczeniu krajowym. Ministerstwo przewodniczy także Narodowym Centrum Obrony Cybernetycznej (Nationale Cyber-Abwehrzentrum – NCAZ), które stanowi platformę współpracy pomiędzy organami bezpieczeństwa, służbami wywiadowczymi i agencjami technologicznymi (§1-3 ustawy BSIG). W kontekście implementacji dyrektywy NIS 2 oraz nowej ustawy IT- Sicherheitsgesetz 3.0, BMI uzyskało rozszerzone uprawnienia w zakresie nadzoru regulacyjnego, koordynacji polityki, bezpieczeństwa IT i reprezentowania Niemiec w europejskich strukturach współpracy w dziedzinie cyberbezpieczeństwa. Dzięki temu pełni funkcję strategicznego i politycznego centrum decyzyjnego w krajowym systemie ochrony cyberprzestrzeni.

Wyróżnić należy organy współdziałające z BSI i BMI w zakresie cyberbezpieczeństwa. W obszarze bezpieczeństwa wewnętrznego kluczową rolę odgrywa Federalny Urząd Kryminalny -BKA, odpowiedzialny za ściganie cyberprzestępczości. W ramach swoich kompetencji BKA, prowadzi śledztwa

[14] Strategia cyberbezpieczeństwa Niemiec 2021, s. 19-20.
[15] Ibidem, s. 19.

dotyczące cyberataków o znaczeniu ponadregionalnym i międzynarodowym, w szczególności tych, które są kierowane przeciwko infrastrukturze krytycznej, administracji federalnej oraz systemom finansowym[16]. Urząd koordynuje także współpracę międzynarodowymi z urzędami kryminalnymi w landach -LKA oraz instuycjami międzynarodowymi, takimi jak Europol czy Interpol. Ponadto BKA uczestniczy w pracach Narodowego Centrum Obrony cybernetycznej (NCAZ), gdzie wraz z BSI, Bundeswera, BfV i innymi służbami wymienia dane o incydentach bezpieczeństwa. Urząd rozwija również specjalistyczne laboratoria informatyki śledczej oraz jednostki analityczne. Zajmujący się wykrywaniem złośliwego oprogramowania i przestępczości w tzw. darknecie. Działania te realizowane są na podstawie ustawy o Federalnym Urzędzie Kryminalnym -BKAG, które w nowelizacji z 2017 roku wprowadziło szczegółowe regulacje dotyczące zwalczania przestępczości cybernetycznej. BKA pełni zatem funkcję operacyjnego filaru systemu cyberbezpieczeństwa, uzupełniając działania o charakterze regulacyjnym, strategicznym prowadzone przez BMI i BSI, zapewnia kompleksową ochronę przed zagrożeniami w cyberprzestrzeni, od prewencji, analizy po ściganie sprawców cyberataków.

Federalny Urząd Ochrony Konstytucji (Bundesemt fur Verfassungsschutz - BfV) służy ochronie bezpieczeństwa wewnętrznego i jest cywilnym organem wywiadu wewnętrznego. Podstawowym zadaniem BfV jest ochrona porządku konstytucyjnego oraz bezpieczeństwa wewnętrznego państwa, a w kontekście cyberbezpieczeństwa odpowiada za rozpoznawanie, analizowanie i przeciwdziałanie cyberzagrożeniom o charakterze wewnętrznym, w szczególności tym związanym z działalnością obcych służb wywiadowczych, organizacji ekstremistycznych oraz prowadzących działania szpiegowskie i sabotażowe w cyberprzestrzeni. Zgodnie z ustawą o Federalnym Urzędzie Ochrony Konstytucji z dnia 20 grudnia 1990 r.[17], BfV posiada uprawnienia do prowadzenia działań rozpoznawczych w zakresie bezpieczeństwa teleinformatycznego, w tym monitorowania i analizowania incydentów, które mogło zagrażać strukturze krytycznej lub bezpieczeństwu instytucji państwowych. BfV w pełni również funkcję punktu kontaktowego dla sektora prywatnego, współpracując z przedsiębiorstwami strategicznymi i instytucjami naukowymi w ramach cyber-alliance, sieci partnerstwa publiczno-prywatnego służącej wymianie informacji o zagrożeniach.

W wymiarze zewnętrznym zadania w zakresie cyberbezpieczeństwa realizuje Federalna Służba Wywiadowcza (Bundesnachrichtendienst-BND), prowadząc rozpoznanie zagrożeń w cyberprzestrzeni pochodzących spoza Niemiec. BND pełni kluczową rolę w zakresie rozpoznawania przeciwdziałania atakom cybernetycznym o charakterze międzynarodowym, zwłaszcza w tych pochodzących od obcych służb wywiadowczych, grup przestępczych lub

[16] Bundeskriminalamtgesetz z 7 lipca 2017, BGBl.I.S.3202
[17] Bundesverfassungsschutzgesetz ; Inkrafttreten am: 29. September 1950; Letzte Neufassung vom: 20. Dezember 1990 (BGBl. i S. 2954, 2970).

organizacji sponsorowanych przez państwa trzecie[18]. BND ma prawo do prowadzenia strategicznego nadzoru ruchu sieciowego, co umożliwia wykrywanie cyberzagrożeń na wczesnym etapie. Kompetencje te zostały doprecyzowane w nowelizacji z 2021 r., w której wprowadzono szczegółowe przepisy dotyczące ochrony danych kontroli parlamentarnej nad działalnością wywiadu (BGBI, I, nr 61/2021). W ramach krajowego systemu cyberbezpieczeństwa BND współpracuje z BSI, BfV oraz NCAZ. Współpraca ta ma charakter operacyjno-analityczny. Koncentrując się na wymianie. Informacje o zagrożeniach oraz ocenie potencjalnych kampanii cyberataków wymierzonych w infrastrukturę państwową i strategiczne sektory gospodarki .

Komponent wojskowy stanowi dowództwo cyberprzestrzeni i przestrzeni informacyjnej Bundeswehry (Bundeswehrcyber -und informationsraum CIR) zostało utworzone w 2017 r. jako odrębny rodzaj sił zbrojnych, obok wojsk lądowych, sił powietrznych, marynarki wojennej. Powstanie CIR było odpowiedzią na rosnące znaczenie przestrzeni cyfrowej jako obszaru działań operacyjnych oraz konieczność zapewnienia zdolności obronnych Niemiec w cyberprzestrzeni. Podstawowym zadaniem jest ochrona systemów informatycznych Bundeswehry, a także przeprowadzenie działań obronnych i ofensywnych w cyberprzestrzeni, zgodnie z systemem prawa międzynarodowego. W ramach swojej struktury odpowiada za monitorowanie i analizę zagrożeń w cyberprzestrzeni, reagowanie na incydenty cybernetyczne dotyczące infrastruktury wojskowej, wsparcie operacji wojskowych w zakresie informacji i komunikacji, współpracę z cywilnymi instytucjami odpowiedzialnymi za cyberbezpieczeństwo, w tym BSI i NCAZ. Dowództwo CIR podlega bezpośrednio Federalnemu Ministrowi Obrony ( BMVg). CIR uczestniczy w pracach Narodowego Centrum Obrony Cybernetycznej (NCAZ) wnosząc wojskowe kompetencje techniczne i analityczne w zakresie ochrony cyberprzestrzeni.

Podstawową platformą współdziałanie wszystkich instytucji w ramach krajowego systemu cyberbezpieczeństwa jest Narodowe Centrum obrony cybernetycznej ( Nationale Cyber - Abwehrzentrum - NCAZ) utworzone w 2011 roku. Jego celem jest bieżąca wymiana informacji, analiza incydentów oraz koordynacja reakcji międzyresortowych. W NCAZ uczestniczą przedstawiciele BSI, BMI, BKA, BND, BfV oraz Bundeswery. Na poziomie strategicznym funkcjonuje ponadto narodowa rada do spraw cyberbezpieczeństwa, działająca przy urzędzie kanclerskim, która ingeruje przedstawiciel rządu federalnego krajów związkowych, sektora prywatnego i nauki. Bundeswehra może również wykorzystać swoje elementy organizacyjne (w tym zespoły reagowania na incydenty) do wniesienia wkładu w ogólne środki bezpieczeństwa w granicach konstytucyjnych[19].

[18] (Bundesnachrichtendienstgestez - z 23 grudnia 2016, BGBI.I.S.2826).
[19] A. Bendiek, Sorgfaltsverantwortung im Cyberraum: Leitlinien für eine deutsche Cyber-Außen- und Sicherheitspolitik, Berlin 2016, s. 13.

Centrum Obrony Cybernetycznej (Nationale Cyber-Abwehrzentrum Cyber A-Z) zostało utworzone w 2011 r. jako międzyresortowa platforma współpracy i niemieckich organów bezpieczeństwa w zakresie wczesnego wykrywania, analiz i reagowania na cyberzagrożenia. Centrum nie jest samodzielnym urzędem administracyjny, lecz instytucję koordynującą, której zadaniem jest integracja działań organów federalnych w ramach krajowego systemu cyberbezpieczeństwa. Jego funkcjonowanie zostało szczegółowo wymienione w dokumentacji wykonawczej BMI i w strategii cyberbezpieczeństwa w 2021 r. Centrum funkcjonuje w strukturze BSI, który pełni funkcję gospodarza i zapewnienie zaplecze administracyjne oraz techniczne. Głównym celem powołania centrum jest wzmocnienie zdolności państwa do ochrony przed złożonymi atakami cybernetycznym, które przekraczają kompetencje pojedynczej instytucji. Do podstawowych zadań należą: koordynację działań między instytucjami odpowiedzialnymi za bezpieczeństwo cybernetyczne, wymiana informacji o incydentach i zagrożeniach w czasie rzeczywistym, analizy skutków cyberataków na infrastrukturę krytyczną oraz systemy administracji publicznej, opracowanie rekomendacji dla organów federalnych i landów w zakresie reagowania na incydenty., udział w krajowych i międzynarodowych ćwiczeniach cybernetycznych. Cyber A-Z nie posiada uprawnień operacyjnych ani dochodzeniowych, jego rola, polega na koordynacji i analizie, a działania praktyczne podejmujące podejmują instytucje wchodzące w jego skład. W skład Cyber A-Z wchodzą: BSI, BMI, BKA, BfV, BND, Bundeswehr (CIR), BBK (Federalny Urząd Ochrony Ludności i pomocy w katastrofach). W razie potrzeby do prac Cyber A-Z mogą być zaproszeni eksperci z innych instytucji federalnych, landów oraz przedstawiciele sektora prywatnego. W konsekwencji NCAZ potrafi w krótkim czasie przedstawić aktualną i kompleksową informację na temat zagrożeń dla cyberprzestrzeni[20].

Niezbędna jest współpraca rządu federalnego z landami. Centralne organy koordynujące współpracę federalno-krajową na poziomie strategicznym to Konferencja Ministrów Spraw Wewnętrznych i jej krajowa grupa robocza ds. cyberbezpieczeństwa, a także Rada Planowania IT i jej grupa robocza ds. bezpieczeństwa informacji. Te ostatnie są również odpowiedzialne za zarządzanie bezpieczeństwem informacji między rządami federalnymi i stanowymi (Strategia 2021, s 21). Istnieje wiele form współpracy między rządem a landami. Przede wszystkim jest to współpraca w ramach CERT (VCV) czy ścisła koordynacja stanowych urzędów policji kryminalnej- BKA jako centralnym urzędem policji. W tę współpracę operacyjną ściśle zaangażowane są także centralne biura koordynacyjne ds. cyberbezpieczeństwa, tworzone coraz częściej przez kraje związkowe i połączony jest z BSI[21].

[20] K. Sacewicz, op.cit., s. 129-130; I. Oleksiewicz, Polityka bezpieczeństwa cybernetycznego RFN, „Studia Bobolanum" 2017, nr 3, s. 47-51.
[21] Strategia cyberbezpieczeństwa Niemiec z 2021, s. 21.

## Dyrektywa NIS 2

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. Dyrektywa NIS 2 wcześniejszą dyrektywę NIS z 2016 r. wprowadza szereg rozwiązań dla państw członkowskich, administracji publicznej i przedsiębiorstw obejmując swoją regulacją znacznie więcej sektorów. Przede wszystkim wyróżnia dwa typy podmiotów: podmioty kluczowe, tj. energetyka, transport, bankowość, zdrowie, infrastruktura cyfrowa i administracja publiczna oraz podmioty ważne, tj. usługi pocztowe, gospodarka odpadami, przemysł, produkcja żywności, producenci sprzętu IT i obbejmuje także średnie i duże przedsiębiorstwo z tych sektorów powyżej 50 pracowników lub 10 milionów euro obrotu. Dyrektywa NIS 2 wprowadza minimalne standardy bezpieczeństwa, takie jak analiza ryzyka i zarządzanie incydentami bezpieczeństwa, łańcucha dostaw i polityki bezpieczeństwa. Wprowadza obowiązek zgłoszenia incydentu cybernetycznego do krajowego CISIRT, dzieląc zgłoszenie do 24 godzin, szczegółowy raport w ciągu 72 godzin, a raport końcowy po rozwiązaniu incydentu. Dyrektywa wprowadza także obowiązek informowania użytkowników, jeśli incydent może mieć wpływ na działanie. Każde państwo musi wyznaczyć organ właściwy do spraw cyberbezpieczeństwa, posiadać krajowe CISIRT i opracować strategię cyberbezpieczeństwa oraz uczestniczyć w sieci współpracy CISIRT. Wprowadza wysokie sankcje za naruszenie w wysokości oraz do 10 milionów euro lub 2% rocznego obrotu dla podmiotów kluczowych 7 milionów euro lub ¼ % obrotu dla podmiotów ważnych. Możliwe jest także zastosowanie środków administracyjnych, na przykład nakaz wdrożenia działań naprawczych. Państwa członkowskie UE mają czas na wdrożenie NIS 2 do 17października 2024 roku.

Dyrektywa NIS 2 wprowadziła znaczące zmiany w systemie cyberbezpieczeństwa Niemiec. Jej implementację wymusiła nowelizację niemieckiej ustawy o cyberbezpieczeństwie informatycznym IT- 3 0 oraz ustawy o BSI. Federalny Urząd ds. Bezpieczeństwa Informacji - BSI pozostał centralnym organem właściwym do spraw bezpieczeństwa, ale jego rola została rozszerzona i ma teraz pełnić funkcję krajowego organu właściwego, organu CISIRT, punktu kontaktowego w ramach Współpracy Europejskiej, koordynatora sektora publicznego i prywatnego w zakresie reagowania na incydenty.

W zakresie zmiany ustawy IT-Sicherheistsgesetz 3.0[22] projekt implementacji dotyczy zmian w zakresie podziału podmiotów na kluczowe i ważne oraz wskazania więcej sektorów, takich jakie wymieniła dyrektywa NIS 2. Wprowadzenie nowych lub wzmocnionych obowiązkiem zarządzania ryzykiem, bezpieczeństwo łańcucha dostaw i obowiązek zgłaszania incydentów w określonym terminie oraz wymogi dotyczące zarządzania i odpowiedzialności kierownictwa. Wzmocnienie roli organu nadzorczego, czyli BSI oraz o nadzoru technicznego i regulującego, tj. nadawanie na przykład wyższego statusu

[22] IT-Sicherheistsgesetz 3.0.

normatywnego dla standardów zabezpieczeń, a także zwiększenia ich zakresu kompetencji kontrolnych i audytowych (IT-3.0).

Kluczowe zmiany nastąpiły w projektowanej utsawie o BSI. W § 28 projektu ustawy o BSI dokonano rozszerzenie zakresu zastosowania prawa, co oznacza, że więcej podmiotów zostanie objętych obowiązkiem regulacji ustawy. W § 30 wprowadzono nowe wymogi zarządzania ryzykiem TI i bezpieczeństwo łańcucha dostaw. Projekt wprowadza obowiązek identyfikację i edukacji ryzyk, nadzoru nad dostawcami i wskazania działań zabezpieczających. Rozwiązanie te wynikają z art. 21 Dyrektywy NIS 2. W § 32 wprowadzono nowy trzystopniowy system zgłaszania incydentów. Pierwszy incydent w ciągu 24 godzin, raport szczegółowy w ciągu 72 godziny i raport kończący w ciągu miesiąca od zdarzenia zamiast jednolitego systemu zgłoszenia. W §330 34 wprowadzono zasady rejestracji, tzn. podmioty zostaną sklasyfikowane w 2 nowych kategoriach z obowiązkami odmiennymi dla każdej z nich. W § 38 wprowadzono przepisy o odpowiedzialności kierownictwa lub przedstawicieli zarządu za niedopełnienie obowiązków w zakresie bezpieczeństwa IT. W § 61 i 62 poszerzono uprawnienia nadzorcze BSI poprzez możliwość dokonywania kontroli, audytu, wdrożenia nakazów bezpieczeństwa i nakładania sankcji administracyjnych. Rząd niemiecki przyjął projekt ustawy wdrażającej wstępnie 24 lipca 2024 roku, jednak pełna implementacja w Niemczech została opóźniona i jest nadal w trakcie procesu legislacyjnego.

## Podsumowanie

Polityka federalnego rządu niemieckiego w zakresie cyberbezpieczeństwa jest spójna z polityką cyberbezpieczeństwa Unii Europejskiej. Niemcy już od pierwszej ustawy w zakresie cyberbezpieczeństwa w 2009 r. i strategii cyberbezpieczeństwa w 2011 r. konsekwentnie wskazują organy właściwe w zakresie cyberbezpieczeństwa. Ustawa o bezpieczeństwie sieci teleinformatycznych IT - 2.0 i następne akty prawne wynikające z implementacji dytektywy NIS z 2016 r., a następnie NIS-2 i zmiany w projektowanych ustawach IT-30 i ustawie o BSI szczególne wzmocniły kompetencje BSI jako organ właściwy w zakresie cyberbezpieczeństwa To właśnie Federalne Biuro Bezpieczeństwa Informacji -BSI wyposażone zostało w coraz większe kompetencje, stało się głównym organem zapewniającą ochronę cyberbezpieczeństwa cywilnego w Niemczech, nie naruszając kompetencji innych organów w ich zakresie działania. Zmiany jakie przynosi wdrożenie NIS - 2 stanowi jakościową zmianę w podejściu państwa do ochrony cyberprzestrzeni. BSI z instytucji o charakterze technicznym przekształciło się w centralny organ regulacyjny, zdolny do wydawania wiążących decyzji, nadzorowanie podmiotów publicznych oraz prywatnych. Nowy model oparty na ścisłej współpracy BSI, BMI i organów ścigania, odpowiada europejskim standardom zarządzania

bezpieczeństwem cyfrowym wzmacniając zdolność Niemiec do reagowania na zagrożenia hybrydowe i cybernetyczne.

## Bibliografia

Bendiek A., Sorgfaltsverantwortung im Cyberraum: Leitlinien für eine deutsche Cyber-Außen- und Sicherheitspolitik, Berlin 2016.

Guitton C., Cyber insecurity as a national threat: overreaction from Germany, France and the UK?, „European Security" 2013, no. 22(1).

Mickiewicz P., System bezpieczeństwa cybernetycznego państw europejskich. Analiza porównawcza, „Rocznik Bezpieczeństwa Międzynarodowego" 2017, vol. 11, nr 1.

Oleksiewicz I., Polityka bezpieczeństwa cybernetycznego RFN, „Studia Bobolanum" 2017, nr 3.

Sacewicz K., Niemiecka strategia ochrony cyberprzestrzeni, „Przegląd Bezpieczeństwa Wewnętrznego" 2021, t. 4, nr 7.

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) (Dz.U. L 333 z 27.12.202).

Strategia cybernetyczna Niemiec 2011 (niem. Cyber Sicheritstrategie fur Deutschland 2011). https://www.cio.bund.de/SharedDocs/Publikationen/DE/Strategische-Themen/css_download.pdf?__blob=publicationFile.

Strategia cyberbepieczństwa Niemiec 2016, (niem. Cyber- Sicherheitsstrategie für Deutschland 2016). Strategia cyberbezpieczeństwa Niemiec 2021 (Cybersicherheitsstrategie für Deutschland 2021), https://www.bmi.bund .de/DE/themen/it-und-digitalpolitik/it-und-cybersicherheit/cyber-sicherheitsstrategie/cyber-sicherheitsstrategie-node.html.

Strategia cyberbezpieczeństwa Niemiec 2021, (Cybersicherheitsstrategie für Deutschland 2021), https://www.bmi.bund.de/DE/themen/it-und-digitalpolitik/it-und-cybersicherheit/cyber-sicherheitsstrategie/cyber-sicherheitsstrategie-node.html.

Zweite Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0) tł. Druga ustawa o zwiększeniu bezpieczeństwa systemów informatycznych (ustawa o bezpieczeństwie IT 2.0). https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/IT-Sicherheitsgesetz.pdf?__blob=publicationFile&v=1.

IT-Sicherheistsgesetz 3.0, https://www.gesetze-im-internet.de/bsig_2009/BJNR282110009.html.

Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung, Drucksache 21/1501.