Monika OJDANA-KOŚCIUSZKO
Uniwersytet w Siedlcach
Wydział Nauk Społecznych
monika.ojdana-kosciuszko@uws.edu.pl
http://orcid.org/0000-0003-0150-2953
https://doi.org/10.34739/dsd.2024.01.07

EWOLUCJA I WYZWANIA POLSKIEGO SYSTEMU CYBERBEZPIECZEŃSTWA

ABSTRAKT: Celem artykułu jest kompleksowe omówienie rozwoju i strategii Krajowego Systemu Cyberbezpieczeństwa w Polsce. Analizowane są etapy rozwoju, które obejmują istotne wydarzenia legislacyjne i technologiczne, kształtujące aktualny stan systemu. Artykuł koncentruje się na ochronie infrastruktury krytycznej oraz zarządzaniu incydentami cybernetycznymi, co ma kluczowe znaczenie dla zapewnienia bezpieczeństwa narodowego. W kontekście rosnących zagrożeń, takich jak ataki ransomware oraz dynamiczny rozwój technologii 5G i IoT, podkreślane jest znaczenie międzynarodowej współpracy. Polska jako członek Unii Europejskiej i NATO aktywnie uczestniczy w globalnych inicjatywach na rzecz wymiany wiedzy i najlepszych praktyk. Artykuł przedstawia, jak te działania przekładają się na budowanie odpornego systemu cyberbezpieczeństwa, zdolnego do adaptacji w obliczu szybko zmieniających się technologii i zagrożeń. Dodatkowo artykuł ukazuje perspektywy rozwoju systemu w Polsce, z naciskiem na ciągłe monitorowanie, adaptację oraz inwestycje w rozwój kadr specjalistycznych. Zwraca uwagę na konieczność edukacji i podnoszenia świadomości społeczeństwa w zakresie cyberbezpieczeństwa, co jest istotne dla skutecznej ochrony przed coraz bardziej zaawansowanymi zagrożeniami cyfrowymi.

SŁOWA KLUCZOWE: bezpieczeństwo, cyberbezpieczeństwo, infrastruktura krytyczna, zagrożenia cyfrowe, CSIRT

EVOLUTION AND CHALLENGES OF THE POLISH CYBERSECURITY SYSTEM

ABSTRACT: The purpose of the article is to comprehensively discuss the development and strategies of the National Cybersecurity System in Poland. It analyzes key developmental stages, including significant legislative and technological events shaping the current state of the system. The article focuses on the protection of critical infrastructure and the management of cyber incidents, which are crucial for ensuring national security. In the context of increasing threats, such as ransomware attacks and the dynamic development of 5G and IoT technologies, the importance of international cooperation is emphasized. As a member of the European Union and NATO, Poland actively participates in global initiatives for the exchange of knowledge and best practices. The article illustrates how these efforts contribute to building a resilient cybersecurity system capable of adapting to rapidly changing technologies and threats. Additionally, the article presents future development prospects for the system in Poland, emphasizing continuous monitoring, adaptation, and investment in the development of specialized personnel. It highlights the necessity of education and raising public awareness about cybersecurity, which is crucial for effective protection against increasingly sophisticated digital threats.

KEYWORDS: security, cybersecurity, critical infrastructure, digital threats, CSIRT

WPROWADZENIE

W dobie rosnących zagrożeń w cyberprzestrzeni[1] jednym z kluczowych wyzwań dla państw na całym świecie stało się cyberbezpieczeństwo. Skuteczne zarządzanie bezpieczeństwem cyfrowym jest niezbędne dla ochrony infrastruktury krytycznej, zachowania ciągłości działania instytucji państwowych oraz zapewnienia bezpieczeństwa obywateli. Polska jako członek Unii Europejskiej i NATO również stoi przed wyzwaniami związanymi z dynamicznym rozwojem technologii i rosnącą liczbą cyberataków.

Celem niniejszego artykułu jest przedstawienie historii oraz głównych strategii Krajowego Systemu Cyberbezpieczeństwa w Polsce. W pierwszej części omówione zostaną etapy rozwoju polskiego systemu cyberbezpieczeństwa, z uwzględnieniem kluczowych wydarzeń legislacyjnych i technologicznych, które ukształtowały jego obecny kształt. Następnie przeanalizowane zostaną główne strategie ochrony infrastruktury krytycznej oraz zarządzania incydentami i kryzysami cybernetycznymi.

Kontekst globalnych wyzwań w cyberbezpieczeństwie, takich jak ataki ransomware czy rosnące zastosowanie technologii 5G i Internetu Rzeczy (IoT), podkreśla potrzebę skoordynowanych działań na poziomie krajowym i międzynarodowym. W związku z tym Polska nieustannie dostosowuje swoje podejście do cyberbezpieczeństwa, inwestując w rozwój kadr specjalistycznych, technologie oraz międzynarodową współpracę. Artykuł ma na celu ukazanie, jak te działania przekładają się na budowanie odpornego systemu ochrony cybernetycznej w Polsce oraz jakie są perspektywy w kontekście dynamicznie zmieniającego się krajobrazu zagrożeń cyfrowych.

METODOLOGIA

W niniejszym artykule zastosowano podejście wieloaspektowe, obejmujące zarówno analizę porównawczą, jak i badania przypadków. Taka metoda badawcza pozwala na wszechstronne zrozumienie dynamiki polskiego systemu cyberbezpieczeństwa oraz wyzwań związanych z zarządzaniem incydentami cybernetycznymi.

Analiza porównawcza strategii cyberbezpieczeństwa – dokonano przeglądu oraz porównania zmian strategii cyberbezpieczeństwa stosowanych w Polsce w związku ze zmieniającymi się zagrożeniami. Analiza ta skupiła się na identyfikacji najważniejszych elementów strategii, takich jak polityki prewencyjne, mechanizmy reakcji na incydenty oraz współpraca międzynarodowa.

Badania przypadków (*case studies*) – przeanalizowano konkretne przypadki incydentów cybernetycznych, które miały miejsce w polskim systemie cyberbezpieczeństwa w ostatnich latach. Każdy przypadek został dokładnie zbadany pod kątem przyczyn, przebiegu i konsekwencji incydentu, jak również zastosowanych środków zaradczych. Dane do analizy przypadków pochodziły z publicznie dostępnych raportów incydentów, publikacji branżowych, komunikatów prasowych oraz wywiadów z ekspertami ds. cyberbezpieczeństwa. Użyto również anonimowych źródeł

[1] R. Burda, *Detection Tools for Cognitive Warfare: Leveraging the Cyber Domain*, STO NATO, 2024.

w postaci wypowiedzi pracowników odpowiedzialnych za zarządzanie incydentami w sektorze publicznym i prywatnym. Analiza przypadków pozwala na zidentyfikowanie słabych punktów w istniejących systemach oraz proponowanie rekomendacji dla przyszłych działań.

Głównym problemem badawczym niniejszego artykułu jest odpowiedź na pytanie: „Jakie są kluczowe wyzwania dla rozwoju polskiego systemu cyberbezpieczeństwa w kontekście dynamicznie zmieniającego się krajobrazu zagrożeń cybernetycznych?".

HISTORIA I ROZWÓJ POLSKIEGO SYSTEMU CYBERBEZPIECZEŃSTWA

Rozwój polskiego systemu cyberbezpieczeństwa[2] można prześledzić przez pryzmat różnych etapów legislacyjnych i technologicznych, które kształtowały jego obecną strukturę. Pierwsze znaczące kroki w tym kierunku zostały podjęte na początku XXI wieku, kiedy to zwiększająca się liczba ataków cybernetycznych na instytucje państwowe i prywatne zwróciła uwagę na potrzebę systematycznych działań w tym obszarze. Ta rosnąca świadomość zagrożeń cyfrowych, zarówno w skali krajowej, jak i globalnej, spowodowała, że bezpieczeństwo cybernetyczne stało się kluczowym elementem narodowej strategii bezpieczeństwa.

Proces rozwoju polskiego systemu cyberbezpieczeństwa nie był jedynie reakcją na cyberataki, lecz również próbą przewidywania przyszłych zagrożeń oraz odpowiedniego przygotowania infrastruktury krytycznej i społeczeństwa na ich potencjalne skutki. Wraz z dynamicznym rozwojem technologii, Polska musiała dostosowywać swoje podejście do cyberbezpieczeństwa, co wymagało systematycznych i przemyślanych działań legislacyjnych oraz technologicznych.

Jednym z kluczowych wyzwań, przed jakimi stanęła Polska, była globalna koordynacja działań na rzecz cyberbezpieczeństwa[3]. Ataki ransomware, takie jak WannaCry i NotPetya, które miały miejsce w latach 2017-2018, ukazały skalę i potencjalne skutki cyberataków, podkreślając potrzebę globalnej współpracy i wymiany informacji między państwami. Polska jako członek Unii Europejskiej i NATO intensywnie współpracowała z międzynarodowymi partnerami w celu wymiany najlepszych praktyk oraz rozwijania wspólnych strategii obrony przed cyberzagrożeniami.

W miarę rozwoju technologii i eskalacji cyberzagrożeń polski system cyberbezpieczeństwa ewoluował, dostosowując się do nowych wyzwań i zagrożeń, co przedstawiono w tabeli 1.

Tabela 1. Kluczowe wydarzenia i rozwój systemu cyberbezpieczeństwa w Polsce

Rok	**Zdarzenia i rozwój zagrożeń**	**Podjęte działania i odpowiedzi prawne**
2000	Rozwój społeczeństwa	Polska zaangażowała się w budowę ery informacyjnej, wykorzystując nowoczesne technologie, zapewniając dostęp do informacji i rozwijając potencjał intelektualny

[2] Uchwała nr 125 Rady Ministrów z dnia 22 października 2019 r. w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024, 2019 (M.P. 2019 poz. 1037).

[3] *NotPetya and WannaCry Call for a Joint Response from International Community*, https://ccdcoe.org/news/2017/notpetya-and-wannacry-call-for-a-joint-response-from-international-community/ (10.06.2024).

Rok	Zdarzenia i rozwój zagrożeń	Podjęte działania i odpowiedzi prawne
	informacyjnego[4].	i gospodarczy. W związku z integracją z Unią Europejską konieczne jest dostosowanie polskich standardów do nowoczesnego społeczeństwa informacyjnego.
2004	Wstąpienie Polski do Unii Europejskiej, co zwiększyło wymogi dotyczące bezpieczeństwa informacji i systemów teleinformatycznych[5].	Implementacja dyrektyw unijnych dotyczących ochrony danych osobowych i bezpieczeństwa informacji.
2016	Dyrektywa NIS (Network and Information Security) przez UE.	Polska zintegrowała wymogi dyrektywy NIS z krajowym prawodawstwem, aktualizacja ustaw i stworzenie nowych regulacji.
2018	Wdrożenie Ustawy o krajowym systemie cyberbezpieczeństwa[6].	Tworzenie specjalistycznych jednostek cyberbezpieczeństwa, wprowadzenie wymogów dla kluczowych operatorów usług[7].
2020	Pandemia COVID-19 i wzrost zagrożeń cybernetycznych związanych z pracą zdalną[8].	Zwiększone inwestycje w technologie zdalnego monitorowania i zabezpieczania danych.
Od 2021	Wojna na Ukrainie[9].	Wprowadzanie stopni alarmowych CHARLIE-CRP, wydawanie rekomendacji NASK.
2022	Rozwój technologii 5G i IoT, nowe zagrożenia cybernetyczne[10].	Bezpieczeństwa 5G i IoT.
2023	Zwiększona współpraca międzynarodowa w zakresie cyberbezpieczeństwa[11].	Intensyfikacja współpracy z UE i NATO, wymiana najlepszych praktyk.

Źródło: Opracowanie własne.

Wprowadzenie dyrektywy NIS przez Unię Europejską w 2016 roku było jednym z kluczowych momentów dla polskiego systemu cyberbezpieczeństwa. Dyrektywa ta narzuciła nowe wymagania dotyczące bezpieczeństwa sieci i informacji, zmuszając państwa członkowskie do podjęcia konkretnych działań w celu zapewnienia ochrony swojej infrastruktury krytycznej. Polska, integrując wymogi dyrektywy NIS z krajowym prawodawstwem, podjęła

[4] Ministerstwo Łączności, *ePolska. Plan działań na rzecz rozwoju społeczeństwa informacyjnego w Polsce na lata 2001-2006*, 2001.
[5] Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej), (Dz.U.UE.L.2002.201.37), https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32002L0058 (11.06.2024).
[6] Ustawa z dnia 5 lipca 2018 o krajowym systemie cyberbezpieczeństwa (Dz.U. 2018 poz. 1560).
[7] M. Wrzosek (red.), *Raport. Cyberbezpieczeństwo A.D. 2018*, NASK, 2019.
[8] E. Kasprzyk, *Pandemia COVID-19 a cyfryzacja w regionie Trójmorza*, [w:] *Raport: Three Seas United in Cyber Power*, Instytut Kościuszki, Kraków, 2022.
[9] *Rzeczpospolita*, https://www.rp.pl/biznes/art40326141-cybernetyczna-wojna-neka-firmy-i-instytucje (06.01.2024).
[10] *Na fali nauki*, https://nafalinauki.pl/bezpieczenstwo-w-erze-5g-nowe-wyzwania-i-rozwiazania/ (18.08.2023).
[11] *Kształtowanie cyfrowej przyszłości Europy*, https://digital-strategy.ec.europa.eu/pl/news/european-union-and-nato-intensify-cooperation-addressing-cyber-threats, European Union, 2024 (10.06.2024).

niezbędne kroki w celu aktualizacji istniejących ustaw oraz stworzenia nowych regulacji, które miały na celu zwiększenie poziomu ochrony przed cyberzagrożeniami.

W 2018 roku Polska przyjęła Ustawę o krajowym systemie cyberbezpieczeństwa[12], która była wynikiem długoletnich doświadczeń i analizy zmieniającego się środowiska zagrożeń. Ustawa ta miała na celu ujednolicenie oraz zwiększenie efektywności działań w zakresie cyberbezpieczeństwa na poziomie krajowym. Przewidywała ona tworzenie specjalistycznych jednostek cyberbezpieczeństwa, które miały koordynować działania i reakcje na incydenty, a także wprowadzenie wymogów bezpieczeństwa dla kluczowych operatorów usług. Wdrożenie ustawy było istotnym krokiem w kierunku zbudowania bardziej odpornego systemu ochrony cybernetycznej w Polsce.

W miarę jak technologia nadal się rozwija, Polska musi być gotowa na nowe wyzwania. Sieci 5G, Internet Rzeczy (IoT) oraz rosnące zastosowanie sztucznej inteligencji stanowią nowe obszary, które wymagają szczególnej uwagi i odpowiednich środków ochrony. W związku z tym przyszłość polskiego systemu cyberbezpieczeństwa będzie zależała od ciągłego monitorowania i adaptacji do zmieniającego się krajobrazu technologicznego i zagrożeń. Inwestycje w edukację, rozwój kadr specjalistycznych oraz międzynarodowa współpraca będą kluczowymi elementami zapewniającymi skuteczność działań w zakresie cyberbezpieczeństwa w nadchodzących latach.

Podsumowując, można stwierdzić, że rozwój polskiego systemu cyberbezpieczeństwa to dynamiczny proces, który wymaga stałej adaptacji do zmieniających się technologii i zagrożeń. Polska, poprzez przyjęcie odpowiednich regulacji prawnych oraz budowanie struktury organizacyjnej, stara się skutecznie chronić swoją infrastrukturę krytyczną oraz społeczeństwo przed cyberzagrożeniami. Współpraca międzynarodowa oraz inwestycje w nowe technologie i kadry specjalistyczne są kluczowymi elementami, które będą decydować o przyszłym bezpieczeństwie cybernetycznym kraju.

STRATEGIE I WYZWANIA W OCHRONIE INFRASTRUKTURY KRYTYCZNEJ

W obliczu rosnących zagrożeń w cyberprzestrzeni skuteczność narodowego systemu cyberbezpieczeństwa staje się podstawą dla zapewnienia ciągłości funkcjonowania państwa i ochrony infrastruktury krytycznej. Krajowy System Cyberbezpieczeństwa (KSC) można analizować pod dwoma aspektami[13]:

- ochrony infrastruktury krytycznej;
- zarządzania incydentami i kryzysami cybernetycznymi.

Takie podejście do strategii KSC, uwzględniające zarówno prewencję, jak i reakcję na same incydenty, zapewni kompleksową ochronę bezpieczeństwa i odporność cyfrową na potencjalne zagrożenia. Realizacja tych zadań wymaga jednak skoordynowanych działań na wielu

[12] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie…, *op. cit.*

[13] S. Stalmach, *Cztery obszary cyberbezpieczeństwa – omówienie zakresu tematycznego*, „Przegląd Policyjny" 2021, t. 141, s. 98-99.

poziomach administracji oraz zaangażowania podmiotów prywatnych i międzynarodowych partnerów.

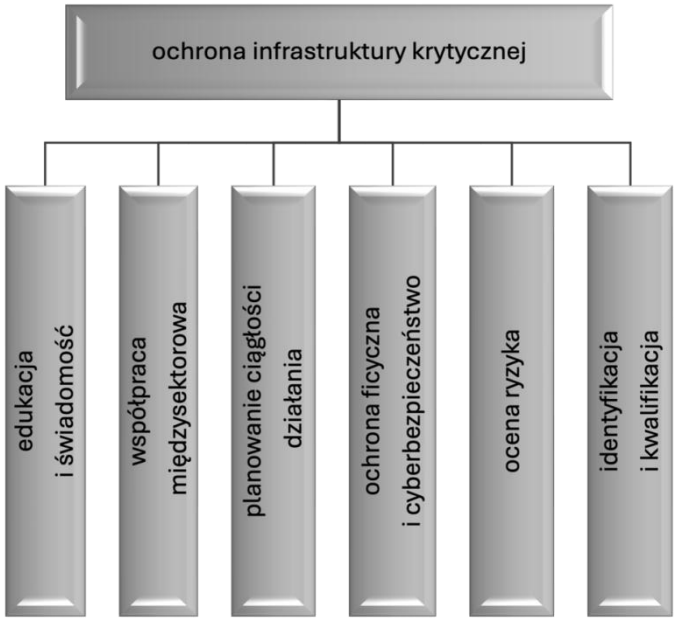
Infrastruktura krytyczna odgrywa kluczową rolę w funkcjonowaniu państwa i codziennym życiu jego obywateli. Jej ochrona przed zagrożeniami cybernetycznymi jest priorytetem dla polskiego systemu cyberbezpieczeństwa. W ostatnich latach Polska doświadczyła kilku znaczących incydentów, które uwidoczniły potrzebę wzmocnienia zabezpieczeń:

1. Atak na polską sieć kolejową[14] – w sierpniu 2023 roku polska sieć kolejowa stała się celem hakerów, którzy zakłócili jej działanie poprzez transmisję sygnału radiowego. Atak ten spowodował awaryjne zatrzymanie około 20 pociągów w północno-zachodniej Polsce, co ujawniło luki w bezpieczeństwie komunikacji radiowej używanej przez polskie koleje.
2. Cyberatak na polską infrastrukturę krytyczną[15] – w marcu 2024 roku polskie służby cyberbezpieczeństwa udaremniły skoordynowany atak na infrastrukturę krytyczną, który miał na celu destabilizację kraju. Atak, przypisywany grupom powiązanym z Rosją, miał na celu zakłócenie działalności operacyjnej w Polsce, będącej kluczowym węzłem transportowym dla wsparcia Ukrainy. W odpowiedzi na te zagrożenia rząd Polski ogłosił plan inwestycji ponad 3 miliardów złotych w ramach tzw. cybertarczy, mającej na celu wzmocnienie ochrony cybernetycznej.
3. Ataki na polską infrastrukturę telekomunikacyjną – w 2022 roku Polska była celem licznych cyberataków, głównie ze strony grup powiązanych z Rosją. Ataki te były częścią szerszej strategii wojny hybrydowej, która miała na celu destabilizację kraju. W ramach tych incydentów przeprowadzono zarówno ataki typu ransomware, jak i phishing, mające na celu wyłudzenie danych i pieniędzy oraz dezinformację, co pokazało potrzebę rozwinięcia zdolności do obrony przed tego rodzaju zagrożeniami.

W kontekście ataków cybernetycznych raport CERT Polska[16] wskazuje na rosnącą liczbę incydentów związanych z bezpieczeństwem informacyjnym, które mogą prowadzić do zakłóceń w funkcjonowaniu kluczowych usług publicznych, takich jak edukacja i służba zdrowia. Ponadto takie wydarzenia negatywnie wpływają na rozwój gospodarczy kraju. Dlatego ochrona infrastruktury krytycznej jest jednym z priorytetów państwa polskiego. Zadania związane z tą infrastrukturą obejmują nie tylko zapewnienie jej ochrony przed zagrożeniami, ale także minimalizowanie czasu trwania ewentualnych uszkodzeń i zakłóceń oraz zapewnienie ich łatwego usunięcia, aby uniknąć dodatkowych strat dla obywateli i gospodarki.

[14] W. Kość, *Polish train chaos blamed on radio hackers*, 28.08.2023, https://www.politico.eu/article/poland-train-chaos-radio-hackers-russia-ukraine-war/ (10.05.2024); *Cyber hackers target Polish rail network, cause operational disruptions*, 29.08.23, https://industrialcyber.co/transport/cyber-hackers-target-polish-rail-network-cause-operational-disruptions/ (10.05.2024).
[15] O. Mukhina, *Hacker attack averted in Poland amid cyberwar with Russia*, 03.06.2024, https://euromaidanpress.com/2024/06/03/hacker-attacks-averted-in-poland-amid-cyberwar-with-russia/ (15.05.2024).
[16] *Raport roczny z działalności CERT Polska 2017*, CERT Polska, 2018..

Ochrona infrastruktury krytycznej obejmuje wszelkie działania mające na celu zapewnienie jej funkcjonalności, ciągłości działania i integralności. Działania te zapobiegają zagrożeniom, ryzykom i słabym punktom oraz ograniczają i neutralizują ich skutki[17]. Ponadto mają na celu szybkie odtworzenie infrastruktury w przypadku awarii, ataków lub innych zdarzeń zakłócających jej prawidłowe funkcjonowanie. W Polsce, w kontekście cyberbezpieczeństwa, kluczowe sektory obejmują energetykę, transport, usługi komunalne, systemy finansowe oraz opiekę zdrowotną. Elementy strategii ochrony infrastruktury krytycznej przedstawiono na rysunku 1.



Rysunek 1. Elementy ochrony infrastruktury krytycznej
Źródło: Opracowanie własne na podstawie: M. Kaźmierczak i S. Byłeń, *Security of critical infrastructure in Poland – selected aspects of research*, „Gospodarka Materiałowa i Logistyka" 2024, t. 1, s. 30, 31.

Pierwszym elementem strategii ochrony infrastruktury krytycznej jest identyfikacja i klasyfikacja zasobów, systemów i sieci, które są kluczowe dla funkcjonowania społeczeństwa. Proces ten obejmuje określenie, które elementy infrastruktury są najważniejsze i jaką pełnią funkcję. Po zidentyfikowaniu, infrastrukturę klasyfikuje się według stopnia krytyczności oraz potencjalnych skutków awarii. Taka klasyfikacja pozwala na priorytetyzację działań ochronnych i skuteczniejsze zarządzanie zasobami[18].

Kolejnym istotnym elementem jest ocena ryzyka, która polega na analizie zagrożeń i słabości zidentyfikowanej infrastruktury krytycznej. W ramach tego procesu przeprowadza się ocenę prawdopodobieństwa wystąpienia różnych incydentów oraz analizuje potencjalne skutki tych zdarzeń.

[17] M. Barć, *Rodzaje ochrony infrastruktury krytycznej*, „Rocznik Bezpieczeństwa Morskiego" 2021, t. 15, s. 1.
[18] J. Rak, *Zasady określania przynależności do infrastruktury krytycznej*, „Czasopismo Inżynierii Lądowej, Środowiska i Architektury" 2016, s. 294-295.

Ocena ryzyka umożliwia zrozumienie, które zagrożenia są najpoważniejsze i wymagają największej uwagi, co pozwala na efektywne planowanie działań prewencyjnych[19].

Trzecim kluczowym elementem strategii jest wdrażanie środków ochrony fizycznej i cyberbezpieczeństwa. Ochrona fizyczna obejmuje zabezpieczenia budynków, monitoring oraz systemy kontroli dostępu, które mają na celu fizyczne zabezpieczenie infrastruktury przed nieautoryzowanym dostępem i atakami. Cyberbezpieczeństwo jest jednym z najważniejszych aspektów ochrony infrastruktury krytycznej, ponieważ wiele systemów i zasobów zależy od technologii informacyjno-komunikacyjnych (ICT)[20].

W dzisiejszym świecie zagrożenia cyfrowe stają się coraz bardziej zaawansowane, co wymaga wprowadzenia kompleksowych środków ochrony. Tabela 2 przedstawia wybrane składowe cyberbezpieczeństwa w kontekście dynamicznie zmieniającego się krajobrazu zagrożeń.

Tabela 2. Wybrane składowe cyberbezpieczeństwa

Element cyberbezpieczeństwa	**Opis**
Zapory sieciowe (firewalle)	Zapory sieciowe są pierwszą linią obrony przed atakami zewnętrznymi. Działają one jako bariery między zaufanymi i niezaufanymi sieciami, monitorując i kontrolując ruch sieciowy na podstawie ustalonych zasad bezpieczeństwa. Firewalle mogą być sprzętowe, programowe lub hybrydowe i są niezbędne do zapobiegania nieautoryzowanemu dostępowi do sieci wewnętrznych.
Systemy wykrywania i zapobiegania włamaniom (IDS/IPS)	Systemy IDS (Intrusion Detection Systems) i IPS (Intrusion Prevention Systems) są kluczowe w monitorowaniu ruchu sieciowego i identyfikowaniu potencjalnych zagrożeń. IDS analizują ruch w poszukiwaniu oznak naruszeń bezpieczeństwa, natomiast IPS nie tylko wykrywają, ale również aktywnie blokują zidentyfikowane ataki.
Szyfrowanie danych	Szyfrowanie danych jest fundamentalnym mechanizmem ochrony informacji. Polega na przekształcaniu danych w taki sposób, aby były one nieczytelne dla osób nieuprawnionych. Szyfrowanie jest stosowane zarówno dla danych w tranzycie (przesyłanych przez sieć), jak i danych w spoczynku (przechowywanych na nośnikach danych). Stosowanie silnych algorytmów szyfrowania zapewnia, że nawet w przypadku przechwycenia danych przez atakującego będą one bezużyteczne bez odpowiedniego klucza deszyfrującego.
Regularne aktualizacje oprogramowania	Aktualizacje oprogramowania są nieodzownym elementem strategii cyberbezpieczeństwa. Zawierają one poprawki błędów oraz łatki zabezpieczające przed nowo odkrytymi lukami bezpieczeństwa. Regularne aktualizowanie systemów operacyjnych, aplikacji i innych komponentów oprogramowania minimalizuje ryzyko wykorzystania znanych luk przez cyberprzestępców.
Autoryzacja i uwierzytelnianie	Implementacja silnych mechanizmów autoryzacji i uwierzytelniania jest kluczowa dla zapewnienia, że tylko uprawnione osoby mają dostęp do zasobów. Uwierzytelnianie wieloskładnikowe (MFA) zwiększa

[19] A. Wygodny, *Metody prowadzenia audytu cyberbezpieczeństwa: Ustawa o KSC,* „Kontrola Państwowa" 2021, t. 66, nr 2, s. 82-84.
[20] W. Kotłowski, *Teleinformatyczne elementy ochrony infrastruktury krytycznej*. *Bezpieczeństwo infrastruktury krytycznej – wymiar teleinformatyczny*, Kraków 2014.

	poziom bezpieczeństwa, wymagając od użytkowników potwierdzenia tożsamości za pomocą więcej niż jednego czynnika (np. hasło i kod SMS).
Bezpieczeństwo aplikacji	Bezpieczeństwo aplikacji koncentruje się na identyfikacji i eliminacji luk w zabezpieczeniach oprogramowania na etapie jego tworzenia oraz podczas eksploatacji. Stosowanie najlepszych praktyk programistycznych, regularne testowanie zabezpieczeń aplikacji (np. testy penetracyjne) oraz szybkie reagowanie na zgłaszane podatności są kluczowe dla ochrony przed atakami skierowanymi na aplikacje.
Monitoring i analiza logów	Systematyczne monitorowanie i analiza logów z systemów informatycznych pozwala na szybkie wykrywanie nietypowych działań i potencjalnych incydentów bezpieczeństwa. Narzędzia do analizy logów mogą automatycznie identyfikować wzorce wskazujące na próbę włamania lub inne niebezpieczne zachowania, co umożliwia szybką reakcję.
Edukacja i szkolenia	Ludzie są często najsłabszym ogniwem w systemie zabezpieczeń. Dlatego regularne szkolenia i edukacja pracowników w zakresie najlepszych praktyk cyberbezpieczeństwa są niezbędne. Pracownicy powinni być świadomi zagrożeń, takich jak np. phishing, oraz znać procedury postępowania w przypadku wykrycia podejrzanych działań.
Zarządzanie dostępem i uprawnieniami	Kontrola dostępu oparta na zasadzie najmniejszego uprzywilejowania (Least Privilege Principle) zapewnia, że użytkownicy mają dostęp tylko do tych zasobów, które są niezbędne do wykonywania ich obowiązków. Regularne przeglądy uprawnień oraz stosowanie zaawansowanych mechanizmów zarządzania tożsamościami i dostępem pomagają w minimalizacji ryzyka nieautoryzowanego dostępu.

Źródło: Opracowanie własne na podstawie: Cyberbezpieczny samorząd – poradnik, NASK – Państwowy Instytut Badawczy, https://bip4.wokiss.pl/chodziezp/zasoby/files/pozostale/cyberbezpieczenstwo/2023/cs-poradnik-25102023.pdf (20.06.2024).

Implementacja powyższych elementów cyberbezpieczeństwa jest niezbędna do skutecznej ochrony infrastruktury krytycznej przed różnorodnymi zagrożeniami cyfrowymi. Każdy z tych elementów działa synergicznie, tworząc wielowarstwową obronę, która chroni przed atakami oraz minimalizuje skutki potencjalnych incydentów.

Następnym elementem ochrony infrastruktury krytycznej jest planowanie ciągłości działania, które obejmuje opracowanie planów awaryjnych i procedur reakcji na incydenty. Te plany są niezbędne do zapewnienia, że infrastruktura krytyczna może szybko odzyskać sprawność po wystąpieniu zakłóceń[21]. Regularne testowanie i aktualizowanie planów w odpowiedzi na zmieniające się zagrożenia i nowe informacje jest kluczowe dla utrzymania ich skuteczności.

Ważnym aspektem strategii ochrony infrastruktury krytycznej jest również współpraca międzysektorowa. Koordynacja działań między sektorem publicznym a prywatnym jest niezbędna, aby skutecznie chronić kluczowe zasoby. Dodatkowo współpraca z międzynarodowymi

[21] A. Rot, *Ryzyko systemów informatycznych a zarządzanie ciągłością działania w organizacji (Business Continuity Management)*, „Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu" 2010, nr 119, „Informatyka Ekonomiczna" nr 18. *Systemy informacyjne w zarządzaniu*, s. 263-273.

partnerami pozwala na wymianę informacji o zagrożeniach i najlepszych praktykach, co zwiększa efektywność działań ochronnych na poziomie globalnym.

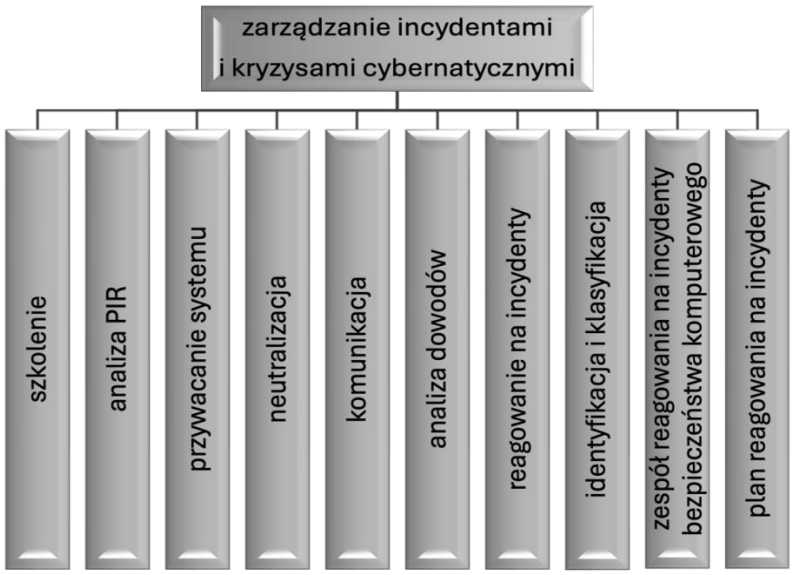
Ostatnim, ale nie mniej ważnym elementem strategii jest edukacja i podnoszenie świadomości. Szkolenia dla pracowników oraz edukacja społeczeństwa na temat zagrożeń i metod ochrony infrastruktury krytycznej są kluczowe dla zapewnienia, że wszyscy zaangażowani mają odpowiednią wiedzę i umiejętności. Regularne szkolenia i ćwiczenia symulacyjne pomagają personelowi odpowiedzialnemu za zarządzanie infrastrukturą krytyczną przygotować się na różne scenariusze i reagować skutecznie na potencjalne incydenty. Te elementy razem tworzą kompleksową strategię ochrony infrastruktury krytycznej, która pozwala na skuteczne zarządzanie zagrożeniami i minimalizowanie ryzyka dla strategicznych zasobów.

Implementacja powyższych elementów cyberbezpieczeństwa jest konieczna do skutecznej ochrony infrastruktury krytycznej przed różnorodnymi zagrożeniami cyfrowymi. Każdy z tych elementów działa synergicznie, tworząc wielowarstwową ochronę przed atakami oraz minimalizując skutki potencjalnych zagrożeń.

ZARZĄDZANIE INCYDENTAMI I KRYZYSAMI CYBERNETYCZNYMI

Podobnie jak ochrona infrastruktury krytycznej, zarządzanie incydentami i kryzysami cybernetycznymi wymaga kompleksowego podejścia. Jest to kolejny kluczowy obszar strategii Krajowego Systemu Cyberbezpieczeństwa. Organizacje muszą być przygotowane na incydenty, które mogą wystąpić pomimo wdrożenia solidnych strategii ochronnych. Skuteczne zarządzanie incydentami i kryzysami cybernetycznymi pozwala minimalizować ich skutki, szybko przywracać normalne funkcjonowanie systemów oraz zapobiegać przyszłym zagrożeniom.

W dzisiejszym silnie zinformatyzowanym świecie zagrożenia cybernetyczne stają się coraz bardziej powszechne i złożone. Organizacje na całym świecie muszą zmierzyć się z wyzwaniami związanymi z ochroną swoich systemów informatycznych przed różnorodnymi atakami. Nawet przy solidnych strategiach ochrony, incydenty cybernetyczne mogą się zdarzyć, a ich skutki mogą być poważne, obejmując straty finansowe, naruszenie prywatności danych oraz uszczerbek na reputacji. W związku z tym skuteczne zarządzanie incydentami i kryzysami cybernetycznymi jest kluczowe dla minimalizacji skutków takich zdarzeń oraz szybkiego przywrócenia normalnego funkcjonowania systemów. Najważniejsze elementy tego procesu przedstawiono na rysunku 2, prezentującym kompleksowy przegląd praktyk i procedur, które mogą pomóc organizacjom w zarządzaniu zagrożeniami cybernetycznymi.



Rysunek 2. Elementy zarządzania incydentami i kryzysami cybernetycznymi
Źródło: Opracowanie własne.

Pierwszym kluczowym elementem zarządzania incydentami i kryzysami cybernetycznymi jest opracowanie i wdrożenie planu reagowania na incydenty (IRP). Plan ten stanowi fundament skutecznego nimi zarządzania. Powinien być szczegółowo opracowany i obejmować wszystkie etapy zarządzania incydentem, od wstępnej jego identyfikacji, przez reakcję, aż po przywrócenie normalnego funkcjonowania systemów i analizę postincydentową[22]. Musi jasno określać role i obowiązki członków zespołu reagowania, przedstawiać procedury eskalacji oraz zasady komunikacji z interesariuszami. Ważne jest, aby IRP był dostosowany do specyfiki organizacji i regularnie aktualizowany w odpowiedzi na zmieniające się zagrożenia i technologie. Wdrożenie IRP wymaga zaangażowania całej organizacji, w tym zarządu, działu IT oraz zespołów operacyjnych. Kluczowym elementem jest przeprowadzenie szkoleń i ćwiczeń symulacyjnych, które pozwalają na przetestowanie planu w praktyce i identyfikację ewentualnych luk w procedurach. Regularne aktualizacje i testy planu są niezbędne, aby zapewnić jego skuteczność w rzeczywistych sytuacjach kryzysowych.

Następnym kluczowym czynnikiem jest utworzenie zespołu reagowania na incydenty bezpieczeństwa komputerowego (CSIRT)[23]. CSIRT to wyspecjalizowany zespół odpowiedzialny za reagowanie na incydenty cybernetyczne. Powinien być złożony z ekspertów w dziedzinie cyberbezpieczeństwa, którzy posiadają wiedzę i doświadczenie niezbędne do skutecznego zarządzania incydentami. Ważne jest, aby zespół był dostępny 24/7, co pozwalałoby na szybką reakcję na incydenty w czasie rzeczywistym. CSIRT pełni kilka istotnych funkcji, w tym takich jak: monitorowanie systemów w celu wykrywania potencjalnych zagrożeń, analiza i ocena incydentów, koordynacja działań naprawczych oraz komunikacja z interesariuszami. Zespół powinien również

[22] T. Gościniak, *Zarządzanie procesami naprawczymi w systemach informatycznych operatorów telekomunikacyjnych*, „Zeszyty Naukowe. Organizacja i Zarządzanie" 2014, nr 70, s. 143-162.
[23] H. Wyrębek, *Cyberprzestrzeń. Zagrożenia. Strategie bezpieczeństwa,* Siedlce 2021, s. 168.

prowadzić regularne szkolenia i ćwiczenia, aby utrzymać wysoką gotowość do reagowania na incydenty. Ważne jest, aby CSIRT współpracował z innymi działami organizacji oraz zewnętrznymi partnerami, co umożliwiałoby skuteczniejsze zarządzanie incydentami.

Kolejnym elementem jest identyfikacja i klasyfikacja incydentów, co jest niezbędne do skutecznego zarządzania nimi. Czynności te należy wykonać jak najszybciej. Identyfikacja polega na wczesnym wykrywaniu podejrzanych działań i anomalii w systemach informatycznych, co pozwala na szybkie podjęcie działań naprawczych. W tym celu wykorzystuje się zaawansowane narzędzia monitorujące i systemy wykrywania włamań IDS (Intrusion Detection System). Klasyfikacja incydentów polega na ocenie ich wpływu na organizację oraz poziomu krytyczności. Incydenty mogą być oceniane jako niosące niskie, średnie lub wysokie ryzyko, co pozwala na priorytetyzację działań. Klasyfikacja uwzględnia takie czynniki jak potencjalne skutki finansowe, wpływ na operacje biznesowe oraz reputacja organizacji. Dzięki temu możliwe jest skoncentrowanie zasobów na najbardziej krytycznych incydentach.

Niezbędnym elementem jest również szybka reakcja na incydenty, aby zminimalizować ich skutki. Po wykryciu incydentu CSIRT powinien natychmiast podjąć działania naprawcze, które mogą obejmować izolację zainfekowanych systemów, zastosowanie łat zabezpieczających, usunięcie złośliwego oprogramowania oraz przywrócenie systemów do normalnego stanu operacyjnego. Ważne jest, aby wszystkie działania były zgodne z opracowanym planem reagowania na incydenty (IRP). Szybka reakcja wymaga również skutecznej komunikacji z interesariuszami. Informowanie zarządu, pracowników, klientów oraz partnerów biznesowych o zaistniałym incydencie oraz podjętych działaniach jest priorytetowe dla budowania zaufania i minimalizowania paniki. Organizacja powinna również współpracować z organami ścigania i innymi odpowiednimi instytucjami w celu ścigania sprawców i zapobiegania przyszłym incydentom.

Równolegle są zbierane dowody, które mogą być wykorzystane do analizy przyczyn zdarzenia oraz ewentualnych postępowań prawnych. Zbieranie dowodów powinno być prowadzone zgodnie z ustalonymi procedurami, aby zachować ich integralność i wartość dowodową. Dowody mogą obejmować logi systemowe, zrzuty pamięci, pliki systemowe oraz inne informacje cyfrowe[24]. Analiza dowodów pozwala na dokładne zrozumienie, jak doszło do incydentu, jakie luki w zabezpieczeniach zostały wykorzystane oraz jakie działania podjął atakujący. Wyniki analizy są bardzo ważne dla opracowania skutecznych działań naprawczych oraz zapobiegania przyszłym incydentom. Dokumentowanie wszystkich kroków podejmowanych podczas analizy dowodów jest niezbędne dla utrzymania przejrzystości i zapewnienia możliwości audytu.

Należy również zauważyć rolę współpracy z mediami. Szczególnie dziś w dobie powszechnego rozprzestrzeniania się fake newsów, zwłaszcza za pośrednictwem mediów społecznościowych, zarządzanie informacją staje się bardzo ważne w czasie wystąpienia kryzysu.

[24] GAZ-SYSTEM CERT, *Szkolenie operatora gazociągów przesyłowych GAZ-SYSTEM S.A. Zagrożenia cyberbezpieczeństwa oraz dobre praktyki zabezpieczenia się przed cyberzagrożeniami*, https://www.gaz-system.pl/dam/jcr:08a4f82b-a42f-4aa6-9d29-4320a3c9e905/szkolenie-cyberbezpieczenstwa-gaz-system-4-0_01022024.pdf, s. 28 (11.06.2024).

Organizacja powinna być przygotowana na udzielanie informacji prasie oraz innym mediom, aby kontrolować narrację i zapobiegać rozprzestrzenianiu się dezinformacji. Wszystkie zainteresowane strony, w tym operatorzy usług kluczowych, powinny być odpowiednio informowane o incydencie oraz podjętych działaniach naprawczych. Przejrzysta i szybka komunikacja pomaga w budowaniu zaufania oraz minimalizowaniu paniki. Organizacja powinna opracować jasne wytyczne dotyczące komunikacji kryzysowej, które określają, kto jest odpowiedzialny za komunikację, jakie informacje powinny być przekazywane i w jakich ramach czasowych. W tym celu warto wyznaczyć rzecznika prasowego, który będzie odpowiedzialny za komunikację zewnętrzną[25].

Kolejnym krokiem jest neutralizacja zagrożeń cybernetycznych, która jest znaczącym etapem zarządzania incydentami i kryzysami cybernetycznymi. Proces ten obejmuje kilka etapów, które muszą być przeprowadzone sprawnie i skutecznie, aby minimalizować szkody i przywrócić normalne funkcjonowanie systemów informatycznych:

1. Izolacja zagrożenia – gdy tylko incydent zostanie wykryty, niezbędne jest szybkie odłączenie zainfekowanych systemów od sieci, aby zapobiec dalszemu rozprzestrzenianiu się zagrożenia. Może to obejmować wyłączenie zainfekowanych komputerów, odłączenie serwerów lub blokowanie określonych protokołów sieciowych. Szybka izolacja pozwala na ograniczenie obszaru, który może zostać zaatakowany, co jest istotne dla ochrony reszty infrastruktury IT.
2. Identyfikacja i eliminacja źródła zagrożenia – zespoły odpowiedzialne za bezpieczeństwo muszą dokładnie przeanalizować zainfekowane systemy, aby zidentyfikować rodzaj i źródło zagrożenia. Mogą to być złośliwe oprogramowanie, exploity, nieautoryzowane dostępy czy inne formy cyberataków. Po zidentyfikowaniu zagrożenia, należy je usunąć z systemów. W sytuacji, gdy zagrożenie pochodzi od nieautoryzowanego dostępu, należy natychmiast zablokować konta użytkowników lub zmienić hasła.

Równolegle z eliminacją zagrożenia ważne jest również przeprowadzenie dokładnej analizy incydentu. Obejmuje ona zbieranie i przeglądanie logów systemowych, ruch sieciowy oraz identyfikację wektorów ataku. Celem jest zrozumienie, jak doszło do incydentu, jakie były jego przyczyny oraz jakie są jego potencjalne konsekwencje. Ta wiedza jest niezbędna do zapobiegania podobnym incydentom w przyszłości.

Po eliminacji zagrożenia następuje etap odzyskiwania systemów[26]. Proces ten obejmuje przywracanie systemów do stanu sprzed incydentu, często z wykorzystaniem kopii zapasowych. W przypadku gdy nie są one dostępne, konieczne może być przeprowadzenie bardziej zaawansowanych działań naprawczych, takich jak odtworzenie danych z dysków twardych lub naprawa uszkodzonych plików. Ważne jest, aby w trakcie tego procesu upewnić się, że zagrożenie zostało całkowicie usunięte i nie ma ryzyka jego ponownego pojawienia się.

[25] P. Meyer, S. Métille, *Computer security incident response teams: are they legally regulated? The Swiss example*, „International Cybersecurity Law Review" 2023, vol. 4, s. 53-54.
[26] A. Michalski, *Bezpieczeństwo informacji w przypadku awarii lub katastrofy*, „Zeszyty Naukowe. Organizacja i Zarządzanie" 2012, s. 7-8.

Ostatnim krokiem w neutralizacji jest komunikacja kryzysowa i analiza post mortem. Należy poinformować wszystkich interesariuszy, w tym pracowników, klientów oraz partnerów biznesowych, o incydencie oraz podjętych działaniach. Transparentna komunikacja jest kluczowa dla utrzymania zaufania oraz minimalizowania negatywnych skutków dotyczących reputacji. Po zakończeniu działań naprawczych przeprowadza się szczegółową analizę incydentu, aby zidentyfikować wszelkie luki w zabezpieczeniach oraz określić, jakie kroki należy podjąć, aby zapobiec podobnym incydentom w przyszłości.

Neutralizacja zagrożeń cybernetycznych jest procesem skomplikowanym i wymagającym. Konieczna jest współpraca wielu zespołów, zastosowanie zaawansowanych narzędzi oraz ciągłe doskonalenie procedur bezpieczeństwa. Dzięki skutecznej neutralizacji organizacje mogą minimalizować szkody i szybko przywracać normalne funkcjonowanie systemów po incydentach cybernetycznych.

Po zneutralizowaniu zagrożenia kolejnym krokiem jest odzyskiwanie i przywracanie normalnych operacji. Proces ten obejmuje naprawę uszkodzonych systemów, przywrócenie danych z kopii zapasowych oraz monitorowanie systemów w celu wykrycia ewentualnych dalszych zagrożeń. Kluczowe jest, aby odzyskiwanie operacji było przeprowadzone zgodnie z planem ciągłości działania, co zapewnia minimalizację przestojów i szybki powrót do normalnej działalności. Przywracanie operacji powinno obejmować również przegląd i aktualizację zabezpieczeń, aby zapobiec ponownemu wystąpieniu incydentu[27]. Organizacja powinna ocenić skuteczność podjętych działań naprawczych oraz zidentyfikować obszary wymagające dalszych ulepszeń. Ważne jest również, aby informować interesariuszy o postępach w przywracaniu operacji oraz o wszelkich zmianach w procedurach bezpieczeństwa.

Następnie przeprowadza się analizę postincydentową (Post-Incident Review, PIR). Jej celem jest zrozumienie przyczyn incydentu, ocena skuteczności podjętych działań oraz zidentyfikowanie obszarów do poprawy. Analiza PIR[28] powinna obejmować przegląd wszystkich kroków podjętych podczas incydentu, w tym identyfikacji, reakcji, odzyskiwania i komunikacji. Wyniki analizy są dokumentowane w raporcie, który służy do ulepszania procedur zarządzania incydentami oraz strategii ochrony. Raport PIR powinien być udostępniany odpowiednim interesariuszom oraz wykorzystywany do celów szkoleniowych. Regularne przeprowadzanie analiz postincydentowych pomaga organizacjom w ciągłym doskonaleniu swoich procedur bezpieczeństwa.

Na koniec trzeba podkreślić, że regularne szkolenia i ćwiczenia symulacyjne dla personelu odpowiedzialnego za zarządzanie incydentami są niezbędne dla utrzymania gotowości do reagowania na rzeczywiste zagrożenia. Szkolenia powinny obejmować zarówno teoretyczne aspekty zarządzania incydentami, jak i praktyczne ćwiczenia, które symulują rzeczywiste

[27] *Disaster Recovery (DR) – proces przywracania działania systemów informatycznych po wystąpieniu nieprzewidzianego incydentu*, https://www.play.pl/duze-firmy/chmura-i-data-center/disaster-recovery.https://www.play.pl/duze-firmy/chmura-i-data-center/disaster-recovery (11.06.2024).
[28] Optimatis, *Jak wygląda praktyka zarządzania incydentami?,* 2024.

scenariusze incydentów[29]. Ćwiczenia symulacyjne pozwalają na przetestowanie planu reagowania na incydenty oraz identyfikację ewentualnych luk w procedurach. Ćwiczenia te powinny być przeprowadzane regularnie i obejmować różnorodne scenariusze, aby przygotować personel na różne typy zagrożeń[30]. Po każdym ćwiczeniu należy przeprowadzić analizę wyników, która pomoże w identyfikacji obszarów wymagających dalszych ulepszeń. Szkolenia i ćwiczenia są kluczowym elementem budowania kultury bezpieczeństwa w organizacji.

Implementacja powyższych elementów zarządzania incydentami i kryzysami cybernetycznymi pozwala organizacjom na skuteczne reagowanie na incydenty, minimalizowanie ich skutków oraz szybkie przywracanie normalnej działalności. Dzięki temu możliwe jest utrzymanie wysokiego poziomu bezpieczeństwa infrastruktury krytycznej oraz zapewnienie ciągłości działania. Stałe doskonalenie tych praktyk oraz współpraca z innymi podmiotami pozwala na lepsze przygotowanie się na przyszłe zagrożenia i skuteczniejsze zarządzanie incydentami. Cyberbezpieczeństwo to proces dynamiczny, który wymaga ciągłego monitorowania, adaptacji i uczenia się na podstawie doświadczeń, co jest niezbędne dla utrzymania bezpiecznej i niezawodnej infrastruktury w dobie rosnących zagrożeń cyfrowych.

Polska, w obliczu rosnących zagrożeń w cyberprzestrzeni, musiała stawić czoła wielu incydentom (przytoczone wcześniej), które wymagały szybkiej reakcji i efektywnego zarządzania.

Dzięki skutecznemu działaniu polskich służb cyberbezpieczeństwa udało się udaremnić atak na infrastrukturę krytyczną kraju, co pokazuje znaczenie gotowości i efektywności zespołów reagowania na incydenty. Utworzenie specjalistycznych jednostek takich jak CSIRT, które są w stanie szybko i skutecznie reagować na zagrożenia, jest istotnym elementem ochrony.

Po serii incydentów związanych z „radiostop" oraz zakłóceniami w sieci kolejowej polskie władze podjęły działania mające na celu zabezpieczenie komunikacji radiowej oraz wprowadzenie dodatkowych środków ochrony. Ten incydent podkreślił konieczność modernizacji systemów komunikacyjnych i dostosowanie ich do standardów szyfrowanych w odpowiedzi na nowe zagrożenia, co jest planowane do realizacji do 2025 roku.

PODSUMOWANIE

Przedstawiona analiza ukazuje ewolucję i wyzwania polskiego systemu cyberbezpieczeństwa, skupiając się na ochronie infrastruktury krytycznej oraz zarządzaniu incydentami cybernetycznymi. Niezbędne działania legislacyjne, w tym wdrożenie ustawy o Krajowym Systemie Cyberbezpieczeństwa oraz dostosowanie krajowych przepisów do wymogów Unii Europejskiej i NATO, miały istotny wpływ na obecny kształt systemu.

Polska kontynuuje inwestycje w rozwój specjalistycznych kadr i nowoczesnych technologii, aby skutecznie przeciwdziałać rosnącym zagrożeniom cybernetycznym. W obliczu

[29] Narodowy Program Ochrony Infrastruktury Krytycznej, tekst jednolity, Rządowe Centrum Bezpieczeństwa, 2023, s. 43.
[30] Narodowy Program Ochrony Infrastruktury Krytycznej, Załącznik 1. Standardy służące zapewnieniu sprawnego funkcjonowania infrastruktury krytycznej – dobre praktyki i rekomendacje, Rządowe Centrum Bezpieczeństwa, 2015, s. 18-19.

globalnych wyzwań, takich jak ataki ransomware i rozwój technologii 5G, międzynarodowa współpraca pozostaje niezbędnym elementem strategii cyberbezpieczeństwa. Konieczne są ciągła adaptacja i monitorowanie, aby zapewnić bezpieczeństwo w dynamicznie zmieniającym się środowisku cyfrowym.

WNIOSKI I REKOMENDACJE

Podsumowując, stwierdzono, że rozwój polskiego systemu cyberbezpieczeństwa wymaga ciągłej adaptacji do dynamicznie zmieniającego się krajobrazu technologicznego oraz ewoluujących zagrożeń cyfrowych. Polska jako członek Unii Europejskiej i NATO skutecznie integruje wymagania międzynarodowe, inwestując w rozwój infrastruktury ochronnej oraz edukację specjalistycznych kadr. Niemniej jednak, aby skutecznie stawić czoła rosnącym zagrożeniom, konieczne jest dalsze rozwijanie systemu cyberbezpieczeństwa poprzez wdrożenie następujących rekomendacji, które mogą stanowić kierunki przyszłych badań i działań w tej dziedzinie:

1. Rozwój zaawansowanych technologii wykrywania zagrożeń – współczesne zagrożenia cybernetyczne stają się coraz bardziej zaawansowane i trudniejsze do wykrycia, co wymaga od systemów bezpieczeństwa adaptacji do nowych wyzwań. Przyszłe badania powinny koncentrować się na rozwoju i wdrażaniu nowoczesnych narzędzi analitycznych oraz systemów wykrywania zagrożeń (IDS/IPS), które wykorzystują sztuczną inteligencję (AI) i uczenie maszynowe (ML). Technologie te mogą pomóc w analizie anomalii i przewidywaniu potencjalnych incydentów, umożliwiając wcześniejsze reagowanie na zagrożenia. W kontekście polskiego cyberbezpieczeństwa istotne jest opracowanie rozwiązań, które będą zdolne do działania w złożonych i różnorodnych środowiskach IT, charakterystycznych dla infrastruktury krytycznej.
2. Wzmacnianie międzynarodowej współpracy – w obliczu globalnych wyzwań, takich jak ataki ransomware czy cyberoperacje sponsorowane przez państwa, międzynarodowa współpraca jest kluczowa dla skutecznej obrony. Polska powinna kontynuować i intensyfikować współpracę z innymi krajami oraz organizacjami międzynarodowymi, takimi jak NATO i UE, w celu wymiany wiedzy i najlepszych praktyk. Przyszłe badania mogą skupić się na analizie skuteczności obecnych form współpracy oraz poszukiwaniu nowych modeli partnerstwa publiczno-prywatnego. Badania te mogą również dotyczyć rozwoju wspólnych platform wymiany informacji o zagrożeniach, co pozwoli na szybsze reagowanie na globalne incydenty cybernetyczne.
3. Edukacja i podnoszenie świadomości społecznej – skuteczny system cyberbezpieczeństwa opiera się nie tylko na technologii, ale także na ludziach. Edukacja i zwiększanie świadomości społecznej na temat zagrożeń cyfrowych są bardzo ważne dla ochrony przed cyberatakami. Przyszłe badania powinny badać efektywność obecnych kampanii edukacyjnych, programów szkoleniowych oraz rozwijać nowe strategie edukacyjne skierowane zarówno do profesjonalistów, jak i całego społeczeństwa. Warto również rozważyć

wdrażanie programów edukacyjnych od najniższych poziomów edukacji, aby budować kulturę cyberbezpieczeństwa już od najmłodszych lat. Edukacja powinna obejmować zarówno podstawy ochrony danych, jak i bardziej zaawansowane zagadnienia, takie jak ochrona prywatności w sieci, bezpieczeństwo aplikacji mobilnych czy zagrożenia związane z Internetem Rzeczy (IoT).

4. Adaptacja do nowych technologii i zagrożeń – w miarę jak technologia ewoluuje, pojawiają się nowe wyzwania i zagrożenia. Rozwój technologii 5G, sztucznej inteligencji, blockchaina oraz innych innowacji stwarza zarówno nowe możliwości, jak i zagrożenia. Polska powinna inwestować w badania nad bezpieczeństwem tych technologii oraz opracowywać standardy i regulacje, które będą chronić infrastrukturę krytyczną przed nowymi rodzajami ataków. Badania mogą również dotyczyć sposobów integracji nowych technologii z istniejącymi systemami zabezpieczeń, aby zapewnić ich zgodność i efektywność.
5. Rozwój narodowych zdolności reagowania na incydenty – skuteczna reakcja na incydenty cybernetyczne jest niezbędna dla minimalizacji ich skutków i szybkiego przywracania normalnego funkcjonowania systemów. W odpowiedzi na rosnącą liczbę i złożoność incydentów cybernetycznych istotne jest dalsze rozwijanie krajowych zespołów reagowania na incydenty (CSIRT) oraz doskonalenie procedur zarządzania kryzysowego. Badania w tej dziedzinie powinny koncentrować się na analizie skuteczności istniejących procedur oraz na opracowywaniu nowych metod szybkiego reagowania i neutralizacji zagrożeń. Dodatkowo warto rozwijać symulacje i ćwiczenia, które pomogą w przygotowaniu personelu na rzeczywiste incydenty, zwiększając jego gotowość i umiejętności operacyjne.
6. Integracja cyberbezpieczeństwa z zarządzaniem ryzykiem – cyberbezpieczeństwo powinno być integralną częścią strategii zarządzania ryzykiem w organizacjach. Przyszłe badania mogą obejmować rozwój zintegrowanych modeli zarządzania ryzykiem, które łączą tradycyjne podejścia z nowoczesnymi technologiami zabezpieczeń cyfrowych. Kluczowym aspektem będzie tu rozwój narzędzi analitycznych, które umożliwią organizacjom identyfikację, ocenę i zarządzanie ryzykiem w sposób holistyczny, przy uwzględnieniu zarówno aspektów technologicznych, jak i ludzkich. Długoterminowym celem powinno być zbudowanie takiej kultury organizacyjnej, w której cyberbezpieczeństwo jest traktowane jako jeden z fundamentalnych elementów strategii biznesowej.

Implementacja powyższych rekomendacji może znacząco zwiększyć odporność polskiego systemu cyberbezpieczeństwa, pozwalając lepiej przygotować się na przyszłe wyzwania i zagrożenia w dynamicznie zmieniającym się środowisku cyfrowym. Kluczowe jest, aby Polska kontynuowała inwestycje w rozwój technologii i kadry oraz aktywnie uczestniczyła w międzynarodowej współpracy, co zapewni jej skuteczność działań w zakresie cyberbezpieczeństwa w nadchodzących latach.

BIBLOGRAFIA

„Cyberbezpieczny samorząd – poradnik". NASK – Państwowy Instytut Badawczy. 2024. W https://bip4.wokiss.pl/chodziezp/zasoby/files/pozostale/cyberbezpieczenstwo/2023/cs-poradnik-25102023.pdf.

Barć Marek. 2021. „Rodzaje ochrony infrastruktury krytycznej". Rocznik Bezpieczeństwa Morskiego. 15: 1-15.

Burda Robin. 2024. „Detection Tools for Cognitive Warfare: Leveraging the Cyber Domain". STO NATO, 1.

Cyber hackers target Polish rail network, cause operational disruptions. 2023. W https://industrialcyber.co/transport/cyber-hackers-target-polish-rail-network-cause-operational-disruptions/.

Disaster Recovery (DR) – proces przywracania działania systemów informatycznych po wystąpieniu nieprzewidzianego incydentu. 2024. W https://www.play.pl/duze-firmy/chmura-i-data-center/disaster-recovery.

Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej). 2002. W https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32002L0058.

European Union. 2024. Kształtowanie cyfrowej przyszłości Europy. W https://digital-strategy.ec.europa.eu/pl/news/european-union-and-nato-intensify-cooperation-addressing-cyber-threats.

GAZ-SYSTEM CERT. 2024. „Szkolenie operatora gazociągów przesyłowych GAZ-SYSTEM S.A. Zagrożenia cyberbezpieczeństwa oraz dobre praktyki zabezpieczenia się przed cyberzagrożeniami". W https://www.gaz-system.pl/dam/jcr:08a4f82b-a42f-4aa6-9d29-4320a3c9e905/szkolenie-cyberbezpieczenstwa-gaz-system-4-0_01022024.pdf.

Gościniak Tomasz. 2014. „Zarządzanie procesami naprawczymi w systemach informatycznych operatorów telekomunikacyjnych". Zeszyty Naukowe. Organizacja i Zarządzanie/Politechnika Śląska 70: 143-162.

Kasprzyk Ewelina. 2022. Three Seas United in Cyber Power Pandemia COVID-19 a cyfryzacja w regionie Trójmorza, W: Raport: Three Seas United in Cyber Power. Kraków: Instytut Kościuszki.

Kaźmierczak Maciej, Byłeń Sławomir. 2024. „Security of critical infrastructure in Poland – selected aspects of research". Gospodarka Materiałowa i Logistyka 75(1): 28-38.

Kość Wojciech. 2024. Polish train chaos blamed on radio hackers. W https://www.politico.eu/article/poland-train-chaos-radio-hackers-russia-ukraine-war/.

Kotłowski Włodzimierz. 2014. Teleinformatyczne elementy ochrony infrastruktury krytycznej. Bezpieczeństwo infrastruktury krytycznej – wymiar teleinformatyczny, Kraków: Instytut Kościuszki.

Meyer Pauline, Métille Sylvain. 2023. „Computer security incident response teams: are they legally regulated? The Swiss example". International Cybersecurity Law Review 4: 39-60.

Michalski Andrzej. 2012. „Bezpieczeństwo informacji w przypadku awarii lub katastrofy" Zeszyty Naukowe. Organizacja i Zarządzanie/Politechnika Śląska 61: 243-254.

Ministerstwo Łączności. 2001. ePolska. Plan działań na rzecz rozwoju społeczeństwa informacyjnego w Polsce na lata 2001-2006.

Mukhina Olena. 2024. Hacker attack averted in Poland amid cyberwar with Russia. W https://euromaidanpress.com/2024/06/03/hacker-attacks-averted-in-poland-amid-cyberwar-with-russia/.

Na fali nauki. 2023. W https://nafalinauki.pl/bezpieczenstwo-w-erze-5g-nowe-wyzwania-i-rozwiazania/.

Narodowy Program Ochrony Infrastruktury Krytycznej. Załącznik 1. Standardy służące zapewnieniu sprawnego funkcjonowania infrastruktury krytycznej – dobre praktyki i rekomendacje. 2015. Rządowe Centrum Bezpieczeństwa.

Optimatis. 2024. Jak wygląda praktyka zarządzania incydentami?

Rak Janusz. 2016. „Zasady określania przynależności do infrastruktury krytycznej". Czasopismo Inżynierii Lądowej, Środowiska i Architektury 63: 291-298.

Raport roczny z działalności CERT Polska 2017. 2018. Krajobraz bezpieczeństwa polskiego internetu, CERT Polska.

Rot Artur. 2010. „Ryzyko systemów informatycznych a zarządzanie ciągłością działania w organizacji (Business Continuity Management)". Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu. Informatyka Ekonomiczna 18. Systemy informacyjne w zarządzaniu. 119: 263-273.

Rzeczpospolita. 2024. W https://www.rp.pl/biznes/art40326141-cybernetyczna-wojna-neka-firmy-i-instytucje.

Stalmach Sławomir. 2021. „Cztery obszary cyberbezpieczeństwa – omówienie zakresu tematycznego". Przegląd Policyjny. 141(1): 94-107.

The NATO Cooperative Cyber Defence Centre of Excellence. NotPetya and WannaCry Call for a Joint Response from International Community. W https://ccdcoe.org/news/2017/notpetya-and-wannacry-call-for-a-joint-response-from-international-community/.

Uchwała nr 125 Rady Ministrów z dnia 22 października 2019 r. w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024 (M.P. 2019 poz. 1037).

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

Wrzosek Magdalena. 2019. Raport. Cyberbezpieczeństwo A.D. 2018, NASK.

Wygodny Adam. 2021. „Metody prowadzenia audytu cyberbezpieczeństwa: Ustawa o KSC", Kontrola Państwowa. 66 (2): 82-84.

Wyrębek Henryk. 2021. „Cyberprzestrzeń. Zagrożenia. Strategie bezpieczeństwa". Siedlce: Uniwersytet Przyrodniczo-Humanistyczny w Siedlcach.