PARP
Grupa PFR

Budowanie odporności przedsiębiorstw w kontekście bezpieczeństwa cyfrowego w klastrach

Grupa PFR

Niniejszy podręcznik powstał na zlecenie Polskiej Agencji Rozwoju Przedsiębiorczości. Polska Agencja Rozwoju Przedsiębiorczości nie ponosi odpowiedzialności za treści prezentowane w podręczniku. Treść podręcznika nie jest dla Polskiej Agencji Rozwoju Przedsiębiorczości w żaden sposób wiążąca.

ISBN 978-83-7633-593-3

Zespół autorski
Łukasz Gawron
Rafał Kolorz
Karolina Nowak
Karolina Wojtyczek

Skład i oprawa graficzna
Wiktoria Konieczniak

Recenzent
dr inż. Michał Suchocki

Współpraca merytoryczna ze strony Polskiej Agencji Rozwoju Przedsiębiorczości
Monika Antonowicz
Paweł Chaber
Aleksandra Walczyk-Jansson
Natalia Wawryniewicz
Rafał Wawrzycki

Realizacja

#CyberMadeInPoland

Polski Klaster Cyberbezpieczeństwa
CyberMadeInPoland Sp. z o.o.

ul. Ogrodowa 1/6, 31-155 Kraków
NIP: 6762583919, REGON: 386754317
WWW: www.cybermadeinpoland.pl
E-mail: office@cybermadeinpoland.pl
Tel: +48 669 614 854

Klastry od lat należą do najważniejszych ekosystemów rozwoju innowacji w Polsce. To w nich spotykają się przedsiębiorstwa, instytucje naukowe i otoczenia biznesu, samorządy oraz partnerzy publiczni, wspólnie wzmacniając konkurencyjność naszych regionów. Szczególną wartość klastrów stanowi zgromadzona w nich wiedza ekspercka oraz gotowość do dzielenia się nią, zarówno pomiędzy członkami jednego klastra, jak i w skali całego krajowego ekosystemu klastrów.

Niniejszy podręcznik powstał właśnie z tej potrzeby, aby praktyczna wiedza wypracowana w Krajowych Klastrach Kluczowych i Ponadregionalnych Klastrach Wzrostowych, w tak strategicznym obszarze jak budowanie odporności przedsiębiorstw w kontekście bezpieczeństwa cyfrowego, została uporządkowana, opisana i udostępniona wszystkim koordynatorom klastrów w Polsce. Podręcznik ten jest efektem współpracy ekspertów z Polskiego Klastra Cyberbezpieczeństwa CyberMadeInPoland Sp. z o.o. (koordynatora Polskiego Klastra Cyberbezpieczeństwa #CyberMadeInPoland) oraz ekspertów Polskiej Agencji Rozwoju Przedsiębiorczości, a jego celem jest wzmocnienie roli klastrów jako partnerów transformacji cyfrowej i budowania odporności MŚP.

Wierzę, że ta publikacja będzie dla Państwa nie tylko źródłem wiedzy, lecz przede wszystkim praktycznym przewodnikiem inspirującym do tworzenia nowych usług, inicjowania wspólnych działań i jeszcze skuteczniejszego wspierania firm członkowskich w mierzeniu się z wyzwaniami współczesnej gospodarki cyfrowej.

Krzysztof Gulda
p.o. Prezesa Polskiej Agencji Rozwoju Przedsiębiorczości

Spis treści

Wstęp **7**
Rozdział 1. Wprowadzenie do cyberbezpieczeństwa **9**
1.1 Czym jest cyberbezpieczeństwo? 10
1.2 Rola bezpieczeństwa cyfrowego w rozwoju MŚP 11
1.3 Typowe zagrożenia w ekosystemie klastra 12
1.3.1 Kto może zaatakować w cyberprzestrzeni? 12
1.3.2 Cyberzagrożenia 12
1.4 Kontekst regulacyjny 18
1.5 Kontekst zewnętrzny (geopolityka i technologia) 21
1.6 Mapa interesariuszy 22
Rozdział 2. Cyberbezpieczeństwo w kontekście regulacyjnym **25**
2.1 Dyrektywa NIS oraz Ustawa o Krajowym Systemie Cyberbezpieczeństwa 26
2.2 Dyrektywa NIS2 oraz Nowelizacja Ustawy o Krajowym Systemie Cyberbezpieczeństwa (UKSC2) 26
2.3. Akt o odporności cyfrowej (Cyber Resilience Act/CRA) 33
2.4 Certyfikaty i standardy 34
2.5. Zarządzanie ryzykiem 36
2.6. Ubezpieczenia od ryzyk cybernetycznych 38
Rozdział 3. Rola koordynatora klastra w budowaniu cyberodporności członków klastra **40**
3.1 Praktyczne podejście do diagnozy cyberodporności wśród członków klastra 41
3.1.1. Ankietowanie członków klastra 41
3.1.2 Proaktywne podejście obserwacyjne koordynatora klastra 42
3.1.3 Porównanie narzędzi 43
3.2 Budowanie świadomości na temat cyberodporności wśród członków klastra 44
3.3 Budowanie sieci wsparcia cyberbezpieczeństwa w podmiotach członkowskich 45
3.4 Wymiana informacji o zagrożeniach – ISAC klastrowy 47
Rozdział 4. Cyberbezpieczeństwo koordynatora klastra **50**
4.1 Główne zagrożenia cyberbezpieczeństwa w kontekście koordynatora klastra 51
4.2. Dobre praktyki budowania cyberodporności u koordynatora klastra 54
Rozdział 5. Praktyczne sposoby wsparcia członków klastra przez koordynatora **58**
5.1 Ocena poziomu cyberbezpieczeństwa członków klastra oraz benchmarking 59
5.2 Bezpieczeństwo łańcucha dostaw 65
5.3 Analiza ryzyka i kontekstu działalności klastra oraz jego członków 66
5.4 Budowanie sieci zaufanych dostawców 67
5.5 Propozycja wsparcia: gotowe pomysły na usługi i działania koordynatora 70
5.5.1 Wspólny SOC 70
5.5.2 Cyber Threat Intelligence (CTI) 70
5.5.3 Opracowanie wspólnego profilu zagrożeń 71
5.5.4 Doradztwo prawne 71
5.5.5 Obsługa incydentów 71
5.5.6 Licencja na szkolenia cyber i testy anty-phishingowe 72
5.5.7 EDR w pakiecie dla podmiotów członkowskich 72

5.5.8 Matchmaking, brokering z dostawcami rozwiązań cyber ... 72
Rozdział 6. Finansowanie działań z zakresu cyberbezpieczeństwa dla koordynatora klastra oraz podmiotów członkowskich ... 74
6.1 Źródła finansowania cyberodporności członków klastra ... 75
6.1.1. Fundusze unijne w obecnej perspektywie – FENG oraz FERC ... 75
6.1.2 Digital Europe Programme (DEP) ... 77
6.1.3. Krajowy Plan Odbudowy (KPO) ... 79
6.1.4 Regionalne Programy Operacyjne (RPO) ... 79
6.1.5 Lista sprawdzająca dofinansowania z zakresu cyberbezpieczeństwa ... 80
6.2. Sposoby finansowania cyberodporności poprzez współpracę podmiotów członkowskich oraz współpracę z European Digital Innovation Hubs (EDIH) ... 80
6.2.1 Współpraca podmiotów członkowskich w celu wspólnego finansowania usług cyberbezpieczeństwa ... 80
6.2.2 Współpraca podmiotów członkowskich z European Digital Innovation Hubs ... 81
Rozdział 7. Działania zbiorowe i budowanie odporności cyfrowej klastra jako całości ... 85
7.1 Tworzenie strategii odporności cyfrowej klastra ... 86
7.1.1 Misja ... 86
7.1.2 Cele strategiczne i operacyjne ... 86
7.1.3 Mierniki Sukcesu (KPI) ... 88
7.1.4 Partnerstwa Strategiczne ... 88
7.2 Ćwiczenia i symulacje ... 89
7.2.1 Table Top Exercises ... 90
7.2.2 Cyber Range ... 91
7.3 Wymiana doświadczeń między klastrami ... 92
Rozdział 8. Studium przypadków ... 100
8.1 Ogólna diagnoza potrzeb ... 101
8.2 Budowa kompetencji wewnętrznych ... 102
8.3 Konsolidowanie wiedzy z zewnątrz ... 103
Rozdział 9. Praktyczne wskazówki dla koordynatora klastra ... 107
9.1 Komunikacja i promocja – wskazówki jak tłumaczyć złożone tematy w sposób zrozumiały i motywujący ... 108
9.2. Mierzenie rezultatów – system monitorowania postępów i raportowania rezultatów zwiększania cyberodporności w klastrze ... 109
9.3 Rekomendowane narzędzia i źródła – lista portali, centrów kompetencji, materiałów szkoleniowych i innych sprawdzonych źródeł wiedzy ... 112
9.4. Przewodnik po narzędziach zaproponowanych w podręczniku ... 115
Rozdział 10. Zakończenie ... 117
Słownik ... 119
Spis tabel ... 123
Spis rysunków ... 123
Bibliografia ... 124

Budowanie odporności przedsiębiorstw w kontekście bezpieczeństwa cyfrowego w klastrach

Wstęp

Choć temat cyberbezpieczeństwa kojarzony jest często z zaawansowanymi technologiami, jego definicja wykracza daleko poza samą technologię. Nie jest to już domena specjalistów IT, ale kluczowy czynnik determinujący stabilność, konkurencyjność i potencjał rozwojowy każdej organizacji, niezależnie od jej wielkości, czy branży, w której funkcjonuje. W rzeczywistości cyberbezpieczeństwo dotyczy każdej organizacji korzystającej z komputerów, sieci i informacji cyfrowych, a więc także klastrów i zrzeszonych w nich przedsiębiorstw, a ujmując temat szerzej – ogółu społeczeństwa.

Oficjalną definicję cyberbezpieczeństwa w Polsce zawiera ustawa o krajowym systemie cyberbezpieczeństwa, która aktualnie (tj. w dniu pisania podręcznika[1]) podlega nowelizacji. Zgodnie z postanowieniami na ten moment funkcjonującej ustawy, cyberbezpieczeństwo jest to: „odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy”[2]. Nowelizacja ustawy proponuje natomiast zmienioną definicję, która brzmi: „działania niezbędne do ochrony sieci i systemów informatycznych, użytkowników takich systemów oraz innych osób przed cyberzagrożeniami”[3]. Jest to proponowany zapis, który może jeszcze ulec zmianie.

Współczesne klastry to złożone ekosystemy współpracy, w których uczestniczą firmy, uczelnie, instytucje publiczne, organizacje otoczenia biznesu i wiele innych podmiotów. Współdzielą one dane, zasoby i wiedzę, a to oznacza, że bezpieczeństwo cyfrowe jednej organizacji ma bezpośredni lub pośredni wpływ na całość sieci. Jeden incydent może osłabić zaufanie partnerów,

zagrozić realizacji wspólnych projektów lub doprowadzić do wycieku poufnych informacji. Właśnie dlatego cyberbezpieczeństwo staje się nie tylko kwestią technologiczną, ale również strategiczną kompetencją klastra – taką samą jak zarządzanie innowacjami, internacjonalizacja czy rozwój kompetencji członków. Odporność cyfrowa przekłada się bezpośrednio na stabilność współpracy, możliwość realizacji projektów B+R, pozyskiwanie kontraktów oraz uczestnictwo w globalnych łańcuchach dostaw.

Niniejszy podręcznik powstał, aby wyposażyć koordynatorów klastrów w wiedzę i narzędzia niezbędne do skutecznego wspierania podmiotów członkowskich w budowaniu ich cyberodporności. Zapraszamy do lektury.

1 Stan na dzień 05.12.2025 r.
2 Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. 2018 poz. 150 ze zm.)
3 Rządowy projekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw, Dostęp: https://www.sejm.gov.pl/sejm10.nsf/agent.xsp?symbol=RPL&Id=RM-0610-195-25. (17 listopada 2025)

Rozdział 1

Wprowadzenie do cyberbezpieczeństwa

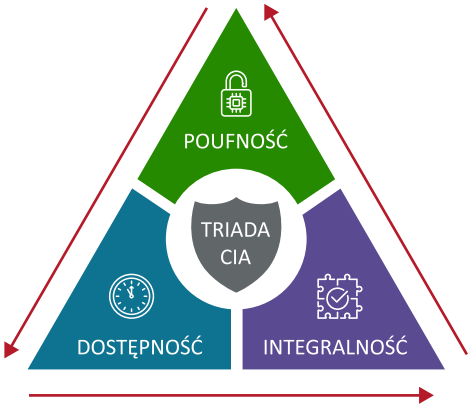
1.1 Czym jest cyberbezpieczeństwo?

Na potrzeby niniejszego poradnika została przyjęta definicja zaproponowana przez NASK (Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy), który definiuje cyberbezpieczeństwo jako dziedzinę wiedzy i praktyki, której celem jest zapewnienie odporności systemów informatycznych oraz danych na działania, które mogłyby naruszyć ich poufność, integralność, dostępność i autentyczność:

- **zapewnienie poufności** polega na zabezpieczeniu przed ujawnieniem danych osobom niepowołanym, zwykle jest to realizowane poprzez mechanizmy kontroli dostępu i szyfrowania, w spoczynku, podczas ich przesyłania i przetwarzania,
- **dbałość o integralność danych** to dążenie do zapewnienia stanu, w którym dane pozostają niezmienione, tzn. zabezpieczone przed nieautoryzowanymi zmianami,
- **dostępność informacji** to możliwość korzystania z nich w dowolnym czasie i bez żadnych utrudnień przez uprawniony podmiot,
- **zapewnienie autentyczności** to możliwość pewnego potwierdzenia pochodzenia danych[4].

Norma ISO/IEC 27001 (międzynarodowy standard zarządzania bezpieczeństwem informacji; szerzej omówiona w rozdziale 2) jako najistotniejsze w celu zapewnienia kompleksowej ochrony wskazuje na trzy ze wspomnianych powyżej

Rysunek 1.1 *Triada CIA.*



Źródło: Opracowanie własne na podstawie: https://websitesecuritystore.com/blog/what-is-the-cia-triad/.

elementów – zostały one przedstawione na Rysunku 1[5]. Jest to tak zwana Triada CIA (ang. CIA Triad) – litery w jej nazwie oznaczają kolejno poufność (ang. confidentiality), integralność (ang. integrity) i dostępność (ang. availability). Co więcej, tak jak wskazuje Rysunek 1, nie należy traktować tych aspektów jako jednorazowej czynności oraz procesu, który zostanie zaprojektowany raz na zawsze. Jest to proces, który wymaga nieustannego monitorowania i doskonalenia[6].

Nieuwzględnienie choćby jednej z trzech wymienionych właściwości podczas planowania systemów i funkcjonowania koordynatora klastra czy członka klastra zwiększa ryzyko wystąpienia incydentów bezpieczeństwa informacji. Te z kolei często odbijają się na wynikach finansowych, a w przypadku wycieku danych – również wizerunkowych.

W praktyce cyberbezpieczeństwo to nie tylko technologia, lecz także organizacja pracy, świa-

4 NASK, Poradnik „Firma Bezpieczna Cyfrowo" [artykuł online]. Dostęp: https://firmabezpiecznacyfrowo.pl/poradnik/#1. (24 listopada 2025)

5 Zespół autorski RCI Kraków, (2024) „Triada CIA jako fundament bezpieczeństwa" [artykuł online]. Dostęp: https://rci-krakow.wp.mil.pl/aktualnosci/triada-cia-jako-fundament-bezpieczenstwa/. (17 listopada 2025)

6 Pachucki, M., (2025) „CIA, ale nie ta z Langley: triada, na której oparte jest bezpieczeństwo informacji" [artykuł online] Dostęp: https://cybershieldon.pl/cia-%E2%80%93-ale-nie-ta-z-langley-triada-na-ktorej-oparte-jest-bezpieczenstwo-informacji. (17 listopada 2025)

domość użytkowników i umiejętność reagowania. W kontekście klastrów oznacza to wspólną troskę koordynatora i wszystkich członków klastra o bezpieczeństwo informacji, które są podstawą współpracy i rozwoju innowacji.

1.2 Rola bezpieczeństwa cyfrowego w rozwoju MŚP

Wśród wielu małych i średnich przedsiębiorstw (MŚP) cyberbezpieczeństwo wciąż postrzegane jest jako koszt, czyli coś, co „warto mieć", ale co można odłożyć na później. Tymczasem w praktyce stanowi ono inwestycję w stabilność biznesu, co niesie ze sobą konkretne korzyści, takie jak:

- **Zachowanie ciągłości działania** – zabezpieczone systemy minimalizują ryzyko przestojów, co jest kluczowe dla realizacji kontraktów.

- **Wiarygodność w łańcuchach dostaw** – coraz więcej dużych podmiotów wymaga od swoich dostawców i partnerów biznesowych spełnienia określonych norm i standardów cyberbezpieczeństwa. Cyfrowa odporność staje się warunkiem możliwości udziału w łańcuchach dostaw, pozyskiwaniu kontraktów i międzynarodowego finansowania. Niespełnienie wymagań cyberbezpieczeństwa może prowadzić do utraty kluczowych klientów.

- **Zgodność z regulacjami** – odpowiednie zabezpieczenia pomagają unikać wysokich kar finansowych nakładanych przez organy nadzorcze, np. w przypadku naruszenia wymogów narzuconych przez RODO[7] w zakresie przetwarzania danych osobowych.

- **Przewaga konkurencyjna** – firmy, które proaktywnie dbają o bezpieczeństwo cyfrowe budują zaufanie klientów i partnerów, pozycjonując się jako wiarygodny podmiot na rynku.

W długoterminowej perspektywie bagatelizowanie cyberbezpieczeństwa przez MŚP oraz zakładanie, że „nam się to nie przytrafi" nie jest ani korzystne, ani opłacalne dla firmy. Inwestowanie w zabezpieczenia często jest pomijane, ponieważ nie są to „inwestycje szybkiego zwrotu". Korzyści z inwestowania w rozwiązania cyberbezpieczeństwa rozkładają się w czasie i nie są tak łatwo policzalne. Dopiero w momencie ataku firma zdaje sobie sprawę z tego, że zakup odpowiednio dopasowanych rozwiązań był kluczowy, aby nie stracić swoich zasobów, danych, czy pieniędzy.

MŚP nierzadko są również częścią łańcucha dostaw dla przedstawicieli kluczowych sektorów gospodarki, dlatego nieustanny rozwój kompetencji cyfrowych wśród polskich przedsiębiorców, a także podnoszenie poziomu ochrony w sektorze MŚP oraz upowszechnienie i wdrożenie standardów cyberbezpieczeństwa w firmach jest kluczowe nie tylko z perspektywy samych zainteresowanych firm, ale także bezpieczeństwa zarówno ich klientów, jak i gospodarki kraju.

Wnioski dla koordynatora: klaster, poprzez koordynatora, powinien wspierać MŚP w przeprowadzeniu prostej analizy i oceny ryzyka, która pomoże uświadomić im realne zagrożenia i przełożyć wydatki na bezpieczeństwo na konkretny zwrot z inwestycji (np. uniknięcie straty – wątek został szerzej opisany w rozdziale 2).

7 Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych. Dostęp: https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20180001000. (24 listopada 2025)

1.3 Typowe zagrożenia w ekosystemie klastra

Ekosystem klastra to przestrzeń intensywnej wymiany informacji – zarówno technologicznych, jak i organizacyjnych. Jego siłą jest współdzielenie wiedzy, ale jednocześnie jest to obszar, w którym pojawiają się szczególne wyzwania w zakresie cyberbezpieczeństwa. Taka wewnętrzna sieć wzajemnie powiązana jest szczególnie narażona na cyberatak, który może być wymierzony w różne elementy infrastruktury oraz dotykać różnych działów w strukturach samego koordynatora klastra, co może wpłynąć na członków klastra. Tak samo ma się to w przypadku sytuacji, w której jeden członek klastra zostanie zaatakowany, może to wpłynąć na cały klaster, z uwagi właśnie na współdzielenie informacji lub przez wspólne przedsięwzięcia.

1.3.1 Kto może zaatakować w cyberprzestrzeni?

ENISA (ang. European Union Agency for Cybersecurity – jest to unijna organizacja, której misją jest wzmacnianie poziomu cyberbezpieczeństwa w UE) co roku publikuje raport ENISA Threat Landscape (ETL), aby zwiększać świadomość na temat bieżących cyberzagrożeń. W raporcie z 2024 roku zostały wskazane cztery grupy atakujących w cyberprzestrzeni oraz ich motywacje[8]:

- **Cyberprzestępcy** – aktorzy o motywacji finansowej, którzy czerpią zysk z kradzieży danych organizacji albo poprzez wymuszania okupu.

- **Grupy rządowe** – składają się z osób prowadzących operacje w cyberprzestrzeni w ramach struktur państwowych. Dysponują zapleczem wywiadowczym i militarnym, zatem są w stanie przygotować złożone i ukierunkowane ataki. Mają na celu głównie szpiegostwo, czy zakłócanie poprawnego działania państwa.

- **Podmioty ofensywne sektora prywatnego (ang. PSOAs – Private Sector Offensive Actors)** – podmioty komercyjne zajmujące się cyberinwigilacją. Specjalizują się w tworzeniu i sprzedaży cyberbroni, w tym exploitów „zero-day” – oraz złośliwego oprogramowania szerokiemu gronu klientów, często rządom i osobom prywatnym. Przykładem takiej cyberbroni jest tzw. „0-day ” – luki w zabezpieczeniach systemu komputerowego, które są wykorzystywane przez cyberprzestępców przed jej odkryciem przez producenta oprogramowania lub przed wydaniem odpowiedniej poprawki. “0-Day” oznacza, że twórcy oprogramowania mają “zero dni” na załatanie tej luki, co czyni ją niezwykle groźną, ponieważ brak czasu na reakcję może prowadzić do poważnych konsekwencji[9]. Również tworzą i sprzedają szerokiemu gronu klientów, często rządom i osobom prywatnym, złośliwe oprogramowanie.

- **Haktywiści** – grupy osób prowadzących działania w cyberprzestrzeni z pobudek ideologicznych. Często przyczyną ich zachowań są bieżące wydarzenia geopolityczne.

1.3.2 Cyberzagrożenia

Warto być świadomym kilku głównych cyberzagrożeń, które dominują w ostatnich latach. Poznanie ich pozwoli zrozumieć jak szeroko należy postrzegać zagadnienie cyberbezpieczeństwa.

8 European Union Agency for Cybersecurity, (2024) „Enisa Threat Landscape 2024” [artykuł online]. Dostęp: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024. (17 listopada 2025)

9 nFlo, „Co to jest 0-Day exploit”, [artykuł online]. Dostęp: https://nflo.pl/slownik/0-day-exploit/#strong-co-to-jest-0-day-exploit-definicja-strong. (24 listopada 2025)

1. **Ataki odmowy usługi (ang. Distributed Denial of Service – DDoS)** – polegają na przeciążeniu serwera, sieci lub usługi internetowej poprzez zalewanie ich ogromną liczbą zapytań. Zwykle wykorzystywane są do tego zainfekowane wcześniej urządzenia, tzw. botnety, które działają jednocześnie z różnych lokalizacji. Wskutek zalania dużą liczbą połączeń system staje się niedostępny i w efekcie dostęp do systemu staje się niemożliwy. Przerwy w dostępności usług cyfrowych mogą bezpośrednio zakłócić obsługę klientów i osłabić zaufanie do organizacji. Oznacza to również realne koszty związane z przywracaniem systemów do działania oraz opóźnienia w realizacji projektów czy zamówień. Warto pamiętać, że takie incydenty bywają wykorzystywane jako forma odwrócenia uwagi – w momencie, gdy organizacja skupia się na usunięciu awarii, cyberprzestępcy mogą próbować przeprowadzić inne działania, np. kradzież danych czy włamanie do infrastruktury[10].

   Przykład: Pod koniec kwietnia 2025 r. doszło do zmasowanego ataku DDoS na kluczowe polskie e-usługi, w tym aplikację mObywatel[11] i system CEPiK[12]. Atak polegał na zasypaniu serwerów ogromną liczbą fałszywych zapytań, co doprowadziło do ich przeciążenia i utrudniło działanie wybranych funkcji. Użytkownicy zgłaszali problemy z dostępem do poszczególnych usług, choć podstawowe dokumenty w aplikacji pozostały dostępne. Termin ataku był szczególnie dotkliwy, ponieważ przypadł na ostatni dzień składania deklaracji podatkowych i wniosków o świadczenia społeczne, co zwiększyło jego skutki[13].

   Sposoby zapobiegania: Stosowanie w organizacji odpowiednich technologii, takich jak zapory sieciowe, systemy wykrywania anomalii, czy usługi filtrowania ruchu. Bardzo istotne jest również regularne aktualizowanie systemów oraz edukacja użytkowników sieci organizacji. Dodatkowym zabezpieczeniem będzie skorzystanie z zewnętrznych usług bezpieczeństwa, które minimalizują ryzyko zakłócenia działania systemów.

2. **Złośliwe oprogramowanie (ang. malware)** – to każdy rodzaj programu stworzonego przez cyberprzestępców w celu wyrządzenia szkody, np. kradzieży lub zniszczenia danych, zakłócania pracy systemów czy uzyskania nieautoryzowanego dostępu do urządzeń i sieci. Do infekcji może dojść na wiele sposobów: poprzez zainfekowane załączniki poczty elektronicznej, niebezpieczne pliki pobierane z Internetu,

10 Centralne Biuro Zwalczania Cyberprzestępczości, „Ataki typu DDoS (Distributed Denial of Service)" [artykuł online]. Dostęp: https://cbzc.policja.gov.pl/bzc/zagrozenia-w-sieci/458,Atak-typu-DDoS-Distributed-Denial-of-Service.html. (24 listopada 2025)

11 mObywatel – bezpłatna aplikacja mobilna stworzona przez Ministerstwo Cyfryzacji oferująca dostęp do cyfrowych usług urzędowych oraz elektronicznych dokumentów takich jak np.: dowód osobisty, prawo jazdy, czy legitymacja studencka.

12 System CEPiK – to system informatyczny, który obejmuje centralną ewidencję kierowców (CEK) oraz centralną ewidencję pojazdów (CEP). W systemie gromadzone są między innymi dane o pojazdach i ich właścicielach oraz o kierowcach.

13 Marszycki, Mikołaj, „Zmasowany atak DDos na polskie e-usługi: mObywatel i CEPIK" [artykuł online]. Dostęp: https://itwiz.pl/zmasowany-atak-ddos-na-polskie-e-uslugi-mobywatel-i-cepik/. (24 listopada 2025)

odwiedzenie spreparowanej strony, użycie niezaufanego nośnika USB czy wykorzystanie luk w nieaktualnym oprogramowaniu. Wśród najczęściej spotykanych typów malware znajdują się wirusy, które przyczepiają się do innych plików i rozprzestrzeniają wraz z nimi, oraz tzw. trojany[14] udające legalne programy, których instalację przestępcy często wymuszają technikami socjotechnicznymi. Po uruchomieniu trojan może umożliwić atakującemu przejęcie kontroli nad systemem, wykradanie danych lub ich niszczenie[15].

Przykład: W 2024 roku jedną z największych kampanii z użyciem malware dystrybuowaną na platformie Google Play był tzw. Joker, który każdorazowo podszywał się pod pozornie niegroźne aplikacje, np. te przeznaczone do poprawiania zdjęć. Kompleksowa analiza zachowania złośliwego oprogramowania ujawniła wyrafinowany i szkodliwy mechanizm zaprojektowany w celu subskrybowania przez użytkowników płatnych usług premium bez ich wiedzy i zgody[16].

Sposoby zapobiegania: Aby skutecznie zapobiegać infekcjom malware, warto łączyć kilka podstawowych zasad bezpieczeństwa. Kluczowe jest korzystanie z nowoczesnych i sprawdzonych rozwiązań, które wykrywają i blokują zagrożenia w czasie rzeczywistym, a także monitorują sieć i anomalie. Należy też zachować czujność w kwestii otwierania linków z podejrzanych źródeł, a także zwracać uwagę na rzetelność stron internetowych, na których podajemy swoje hasła i inne dane wrażliwe. Regularne tworzenie kopii zapasowych pozwala przywrócić dane w przypadku ich utraty. Dodatkowe zabezpieczenia, takie jak firewall, uwierzytelnianie wieloskładnikowe czy VPN, wzmacniają ochronę i pomagają utrzymać wysoki poziom bezpieczeństwa cyfrowego[17].

3. **Atak ransomware** – jest to jeden z rodzajów malware, który polega na zainfekowaniu systemu informatycznego organizacji złośliwym oprogramowaniem, które może uniemożliwić dalsze korzystanie z danych lub systemów poprzez ich zaszyfrowanie lub zablokowanie dostępu. Odzyskanie dostępu do systemu ICT wymaga zapłaty okupu w zamian za przywrócenie funkcjonalności lub odzyskanie danych. W niektórych wariantach przestępcy, poza szyfrowaniem, równolegle wykradają dane i grożą ich ujawnieniem, jeśli okup nie zostanie zapłacony[18].

   Istnieją trzy główne sposoby zainfekowania:

   - wykorzystanie podatności (np. niezałatanych błędów) w aplikacjach, systemach i usługach,
   - nieprawidłowo zabezpieczony dostęp do stacji roboczych,

14 Trojan to wirus komputerowy (rodzaj złośliwego oprogramowania), które może samodzielnie się powielać oraz rozprzestrzeniać na urządzeniu. Początkowo utrudnia codzienne użytkowanie, np. poprzez spowolnienie systemu. Następnie niektóre z wirusów mogą powodować poważne szkody typu utrata danych.

15 Baramundi, „Złośliwe oprogramowanie (malware)" [artykuł online]. Dostęp: https://www.baramundi.com/pl-pl/zasoby/slowniczek/pojecie/malware/. (24 listopada 2025)

16 CERT Polska, „Mroczny rycerz powraca: Analiza złośliwego oprogramowania Joker" [artykuł online]. Dostęp: https://cert.pl/posts/2024/10/analiza-joker/. (24 listopada 2025)

17 Chudziński, Paweł, „Czym jest malware i jak chronić się przed jego atakami" [artykuł online]. Dostęp: https://securivy.com/blog/malware/#Jak_chronic_sie_przed_szkodliwym_oprogramowaniem. (24 listopada 2025)

18 Dowództwo Komponentu Wojsk Obrony Cyberprzestrzeni, „Przebieg ataku oraz zabezpieczanie przed ransomware" [artykuł online]. Dostęp: https://www.wojsko-polskie.pl/woc/articles/publikacje-r/przebieg-ataku-oraz-zabezpieczanie-przed-ransomware/. (24 listopada 2025)

Rysunek 1.2 *Uproszczony atak z wykorzystaniem oprogramowania ransomware.*

Źródło: pchor. Słupczewski, Bartosz, „Przebieg ataku oraz zabezpieczanie przed ransomware" [artykuł online]. Dostęp: https://www.wojsko-polskie.pl/woc/articles/publikacje-r/przebieg-ataku-oraz-zabezpieczanie-przed-ransomware/ (24 listopada 2025)

- phishing – nakłanianie do pobrania zainfekowanego załącznika lub otwarcia złośliwej witryny.

Przykład: Jesienią 2025 roku platforma sky-shop.pl, która umożliwia każdemu założenie swojego sklepu internetowego, poinformowała klientów (właścicieli sklepów), że dane ich klientów zostały wykradzione. Poszkodowanych miało zostać 9000 różnych sklepów[19]. Przykład ten możemy uznać za zbliżony do ataku na jeden z podmiotów członkowskich klastra – sky-shop.pl jako platforma również przetwarzała wiele danych z różnych sklepów, podobnie jak koordynator klastra.

Sposoby zapobiegania: Aby zapobiegać atakom ransomware, warto stosować podejście wielowarstwowej ochrony, tj. regularnie tworzyć i przechowywać offline kopie zapasowe i regularnie testować prawidłowość ich wykonania, blokować przedostawanie się złośliwego oprogramowania poprzez filtrowanie poczty i stron oraz stosowanie oprogramowania antywirusowego, dbać o aktualizację systemów i aplikacji, ograniczać uprawnienia użytkowników do koniecznego minimum i wyłączać makra[20] w plikach, a także używać dwustopniowego uwierzytelniania i segmentacji sieci, aby utrudnić rozprzestrzenianie się infekcji. Niezbędne jest również posiadanie procedury reagowania na incydenty, dzięki której możliwe będzie podjęcie skutecznych działań zaradczych w celu zminimalizowania skutków wystąpienia incydentu, podjęcie działań zapobiegawczych, których celem będzie zminimalizowanie możliwości wystąpienia zbliżonych zdarzeń w przyszłości, a także przywrócenie działania organizacji do poziomu sprzed wystąpienia incydentu[21].

4. **Phishing** – to najpopularniejszy rodzaj cyberataku oparty na inżynierii społecznej, którego celem jest wyłudzenie poufnych informacji (np. loginów, haseł, numerów kart kredytowych, danych bankowych lub wrażliwych informacji firmowych). Zamiast wykorzystywać luki w oprogramowaniu, phishing celuje w człowieka i jego podatność na manipulację. Atakujący podszywa się pod zaufaną instytucję (np. bank, operatora, partnera biznesowego) lub osobę, stosując techniki wywołujące strach, poczucie pilności lub ciekawość, aby skłonić ofiarę do natychmiastowej reakcji (np. kliknięcia w złośliwy link, zalogowania się na fałszywej stronie w celu autoryzacji lub pobrania zainfekowanego pliku zawierającego

19 Niebezpiecznik, „Atak na klientów 9000 różnych polskich sklepów internetowych" [artykuł online]. Dostęp: https://niebezpiecznik.pl/post/atak-na-klientow-9000-roznych-polskich-sklepow-internetowych/. (24 listopada 2025)

20 Makra w plikach to sekwencje poleceń, które automatyzują powtarzalne zadania, np. w programach typu Excel. Można je nagrywać (rejestrować) jako zbiór akcji, a następnie uruchamiać za pomocą skrótu klawiszowego lub przycisku.

21 Ministerstwo Cyfryzacji, „Jak zapobiegać atakom typu ransomware? – Poradnik PRCyber-03" [artykuł online]. Dostęp: https://www.gov.pl/web/baza-wiedzy/jak-zapobiegac-atakom-typu-ransomware--poradnik-prcyber-03. (24 listopada 2025)

złośliwe oprogramowanie, czyli malware)[22]. Rodzajem phishingu jest również **smishing**, czyli atak przeprowadzany przy wykorzystaniu wiadomości SMS lub komunikatorów internetowych oraz **vishing** (ang. voice phishing), czyli atak przeprowadzany podczas rozmowy głosowej (np. rozmowy telefonicznej).

Przykład: W jednej z kampanii analizowanych przez CERT Polska oszuści w wiadomościach poczty elektronicznej podszywali się pod Microsoft 365. Wiadomość nakłaniała do „resetu hasła", prowadząc do spreparowanej strony, która zapisywała dane użytkownika[23].

Sposoby zapobiegania: Aby uchronić się przed phishingiem należy dokładnie sprawdzać adresy URL, ograniczyć zaufanie do wiadomości z pilnymi komunikatami/prośbą o wykonanie jakiejś czynności, nie klikać pochopnie w linki przesyłane w SMS lub mailu, nie uruchamiać makr w plikach Office oraz, jak w przypadku każdego innego cyberzagrożenia, **regularnie edukować swój zespół oraz członków kastra**.

5. **Socjotechnika/inżynieria społeczna (ang. social engineering)** – jest to forma manipulacji psychologicznej, w której przestępcy wykorzystują emocje, takie jak strach, zaufanie, pośpiech, ciekawość, czy potrzebę pomocy, aby nakłonić nas do zrobienia czegoś niebezpiecznego z punktu widzenia bezpieczeństwa cyfrowego. Celem działań socjotechnicznych zawsze jest skłonienie ofiary do podjęcia określonego działania, na przykład udostępnienia informacji lub zainstalowania czegoś na urządzeniu[24].

   Przykład: Atakujący często podszywają się pod pracowników wsparcia IT, przechwytują prywatne dane, takie jak imię i nazwisko, data urodzenia lub adres oraz dane logowania. Przykładem może być podszywanie się za reprezentanta banku, który będzie chciał, aby podać mu numer PIN do karty. W przypadku organizacji klastrowych możemy wyobrazić sobie sytuację, w której ktoś podaje się za reprezentanta koordynatora klastra i prosi o podanie poufnych danych nt. podmiotu członkowskiego.

   Sposoby zapobiegania: Między innymi ważne jest weryfikowanie wszystkich maili, treści wiadomości SMS[25] itp. oraz ich nadawców (adresów, z których są wysyłane[26]), włączenie filtru SPAM, zwracanie uwagi na wszystkie linki oraz załączniki[27] dołączone w mailu, bieżące aktualizowanie oprogramowania antywirusowego.

6. **Ataki na infrastrukturę OT (ang. Operational Technology – infrastruktura odpowiadająca za sterowanie systemami przemysłowymi)** – to cyberzagrożenia wymierzone w sieci OT, czyli systemy, które kontrolują fizyczne procesy przemysłowe, na przykład procesy produkcji, przepływy energii, organizację transportu czy

22 EY, „Phishing – co to jest I jak reagować na oszustwa internetowe?" [artykuł online]. Dostęp: https://www.ey.com/pl_pl/insights/consulting/phishing-co-to-jest#definicja. (24 listopada 2025)

23 ODO24.pl, „Przykłady phishingu – analiza najczęstszych błędów użytkowników" [artykuł online]. Dostęp: https://odo24.pl/blog-post.przyklady-phishingu. (24 listopada 2025)

24 ComCert, „Socjotechnika, czyli włamanie do naszych emocji" [artykuł online]. Dostęp: https://www.comcert.pl/socjotechnika-czyli-wlamanie-do-naszych-emocji/. (24 listopada 2025)

25 Przykłady fałszywych SMS można znaleźć na stronie CERT.Polska. Dostęp: https://cert.pl/baza-wiedzy/falszywe-sms-y/. (24 listopada 2025)

26 Przykłady takich kampanii phishingowych na serwisy pocztowe można znaleźć na stronie CERT.Polska. Dostęp: https://cert.pl/posts/2023/04/phishing-webmail/. (24 listopada 2025)

27 Przykłady fałszywych załączników można znaleźć na stronie CERT.Polska. Dostęp: https://cert.pl/falszywe-zalaczniki/. (24 listopada 2025)

też całe zakłady przemysłowe. W odróżnieniu od typowych środowisk IT, sieci OT zarządzają realnymi urządzeniami: maszynami, sterownikami PLC (ang. uniwersalne urządzenie mikroprocesorowe przeznaczone do sterowania pracą maszyny lub urządzenia technologicznego), systemami SCADA (ang. Supervisory Control and Data Acquisition – system informatyczny do nadzorowania, kontrolowanie i zbierania danych z procesów przemysłowych), które wpływają na fizyczne procesy. Najczęstszymi zagrożeniami są: ransomware, DDoS, Malware, czy szpiegostwo przemysłowe[28], co zostało objaśnione wcześniej.

Przykład: W lipcu 2024 roku rosyjskie grupy hakerskie przeprowadziły ataki DDoS na polską infrastrukturę krytyczną, co zbiegło się w czasie z oświadczeniem polskiego rządu o aprobacie zestrzeliwania rosyjskich rakiet na terytorium Ukrainy.

Sposoby zapobiegania: Kluczowe jest przede wszystkim odseparowanie sieci OT od sieci, aby ograniczyć ryzyko przeniesienia zagrożeń z komputerów pracowników na systemy sterujące produkcją. Ważna jest również segmentacja sieci, tak aby incydent w jednym obszarze nie sparaliżował całej infrastruktury. Należy również dbać o aktualizację urządzeń i sterowników, kontrolę dostępu, tworzenie kopii zapasowych konfiguracji systemów i sterowników, a także szkolić pracowników produkcji, operatorów i techników, by potrafili rozpoznawać podejrzane sytuacje i właściwie zareagować.

7. **Ataki na łańcuchy dostaw (ang. supply chain attacks)** – to strategia cyberprzestępców, polegająca na pośrednim ataku na docelową organizację. Zamiast atakować podmiot bezpośrednio (np. dużą korporację), hakerzy celują w jej mniej zabezpieczonych, ale zaufanych partnerów, dostawców lub sprzedawców (tzw. podmioty trzecie), czyli w jeden z elementów jej łańcucha dostaw. Uzyskując dostęp do sieci lub produktów tego dostawcy, hakerzy wykorzystują zaufanie, jakim obdarza go docelowa ofiara, aby dostarczyć złośliwe oprogramowanie (malware), które jest często zaszyte w legalnych aktualizacjach oprogramowania, kodzie źródłowym, a nawet w fizycznym sprzęcie (np. zainfekowany dysk USB lub oprogramowanie używanego urządzenia). Ponieważ złośliwe ładunki docierają z zaufanego źródła, są niezwykle trudne do wykrycia i mogą spowodować katastrofalne szkody, dotykając jednocześnie wielu partnerów w łańcuchu. W kontekście klastra oznacza to, że brak odpowiednich zabezpieczeń u jednego członka klastra może otworzyć „tylne drzwi" do sieci i danych wszystkich pozostałych członków współpracujących z tym podmiotem[29].

28 nFlo, „Bezpieczeństwo sieci OT: analiza, różnice z IT, zagrożenia i najlepsze praktyki" [artykuł online]. Dostęp: https://nflo.pl/baza-wiedzy/bezpieczenstwo-sieci-ot-analiza-roznice-z-it-zagrozenia-i-najlepsze-praktyki/#jakie-zagrozenia-cybernetyczne-zagrazaja-sieciom-przemyslowym. (24 listopada 2025)

29 Keepersecurity, „Czym jest atak na łańcuch dostaw?" [artykuł online]. Dostęp: https://www.keepersecurity.com/pl_PL/threats/supply-chain-attack/. (24 listopada 2025)

Przykład: W lutym 2024 r., Change Healthcare, dostawca usług zarządzania przychodami i płatnościami, który łączy płatników, dostawców i pacjentów w USA, został zaatakowany przez oprogramowanie ransomware. Atak zakłócił usługi opieki zdrowotnej w całym kraju na kilka tygodni i pozwolił oszustom na wyniesienie danych medycznych „istotnej liczby Amerykanów". Jej firma macierzysta, UnitedHealth, stwierdziła, że całkowite koszty tego ataku prawdopodobnie przekroczą 1 miliard dolarów[30].

Zapobieganie: Zapobieganie atakom na łańcuch dostaw opiera się przede wszystkim na kontroli i ograniczeniu zaufania do partnerów zewnętrznych. Wymaga to weryfikacji zabezpieczeń dostawców, a następnie egzekwowania zasady najmniejszego przywileju[31], minimalizując ich dostęp do sieci tylko do niezbędnego zakresu.

Wnioski dla koordynatora: Warto uświadamiać członków klastra na temat zagrożeń, jakie mogą pojawić się w cyberprzestrzeni i informować o ostatnich atakach np. wysyłając raz w miesiącu krótką informację dot. Tego, co wydarzyło się w cyberprzestrzeni, polecić stronę internetową lub profil organizacji, która informuje o takich incydentach na bieżąco.

1.4 Kontekst regulacyjny

Cyberbezpieczeństwo to dziś domena objęta ścisłymi regulacjami, a dynamiczny rozwój zagrożeń w cyberprzestrzeni wymusza na państwach, w tym Polsce, implementację kompleksowych ram prawnych. Jako członek Unii Europejskiej, Polska adaptuje unijne akty prawne do krajowego porządku prawnego, kształtując tym samym obowiązkowe ramy ochrony danych, bezpieczeństwa teleinformatycznego i budowania odporności cyfrowej. Z perspektywy prawnej regulacje te nakładają na podmioty, zarówno z sektora publicznego, jak i prywatnego, szereg obowiązków. Wszystkim przepisom przyświeca jeden cel: zbudować w kraju trwałą odporność oraz stworzyć ramy regulacyjne pozwalające na budowanie trwałej odporności systemów teleinformatycznych na współczesne zagrożenia cybernetyczne, co jest fundamentalne dla zachowania stabilności gospodarki cyfrowej i ochrony interesów państw oraz samych przedsiębiorstw i instytucji publicznych.

Wśród kluczowych polskich regulacji kształtujących rynek cyberbezpieczeństwa możemy wyróżnić:

- **Ustawę o Krajowym Systemie Cyberbezpieczeństwa** – stanowi polską implementację prawa Unii Europejskiej (dyrektywy NIS2). Jej głównym celem jest ustanowienie ram bezpieczeństwa cybernetycznego państwa poprzez określenie katalogu podmiotów kluczowych (np. operatorów usług kluczowych i dostawców usług cyfrowych) oraz nałożenie na nie obowiązków w zakresie zarządzania ryzykiem, stosowania adekwatnych zabezpieczeń i raportowania incydentów do odpowiednich jednostek CSIRT (ang. Computer Security Incident Response Team, czyli zespół reagowania na incydenty bezpieczeństwa). W praktyce jest to podstawowy akt prawny, który reguluje, w jaki

30 Sekurak, „Jedna z największych korporacji z branży ochrony zdrowia w USA zapłaciła $ 22000000 okupu ransomware. Dostali do nich z wykorzystaniem wykradzionych danych logowanie. Change Healthcare" [artykuł online]. Dostęp: https://sekurak.pl/jedna-z-najwiekszych-korporacji-z-branzy-ochrony-zdrowia-w-usa-zaplacila-22000000-okupu-ransomware-dostali-sie-do-nich-z-wykorzystaniem-wykradzionych-danych-logowania-change-healthcare/. (24 listopada 2025)

31 Zasada najmniejszych przywilejów to koncepcja bezpieczeństwa informatycznego, która polega na przyznawaniu użytkownikom, procesom, aplikacjom i systemom tylko tych uprawnień, które są absolutnie niezbędne do wykonania konkretnych zadań.

sposób polskie firmy i instytucje mają budować swoją cyberodporność oraz reagować na stwierdzone zdarzenia i incydenty bezpieczeństwa informacji[32].

- **Rozporządzenie Ogólne o Ochronie Danych Osobowych (RODO)** – dotyczy ochrony danych osobowych osób fizycznych. Nakłada na każdą firmę, która przetwarza te dane, obowiązek wdrożenia odpowiednich środków technicznych i organizacyjnych. W przypadku naruszenia danych, organizacje są narażone na wysokie kary finansowe i poważne straty wizerunkowe[33].

- **Strategię cyberbezpieczeństwa RP** – kluczowy dokument państwowy, który wyznacza długoterminowe cele, priorytety i kierunki działań w zakresie cyberbezpieczeństwa na poziomie krajowym. Jest to strategiczna mapa dla administracji publicznej i sektora prywatnego, definiująca ambicje państwa w zakresie odporności cyfrowej, zarządzania ryzykiem oraz współpracy międzysektorowej (Publiczno-Prywatnej), mająca na celu ochronę infrastruktury krytycznej i zapewnienie bezpieczeństwa informacji. Strategia ta stanowi podstawę do planowania wszystkich działań w ramach Krajowego Systemu Cyberbezpieczeństwa (KSC). Wraz z końcem 2024 r. upłynął 5-letni okres na jaki ustanowiona została Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024, nowa strategia na lata 2025-2029 ma zostać przyjęta w IV kwartale 2025 roku.

W kontekście europejskich regulacji są to:

- **Cybersecurity Act** – rozporządzenie UE, które ustanawia ramy certyfikacji cyberbezpieczeństwa dla produktów, usług i procesów teleinformatycznych w całej Unii. Jego głównym celem jest zwiększenie zaufania do technologii cyfrowych poprzez stworzenie wspólnego, europejskiego systemu znakowania (certyfikatów), który ułatwia firmom i konsumentom ocenę poziomu bezpieczeństwa zakupionych rozwiązań[34].

- **Rozporządzenie DORA (ang. Digital Operational Resilience Act)** – rozporządzenie UE, które ujednolica zasady zarządzania ryzykiem cyfrowym i odporności operacyjnej w sektorze finansowym. Nakłada ono na banki, firmy ubezpieczeniowe i kluczowych dostawców technologii finansowych obowiązek zapewnienia, że ich systemy IT są w stanie wytrzymać, reagować i szybko powracać do działania po poważnych zakłóceniach operacyjnych i cyberatakach[35].

- **Dyrektywa NIS2 (ang. Network and Information Security Directive)** – zaktualizowana dyrektywa, która znacząco rozszerza zakres sektorów, firm i podmiotów objętych obowiązkami cyberbezpieczeństwa, w tym kluczowych dostawców w łańcuchach dostaw. Nakłada ona na te podmioty obowiązek wdrożenia

32 Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. Dz.U. 2018, poz. 1560. Dostęp: https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20180001560. (24 listopada 2025)

33 Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych. Dz.U. 2018, poz. 1000. Dostęp: https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20180001000. (24 listopada 2025)

34 Rozporządzenie (UE) 2019/881 w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych. Dz.U. L 151 z 07.06.2019. Dostęp: https://eur-lex.europa.eu/legal-content/PL/ALL/?uri=CELEX:32019R0881. (24 listopada 2025)

35 Rozporządzenie (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego oraz zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014 i (UE) 2019/2033. Dz.U. L 333 z 27.12.2022. Dostęp: https://eur-lex.europa.eu/legal-content/PL/ALL/?uri=CELEX:32022R2554. (24 listopada 2025)

surowszych środków zarządzania ryzykiem, zwiększa wymagania w zakresie ciągłości działania i sprawnego reagowania na incydenty, harmonizując jednocześnie zasady nadzoru i egzekwowania prawa w całej UE[36].

- **Dyrektywa CER (ang. Critical Entities Resilience)** – dyrektywa, która ma na celu wzmocnienie odporności fizycznej i operacyjnej kluczowych podmiotów infrastruktury krytycznej (np. energetyka, transport, zdrowie) na zagrożenia inne niż cybernetyczne (np. klęski żywiołowe, terroryzm). Dyrektywa uzupełnia NIS2, wspierając kompleksowe zarządzanie ryzykiem, które obejmuje zarówno zagrożenia cyfrowe, jak i fizyczne.

- **Rozporządzenie CRA (ang. Cyber Resilience Act)** – wdrożenie rozporządzenia ma na celu zmniejszenie liczby kluczowych podatności w oprogramowaniach i zwiększenie bezpieczeństwa użytkowników poprzez m.in. uwzględnienie przez producentów sprzętu elektronicznego zasad cyberbezpieczeństwa już na etapie projektowania produktu, czy zobligowania producentów do zapewnienia, że przez określony czas podatności są skutecznie obsługiwane[37].

W rozdziale drugim niniejszego podręcznika zostanie przedstawiona szersza analiza implementacji dyrektywy NIS2 do polskiego porządku prawnego oraz Cyber Resilience Act, czyli dwóch regulacji prawnych najważniejszych z perspektywy koordynatora klastra. Są to dokumenty, które obejmują najszerszą grupę sektorów, w które wpisuje się działalność polskich klastrów.

Na tym etapie warto również wspomnieć o normach i standardach, które opracowywane są przez Międzynarodową Organizację Normalizacyjną w Genewie. Mają one kluczowe znaczenie dla regulowania praktyk biznesowych, produkcji oraz jakości. Normy ISO są dokumentami opracowanymi przez niezależnych, międzynarodowych ekspertów z danych dziedzin gospodarki. Zawierają informacje, wskazówki oraz zbiory dobrych praktyk dla różnorodnych aspektów działalności. Mają charakter uniwersalny, dlatego mogą być stosowane przez firmy i organizacje państwowe oraz prywatne, należące do każdej branży i sektora, niezależnie od wielkości i posiadanych rozwiązań[38].

W rozdziale drugim niniejszego poradnika zostaną omówione te normy, które odgrywają istotną

36 Dyrektywa (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 (NIS2). Dz.U. L 333 z 27.12.2022. Dostęp: https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32022L2555. (24 listopada 2025)

37 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/2847 z dnia 23 października 2024 r. w sprawie horyzontalnych wymagań w zakresie cyberbezpieczeństwa w odniesieniu do produktów z elementami cyfrowymi oraz w sprawie zmiany rozporządzeń (UE) nr 168/2013 i (UE) 2019/1020 i dyrektywy (UE) 2020/1828 (akt o cyberodporności)/ Dostęp: https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng. (24 listopada 2025)

38 Resilia, „Normy ISO w firmie: czym są? Wszystko o normach ISO, wdrażaniu i certyfikatach”[artykuł online]. Dostęp: https://resilia.pl/blog/normy-iso-definicja-rodzaje-czy-warto-wdrazac/. (24 listopada 2025)

rolę w standaryzacji obszaru bezpieczeństwa informacji, ciągłości działania oraz cyberbezpieczeństwa, tj. ISO 27001 oraz ISO 22301.

Warto wspomnieć, że oprócz norm ISO funkcjonują również m.in. standardy NIST (ang. National Institute of Standards and Technology), które są zbiorem rekomendacji, wytycznych i ram cyberbezpieczeństwa opracowanych przez amerykański instytut NIST. Rekomendacje te mają na celu pomoc organizacjom w zarządzaniu ryzykiem cybernetycznym.

Wnioski dla koordynatora: Aktywna pomoc w zrozumieniu i spełnieniu regulacji oraz wymogów jest jedną z kluczowych usług klastra. Jest to podstawa budowania cyfrowej odporności wymaganej przez prawo i rynek. Brak zgodności z przepisami może skutkować nie tylko karami finansowymi, ale również utratą zaufania partnerów i ograniczeniem możliwości uczestnictwa w projektach finansowanych ze środków publicznych. Dlatego też warto pomyśleć o dodatkowej usłudze dla członków klastra polegającej na doradztwie w zakresie cybersecurity compliance (zgodności z normami i przepisami dot. cyberbezpieczeństwa).

1.5 Kontekst zewnętrzny (geopolityka i technologia)

Współczesny krajobraz cyberbezpieczeństwa jest nierozerwalnie związany z geopolityką i cyberwojną. Cyberprzestrzeń stała się kluczowym elementem rywalizacji państwowej, dlatego państwowi aktorzy (grupy APT – ang. Advanced Persistent Threat – zorganizowane jednostki przeprowadzające ataki w cyberprzestrzeni), w tym grupy z Chin, Rosji, Iranu czy Korei Północnej, prowadzą coraz bardziej zaawansowane operacje, których głównym celem jest infrastruktura krytyczna (np. energetyka, transport, komunikacja). Ich taktyki często obejmują „pre-pozycjonowanie" (umieszczanie uśpionych złośliwych implantów w celu przyszłej destabilizacji) oraz wykorzystanie sztucznej inteligencji (AI) do tworzenia wyrafinowanych ataków i dezinformacji.

Co ważne, ataki państwowe (lub inspirowane przez państwa) są często skierowane nie tylko w cele militarne czy rządowe, ale też szeroko pojęty biznes. Od początku rosyjskiej inwazji na Ukrainę, Polska jest stałym obiektem działań hybrydowych Kremla, w tym ataków w cyberprzestrzeni. Według informacji Ministerstwa Cyfryzacji jest to konsekwencja zaangażowania w pomoc walczącej Ukrainie, a także zdecydowanego zabiegania o wsparcie Kijowa na arenie międzynarodowej[39].

Odporność cyfrowa klastra jest częścią bezpieczeństwa ekonomicznego regionu i kraju. Organizacje działające w sektorze prywatnym mogą stać się pośrednimi celami, np. przez powiązania z dostawcami infrastruktury lub przez używanie powszechnych rozwiązań chmurowych. Klastry, zrzeszające setki przedsiębiorstw, instytucji naukowych i samorządów, mogą pełnić rolę „tarczy" – przestrzeni wymiany informacji o zagrożeniach i wspólnego budowania odporności.

Znaczenie w kontekście technologicznym ma również nieustający wzrost liczby urządzeń IoT (ang. Internet of Things – urządzenia połączone w sieci), np. kamery, sensory, automatyka przemysłowa itd. Eksperci z IoT Analytics przewidują, że do 2030 roku będzie aktywnych prawie 30 miliardów tego

39 Ministerstwo Cyfryzacji, „Rosyjskie cyberataki" [artykuł online]. Dostęp: https://www.gov.pl/web/sluzby-specjalne/rosyjskie-cyberataki. (24 listopada 2025)

typu urządzeń[40]. Stają się one potencjalnymi punktami wejścia dla ataków, co jest szczególnie istotne w klastrach produkcyjnych lub energetycznych.

Wnioski dla koordynatora: Warto śledzić aktualną sytuację geopolityczną i reagować na bieżące komunikaty, dzieląc się nimi z członkami klastra. W tym kontekście istotne są również raporty roczne CERT Polska (www.cert.pl), czy biuletyn informacji NASK dostępny na portalu Linkedin[41].

1.6 Mapa interesariuszy

W kontekście bezpieczeństwa cyfrowego klaster funkcjonuje jako sieć zależności, w której uczestniczy wiele podmiotów mających realny wpływ na poziom ochrony informacji, systemów i procesów. Ci interesariusze tworzą złożony ekosystem, w którym działania jednego podmiotu mogą wzmacniać lub osłabiać cyberodporność całej struktury.

Najważniejszą grupę stanowią członkowie klastra, czyli przedsiębiorstwa, instytucje badawcze, uczelnie i inne. To oni na co dzień przetwarzają dane, prowadzą projekty, korzystają z systemów informatycznych i podejmują decyzje operacyjne. Poziom ich dojrzałości cyberbezpieczeństwa, w tym podstawowe praktyki, takie jak aktualizacje oprogramowania czy zarządzanie hasłami, bezpośrednio lub pośrednio wpływa na bezpieczeństwo partnerów. W praktyce oznacza to, że nawet mała firma z klasycznej branży produkcyjnej może stać się „wejściem" do bardziej zaawansowanych podmiotów, jeśli nie stosuje odpowiednich zabezpieczeń.

Kluczową rolę pełni również koordynator klastra, który w naturalny sposób staje się centrum wymiany informacji i inicjatorem działań zwiększających bezpieczeństwo. To on może organizować szkolenia, przekazywać ostrzeżenia o nowych zagrożeniach, koordynować działania prewencyjne i reagować na incydenty. Jako podmiot zaufania publicznego w ekosystemie współpracy, koordynator bywa pierwszym źródłem wiedzy dla członków klastra, które nie mają własnych specjalistów ds. bezpieczeństwa.

Ważną grupą są również dostawcy technologii i usług IT. To oni zapewniają narzędzia, takie jak systemy chmurowe, oprogramowanie komunikacyjne, platformy CRM (ang. Customer Relationship Management, tłum. oprogramowanie do zarządzania relacjami z klientami), czy usługi serwisowe. Od jakości ich pracy, sposobu zarządzania podatnościami i reakcji na incydenty zależy bezpieczeństwo wielu członków klastra. Z tego względu ocena dostawców, stosowanie umów SLA (ang. Service Level Agreement – umowy gwarantujące określony zakres i poziom usług), wymogów bezpieczeństwa, czy certyfikacji staje się kluczowym elementem zarządzania ryzykiem.

Nie można również pominąć instytucji publicznych, takich jak NASK, CERT Polska, Ministerstwo Cyfryzacji, PARP (Polska Agencja Rozwoju Przedsiębiorczości), czy ARP (Agencja Rozwoju Przemysłu), które dostarczają wytyczne, programy wsparcia, raporty o zagrożeniach, a często także finansowanie działań podnoszących odporność cyfrową. W sytuacjach kryzysowych stanowią one również źródło oficjalnych komunikatów i wsparcia merytorycznego.

W ekosystemie bezpieczeństwa istotną rolę odgrywają także podmioty międzynarodowe i inne

40 NASK, „Inteligentne sprzęty domowe potrafią nas przechytrzyć. Zbierają dane, mogą ułatwić dostęp do konta" [artykuł online]. Dostęp: https://www.nask.pl/magazyn/inteligentne-sprzety-domowe-potrafia-nas-przechytrzyc-moga-ulatwic-cyberprzestepcom-dostep-do-konta. (24 listopada 2025)

41 NASK, „BiuletynNASK". Dostęp: https://www.linkedin.com/newsletters/biuletyn-nask-7048947139384623104/. (24 listopada 2025)

klastry oraz instytucje otoczenia biznesu, zwłaszcza w obszarach o wysokim stopniu cyfryzacji.

Współpraca w ramach europejskich sieci i projektów transgranicznych pozwala na wymianę wiedzy, szybkie reagowanie na globalne zagrożenia oraz adaptację sprawdzonych praktyk. Często to właśnie inne klastry lub ich partnerzy jako pierwsi identyfikują nowe kampanie czy rodzaje cyberataków, które mogą dotknąć również polski rynek. Należy również pamiętać o kontrahentach i klientach członków klastra. Coraz częściej wymagają oni spełnienia określonych standardów bezpieczeństwa lub przedstawienia dowodów zgodności z regulacjami (np. NIS2). Ich oczekiwania kształtują poziom bezpieczeństwa całego ekosystemu – brak odpowiedniego przygotowania może oznaczać utratę kontraktów lub ograniczenie dostępu do łańcuchów dostaw.

Każdy z tych interesariuszy ma inną rolę, kompetencje i poziom świadomości, ale wszyscy wspólnie tworzą system naczyń połączonych, w którym słabość jednego podmiotu może zagrozić pozostałym. Stąd w dobrze funkcjonującym klastrze niezwykle ważna staje się współpraca, wymiana informacji i budowanie wspólnych standardów bezpieczeństwa.

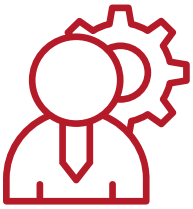
Rysunek 1.3 *Mapa interesariuszy w kontekście cyberbezpieczeństwa klastra.*

Grupa interesariuszy

Rola i wpływ na bezpieczeństwo.

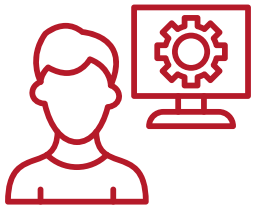
Członkowie klastra

Podstawowi uczestnicy ekosystemu. Ich praktyki bezpieczeństwa wpływają bezpośrednio na odporność całej sieci.



Koordynator klastra

Lider działań w zakresie cyberbezpieczeństwa, inicjator szkoleń, projektów i standardów.



Dostawcy technologii i usług IT

Zapewniają narzędzia i rozwiązania; mogą być źródłem ryzyka lub wsparcia w ochronie.

Instytucje publiczne

Źródło programów wsparcia, funduszy i rekomendacji regulacyjnych.

Partnerzy międzynarodowi i inne klastry

Wymiana wiedzy i dobrych praktyk, wspólne projekty w ramach sieci europejskich.

Klienci i kontrahenci

Wymuszają określone standardy bezpieczeństwa w łańcuchu dostaw.

Źródło: Opracowanie własne.

Rozdział 2

Cyberbezpieczeństwo w kontekście regulacyjnym

Cyberbezpieczeństwo jest ściśle powiązane z polskimi i europejskimi regulacjami, które określają funkcjonowanie krajowego systemu cyberbezpieczeństwa, a także nakładają na poszczególne podmioty szereg obowiązków z tego obszaru. Regulacje wprowadzają też określone standardy i zwykle dotyczą organizacji działających w określonym sektorze. Poniżej omówione zostaną regulacje, które wchodzą w życie w najbliższych latach.

Rozdział przedstawia najważniejsze europejskie i krajowe regulacje dotyczące cyberbezpieczeństwa (NIS2/UKSC2, CRA) oraz rolę, jaką powinny pełnić klastry we wspieraniu członków w procesie dostosowania do nowych obowiązków. Opisuje zakres sektorów objętych ustawą, różnice między podmiotami kluczowymi i ważnymi, znaczenie samoidentyfikacji oraz konieczność podejścia opartego na analizie ryzyka. Podkreśla, że regulacje wymagają zarówno środków technicznych, jak i organizacyjnych, a także wiążą się z istotnymi sankcjami finansowymi oraz odpowiedzialnością osobistą zarządu. Rozdział wskazuje konkretne działania, jakie koordynator klastra powinien podjąć – od edukacji i dystrybucji narzędzi, przez organizację szkoleń z ekspertami, po pomoc we wdrażaniu norm (ISO 27001, ISO 22301), analizę ryzyka oraz wsparcie w uzyskaniu polis cyber. Całość pokazuje, że klastry pełnią kluczową rolę w podnoszeniu świadomości i odporności cyfrowej podmiotów klastrowych w swoich sektorach.

2.1 Dyrektywa NIS oraz Ustawa o Krajowym Systemie Cyberbezpieczeństwa

Obecnie najważniejszym aktem prawnym z dziedziny cyberbezpieczeństwa obowiązującym w Polsce jest Ustawa o Krajowym Systemie Cyberbezpieczeństwa (dalej: UKSC), która wdraża w polski porządek prawny europejską dyrektywę NIS. W 2022 r. Dyrektywa ta uległa aktualizacji (aktualnie dyrektywa NIS2), nakładając na Państwa członkowskie obowiązek nowelizacji rodzimych przepisów do października 2024 r. Obecna wersja nowelizacji UKSC została przyjęta przez Radę Ministrów w październiku 2025 r., a następnie przekazana do prac Sejmu. Dlatego też w niniejszym poradniku skupimy się przepisach (głównie NIS2/UKSC2), które w przeciągu kilku najbliższych miesięcy zaczną obowiązywać w kraju.

2.2 Dyrektywa NIS2 oraz Nowelizacja Ustawy o Krajowym Systemie Cyberbezpieczeństwa (UKSC2)

Ustawa będzie obowiązywać podmioty prywatne i publiczne, które spełniają określone kryteria oraz działają w sektorach zdefiniowanych jako kluczowe lub ważne[42].

Powyższe zestawienie przedstawia ogólne sektory objęte regulacjami. Każdy sektor dzieli się na podsektory, a szczegółowy opis wyjaśnia, jaki rodzaj podmiotu kwalifikuje się do danego katalogu. Dokładne zapoznanie się z treścią Załącznika nr 1 oraz nr 2 do ustawy jest kluczowe, ponieważ każdy podmiot musi dokonać samoidentyfikacji, której brak będzie skutkował konsekwencjami finansowymi.

Różnice pomiędzy sektorami kluczowymi i ważnymi są niewielkie – można ująć je w stwierdzeniu, że podmioty kluczowe są ściślej niż podmioty ważne nadzorowane przez organy właściwe,

42 Projekt Ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (projekt z dnia 7 października 2025 r.). Dostęp: https://legislacja.gov.pl/projekt/12384504/katalog/13055207, https://legislacja.gov.pl/projekt/12384504/katalog/13055207. (24 listopada 2025)

Tabela 2.1. *Wykaz sektorów objętych Nowelizacją Ustawy o Krajowym Systemie Cyberbezpieczeństwa na podstawie projektu nowelizacji Ustawy o Krajowym Systemie Cyberbezpieczeństwa z dnia 7 października 2025 r.*

Sektory Kluczowe	Sektory Ważne
• energia, • transport, • bankowość i infrastruktura rynków finansowych, • ochrona zdrowia, • zaopatrzenie w wodę pitną i jej dystrybucja, • zbiorowe odprowadzanie ścieków, • infrastruktura cyfrowa, • zarządzanie usługami ICT, • przestrzeń kosmiczna, • podmioty publiczne (ministerstwa, urzędy centralne, wybrane agencje i jednostki wykonujące zadania publiczne).	• usługi pocztowe, • inwestycje energetyki jądrowej, • gospodarowanie odpadami, • produkcja, wytwarzanie i dystrybucja chemikaliów, • produkcja, przetwarzanie i dystrybucja żywności, • produkcja wyrobów medycznych, elektroniki, maszyn, pojazdów, • dostawcy usług cyfrowych, • badania naukowe, • podmioty publiczne (samorządowe jednostki budżetowe, zakłady budżetowe, instytucje kultury).

Źródło: Opracowanie własne na podstawie: Projekt Ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (projekt z dnia 7 października 2025 r.). Dostęp: https://legislacja.gov.pl/projekt/12384504/katalog/13055207. (24 listopada 2025)

a obowiązki są pełniejsze i bardziej szczegółowe. Różnica wynika też z poziomu kar finansowych – w przypadku podmiotów kluczowych są one wyższe niż w przypadku ważnych.

Nie jest to jednak jedyne kryterium, które decyduje o tym czy dany podmiot objęty zostanie regulacją. Nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa (KSC) przewiduje kilka niezależnych ścieżek, które mogą spowodować, że organizacja zostanie uznana za podmiot kluczowy lub podmiot ważny.

Poniższa przykładowa checklista może zostać wykorzystana przez członków klastra celem wstępnej samoidentyfikacji[43]:

Tabela 2.2 *Przykładowa checklista wspomagająca proces samoidentyfikacji podmiotów*

Kryterium	Odpowiedź	Wyjaśnienie
Działalność w sektorach ważnych i kluczowych	TAK/NIE	Jeśli TAK to podlega ustawie
Czy jesteś dużym przedsiębiorstwem? (≥250 pracowników lub ≥50 mln EUR obrotu)	TAK/NIE	Jeśli TAK to staje się podmiotem kluczowym
Czy jesteś średnim przedsiębiorstwem? (50–249 pracowników)	TAK/NIE	Jeśli TAK to staje się podmiotem ważnym

43 Tamże.

Kryterium	Odpowiedź	Wyjaśnienie
Czy system informacyjny przedsiębiorstwa jest niezależny od grupy kapitałowej do której należy firma?	TAK/NIE	Jeśli TAK, jest możliwość wyłączania z klasyfikacji
Czy jesteś jednostką budżetową, zakładem budżetowym, samodzielną instytucją kultury, spółką komunalną realizującą zadania publiczne?	TAK/NIE	Jeśli TAK, to staje się podmiotem ważnym
Czy jesteś podmiotem leczniczym zatrudniającym powyżej 250 pracowników?	TAK/NIE	Jeśli TAK to staje się podmiotem kluczowym
Czy jesteś podmiotem leczniczym zatrudniającym poniżej 250 pracowników?	TAK/NIE	Jeśli TAK to staje się podmiotem ważnym
Czy działasz na podstawie określonego zezwolenia lub koncesji w sektorze energii elektrycznej lub energetyki jądrowej?	TAK/NIE	Jeśli TAK to staje się podmiotem kluczowym

Źródło: Opracowanie własne na podstawie: Projekt Ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (projekt z dnia 7 października 2025 r.). Dostęp: https://legislacja.gov.pl/projekt/12384504/katalog/13055207. (24 listopada 2025)

Dodatkowo:

- Organ właściwy może uznać podmiot za kluczowy lub ważny, nawet jeśli nie spełnia kryteriów sektorowych lub wielkościowych, jeśli wystąpi **przynajmniej jedna z poniższych przesłanek**:
  - » podmiot jako jedyny świadczy usługę kluczową, której zakłócenie może spowodować znaczne straty dla gospodarki państwa lub zagrozić funkcjonowaniu usług niezbędnych dla funkcjonowania społeczeństwa np. dostawy energii,
  - » zakłócenie jego działalności powoduje istotne zagrożenie dla bezpieczeństwa państwa, porządku publicznego lub zdrowia publicznego,
  - » działalność podmiotu wywołuje ryzyko systemowe dla innych podmiotów – oznacza to, że zakłócenie działania takiego podmiotu w znacznym stopniu spowoduje zakłócenie funkcjonowania podmiotu objętego regulacjami (np. dostawca kluczowej usługi IT dla przedsiębiorstwa z sektora energii),
  - » znaczenie usługi jest ponadregionalne lub międzysektorowe.

- Minister właściwy ds. informatyzacji może uznać państwową osobę prawną za podmiot kluczowy, jeśli realizuje zadania publiczne z wykorzystaniem systemów informacyjnych istotnych dla funkcjonowania państwa.

- Podmiot spoza UE, który świadczy usługi na terenie Polski i nie ma tu siedziby, musi wyznaczyć przedstawiciela. Taki podmiot podlega ustawie i może zostać uznany za podmiot kluczowy lub ważny na takich samych zasadach jak firma krajowa.

Jak widać kryteria identyfikacji w wielu wypadkach nie są jednoznaczne i mogą wymagać indywidualnej interpretacji dokonanej przez organy właściwe lub kwalifikowanych prawników.

Koordynatorzy klastrów mogą wspierać swoich członków w samoidentyfikacji poprzez:

- udostępnienie narzędzi wspomagających proces samoidentyfikacji zamieszczonych w tym poradniku,
- zorganizowanie spotkania z prawnikami specjalizującymi się w dziedzinie cyberbezpieczeństwa, którzy wspomogą członków klastra w procesie samoidentyfikacji,
- dystrybucję informacji o pozostałych ogólnodostępnych narzędziach wspierających ten proces:
  - » https://www.traple.pl/formularz-samosprawdzenie-nis2/,
  - » https://grantthornton.pl/czy-moja-firma-podlega-pod-nis2/,
  - » https://www.sisoft.pl/baza-wiedzy/czy-firma-podlega-pod-nis2.

Warto zaznaczyć, że ani dyrektywa, ani krajowa ustawa nie określa z jakich narzędzi i rozwiązań należy skorzystać. Nowoczesne regulacje z obszaru cyberbezpieczeństwa stawiają na podejściu opartym o analizę ryzyka i w przypadku NIS2 nie jest inaczej. Istotny w tym kontekście jest art. 8 UKSC2, który mówi, że każdy podmiot kluczowy lub ważny wdrażając system zarządzania bezpieczeństwem informacji, zapewnia w nim:

- prowadzenie systematycznego szacowania ryzyka,
- wdrożenia odpowiednich i proporcjonalnych środków technicznych i organizacyjnych,
- zbieranie informacji o cyberzagrożeniach i podatnościach,
- zarządzanie incydentami,
- stosowanie środków zapobiegających i ograniczających wpływ incydentów na bezpieczeństwo systemu informacyjnego. Należy zaznaczyć, że system informacyjny definiowany w UKSC2 nie jest tożsamy z tradycyjną definicją systemu informacyjnego zdefiniowaną np. w normie ISO 27001[44].

Warto zapoznać się z uszczegółowieniem środków technicznych i organizacyjnych wspomnianych przez regulatora w treści:

Tabela 2.3 *Zestawienie środków organizacyjnych i technicznych zgodnie z Art. 8 nowelizacji UKSC.*

Środki techniczne	Środki organizacyjne
• bezpieczeństwo fizyczne (w tym kontrole dostępu), • bezpieczeństwo zasobów ludzkich, • monitorowanie usługi w trybie ciągłym.	• polityka szacowania ryzyka, • testowanie systemu bezpieczeństwa informacji, • wdrażanie, dokumentowanie, testowanie i utrzymanie planów ciągłości działania, • polityki i procedury oceny skuteczności środków technicznych i organizacyjnych, • edukacja personelu, • zarządzanie aktywami, • polityki kontroli dostępu.

44 Tamże.

Środki zarówno techniczne i organizacyjne
• bezpieczeństwo i ciągłość łańcucha dostaw produktów i usług ICT, od których zależy funkcjonowanie usługi, • Stosowanie zasad cyberhigieny, • Polityki i procedury stosowania kryptografii, • Stosowanie bezpiecznych środków komunikacji elektronicznej w ramach KSC.

Źródło: Opracowanie własne na podstawie: Projekt Ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (projekt z dnia 7 października 2025 r.). Dostęp: https://legislacja.gov.pl/projekt/12384504/katalog/13055207. (24 listopada 2025)

Z powyżej przedstawionych informacji jasno wynika kilka kluczowych elementów, które pozwalają zrozumieć logikę przepisów zawartych w ustawie:

1. Nie zbuduje się w organizacji cyberbezpieczeństwa wdrażając same rozwiązania techniczne, potrzebne są również odpowiednie polityki i procedury, czyli zabezpieczenia organizacyjne.

2. Budowa systemu cyberbezpieczeństwa w organizacji powinna bazować na analizie ryzyka, która uwzględnia kontekst funkcjonowania podmiotu.

3. To co wdrożymy w organizacji musi odpowiadać analizie ryzyka i kontekstowi organizacji – inne potrzeby będą mieć MŚP, inne administracja publiczna, a jeszcze inne duże spółki skarbu państwa.

4. Wdrożenie standardu ISO 27001 nie zapewni nam automatycznej zgodności z ustawą.

Oprócz wymagań związanych z budową systemu bezpieczeństwa informacji ustawa wprowadza również dodatkowe wymagania związane z procedurą obsługi i raportowania incydentów, komunikacji z organami właściwymi przez dedykowany system teleinformatyczny, a także obowiązek przeprowadzania regularnych audytów. Niespełnienie obowiązków związanych z przepisami może być podstawą do nałożenia kary finansowej sięgającej nawet 10 mln EUR lub 2% globalnego obrotu dla podmiotów ważnych i 7 mln EUR i 1,4% globalnego obrotu w przypadku podmiotów ważnych. Co ważne, ustawa wprowadza również kary osobiste dla kierownika podmiotu regulowanego (np. Zarządu, dyrektora generalnego) sięgające nawet do 300% miesięcznego wynagrodzenia. To w dobitny sposób pokazuje, że cyberbezpieczeństwo staje się nierozerwalnie połączone z procesami biznesowymi w firmie.

W niniejszym poradniku nie zostaną omówione szczegółowo wszystkie zapisy ustawy zostanie natomiast pokazane jak koordynatorzy polskich klastrów mogą wspierać swoich członków w zapewnieniu zgodności z regulacjami, które wg. szacunków ekspertów będą dotyczyć nawet kilkudziesięciu tysięcy przedsiębiorstw i organizacji w skali całego kraju:

1. **Identyfikacja kontekstu samego klastra:** na podstawie powyższych informacji oraz wskazanych źródeł postaraj się ocenić czy sektor, w którym działają Twoi członkowie może być objęty regulacją.

2. **Szerzenie świadomości:** jeśli kontekst klastra wskazuje na to, że regulacje mogą dotyczyć Twoich członków zacznij od działań informacyjnych. Na podstawie wskazanych źródeł przygotuj wysyłkę mailową dla twoich członków lub zorganizuj spotkanie online/onsite aby przybliżyć swoim członkom kwestię ustawy.

3. **Wesprzyj w samoidentyfikacji:** udostępnij swoim członkom informację o ogólnodostępnych narzędziach wspierających proces samoidentyfikacji. W skrajnym przypadku wystosuj do Ministerstwa Cyfryzacji zapytanie w imieniu członków klastra z danego sektora.

4. **Zorganizuj szkolenie z ekspertem:** rekomendowane jest zorganizowanie szkolenia online/onsite z ekspertem z dziedziny zgodności z regulacjami, który przybliży zainteresowanym członkom Twojego klastra najważniejsze kwestie związane z Ustawą[45]. Specyfika klastra, który działa w określonym sektorze, pomoże zawęzić Ci temat do potrzeb danego sektora. Dzięki temu Twoi członkowie otrzymają szkolenie dostosowane do rodzaju prowadzonej przez nich działalności. Możesz również negocjować stawki grupowe dla członków klastra w modelu „shared consulting".

5. **Śledź na bieżąco komunikaty z Ministerstwa Cyfryzacji i przekazuj je swoim członkom:** na obecnym etapie informacje dotyczyć będą daty podpisania ustawy przez Prezydenta, która wyznaczać będzie datę wejścia w życie przepisów, rozporządzenia wykonawcze Ministra Cyfryzacji, które wspomagają proces implementacji ustawy do porządku krajowego czy inne wytyczne, rekomendacje i interpretacje podawane przez Ministerstwo Cyfryzacji do wiadomości opinii publicznej.

Jak wynika z powyższych informacji przygotowanie do wdrożenia postanowień ustawy w firmie nie jest procesem prostym i łatwym do przeprowadzenia. Dlatego rolą koordynatora jest pilne podnoszenie świadomości, aby informacje o NIS2/UKSC2 dotarły do szerokiego grona odbiorców klastra.

Poniżej zaprezentowana została ekspercka analiza które sektory reprezentowane przez Krajowe Klastry Kluczowe (na podstawie katalogu na grudzień 2025 r.[46]) mogą podlegać pod postanowienia Ustawy:

Tabela 2.4. *Kwalifikacja sektorowa Krajowych Klastrów Kluczowych pod kątem NIS2/UKSC2.*

Klaster	Sektor	Ocena ryzyka podlega NIS2	Firmy najbardziej narażone na kwalifikację
Dolina Lotnicza	Lotnictwo	**Wysokie**	Producenci komponentów, integratorzy, MRO, firmy IT obsługujące lotnictwo
Evoluma (d. Obróbka Metali)	Przemysł, metal	**Średnie**	Dostawcy dla lotnictwa/automotive, duże zakłady produkcyjne
Mazowiecki Klaster ICT	ICT, IT, software	**Wysokie**	Dostawcy chmury, data center, integratorzy, software house'y krytycznych systemów

45 Takie usługi świadczy Polski Klaster Cybebezpieczeństwa #CyberMadeInPoland, autor niniejszej publikacji.

46 „Lista Krajowych Klastrów Kluczowych" [artykuł online]. Dostęp: https://www.gov.pl/web/rozwoj-technologia/lista-k-kk. (24 listopada 2025)

Klaster	Sektor	Ocena ryzyka podlegania NIS2	Firmy najbardziej narażone na kwalifikację
Polski Klaster Budowlany	Budownictwo	**Niskie / Średnie**	Firmy budujące infrastrukturę krytyczną, duże przedsiębiorstwa
NUTRIBIOMED	Żywność, biotech	**Średnie**	Producenci żywności, dodatków, dużych linii produkcyjnych
MedSilesia	Wyroby medyczne	**Wysokie**	Producenci urządzeń medycznych, szczególnie wysokiego ryzyka; duże firmy
Polski Klaster Technologii Kompozytowych	Kompozyty, przemysł	**Średnie**	Dostawcy materiałów dla lotnictwa, automotive, energetyki
Silesia Automotive & Advanced Manufacturing	Automotive	**Wysokie**	Fabryki, producenci komponentów bezpieczeństwa, Tier1, Tier2
Zachodniopomorski Klaster Chemiczny	Chemia	**Wysokie**	Producenci chemikaliów strategicznych, duże zakłady
Polska Grupa Motoryzacyjna	Automotive	**Wysokie**	Producenci części, systemów, duże zakłady produkcyjne
Pomorski Klaster ICT Interizon	ICT	**Wysokie**	Integratorzy, software, data center, operatorzy infrastruktury
Śląski Klaster Lotniczy	Lotnictwo	**Wysokie**	Producenci, komponenty lotnicze, integratorzy, firmy IT
Bydgoski Klaster Przemysłowy Dolina Narzędziowa	Narzędzia, produkcja	**Średnie**	Dostawcy do automotive, AGD, lotnictwa; duże zakłady
Klaster LifeScience Kraków	Life science, biotech, farmacja	**Wysokie**	Firmy medtech, farmacja, R&D kluczowych technologii
Klaster Zrównoważona Infrastruktura	Infrastruktura, energetyka, wod-kan	**Wysokie**	Podmioty wod-kan, energetyczne, infrastruktura publiczna
Klaster Gospodarki Cyrkularnej i Recyklingu	Odpady	**Wysokie**	Przedsiębiorstwa gospodarki odpadami (sektor ważny NIS2)

Klaster	Sektor	Ocena ryzyka podlegania NIS2	Firmy najbardziej narażone na kwalifikację
Klaster Gospodarki Cyrkularnej i Recyklingu	Odpady	**Wysokie**	Przedsiębiorstwa gospodarki odpadami (sektor ważny NIS2)
Klaster Innowacyjnych Technologii w Wytwarzaniu	Produkcja, Industry 4.0	**Średnie**	Dostawcy technologii dla sektorów krytycznych
Śląski Klaster NANO	Nanotechnologie, R&D	**Średnie**	Jednostki badawcze i firmy rozwijające technologie strategiczne

Źródło: Opracowanie własne.

2.3. Akt o odporności cyfrowej (Cyber Resilience Act/CRA)

Nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa i związane z tym obowiązki są obecnie regulacjami, które dotyczą wielu sektorów polskiej gospodarki. w najbliższej perspektywie czasowej. Obecnie Powstaje jednak kolejna europejska regulacja z zakresu cyberbezpieczeństwa – Cyber Resilience Act[47].

CRA to unijne rozporządzenie, które nakłada obowiązkowe wymagania cyberbezpieczeństwa na wszystkie produkty z komponentem cyfrowym – zarówno hardware, jak i software – i obejmuje cały cykl życia produktu: od projektowania przez rozwój i produkcję po wprowadzenie na rynek i utrzymanie. W praktyce rozporządzenie to nakłada na producentów obowiązek wdrożenia zasady „Secure by design", czyli takiego projektowania i wytwarzania produktów cyfrowych, które od samego początku uwzględniają kwestie cyberbezpieczeństwa[48].

Rozporządzenie weszło w życie w grudniu 2024 r., a główne obowiązki zawarte w przepisach zaczną obowiązywać producentów od 11 grudnia 2027 r. Obecnie na rynku polskim i europejskim temat CRA nie jest poruszany z taką częstotliwością jak NIS2/UKSC2. Wynika to z harmonogramu wdrożenia, gdzie obecnie europejski rynek mierzy się z wyzwaniem wdrożenia NIS2 oraz wszystkimi obowiązkami z tego wynikającymi.

Warto również wspomnieć, że CRA jest rozporządzeniem, zatem obowiązywać będzie w całej Unii Europejskiej bez konieczności krajowej implementacji, co w praktyce oznacza jasną datę początku obowiązywania regulacji.

Poniżej znajduje się lista najważniejszych postanowień rozporządzenia:

1. Producent musi zapewnić aktualizację zabezpieczeń.
2. Producent odpowiada za bezpieczne użytkowanie produktu.

47 Cyber Resilience Act. Dostęp: https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act. (24 listopada 2024)

48 Rozporządzenie Parlamentu Europejskiego i Radu UE 2024/2847 z dnia 23 października 2024 r. W sprawie horyzontalnych wymagań w zakresie cyberbezpieczeństwa w odniesieniu do produktów z elementami cyfrowymi oraz w sprawie zmiany rozporządzeń UE nr 168/2013 i UE 2019/1020 i dyrektywy UE 2020/1828 (akt o cyberodporności). Dostęp: https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng. (24 listopada 2025)

3. Produkty zgodne z CRA będą oznaczone znakiem CE, co ułatwi konsumentom identyfikację bezpiecznych urządzeń.
4. Regulacja nie dotyczy niektórych kategorii produktów (np. urządzeń medycznych, samochodów czy samolotów), które już są regulowane.
5. Krytyczne podmioty o wysokim ryzyku (jak np. dostawcy kluczowych urządzeń IoT) przed dopuszczeniem na rynek będą poddawane ocenie przez autoryzowane jednostki[49]. W Polsce będą do podmioty akredytowane przez Polskie Centrum Akredytacji np. NASK lub Instytut Łączności.

Rekomendowane jest śledzenie sprawdzonych źródeł dotyczących Cyber Resilience Act[50]:

- https://cyrima.com/cyber-resilience-act-cra--poradnik-dla-firm/,
- https://kompetencjecyfrowe.gov.pl/aktualnosci/wpis/cyber-resilience-act-cra-i-nowe-standardy-bezpieczenstwa,
- https://cyberpolicy.nask.pl/akt-o-cyberodpornosci-cele-i-zakres-regulacji/,
- https://kompetencjecyfrowe.gov.pl/aktualnosci/wpis/cyber-resilience-act-cra-i-nowe-standardy-bezpieczenstwa.

W przypadku CRA koordynatorzy klastrów mogą zastosować podobny schemat wsparcia swoich członków jak w przypadku innych regulacji:

Uświadamianie – pomoc w identyfikacji – szkolenia dedykowane sektorowi – dystrybucja materiałów informacyjnych

Dodatkowo koordynator klastra może podjąć następujące działania, które ułatwią członkom klastra przygotowanie się do wejścia regulacji w życie i spełnienie ich wymagań:

1. **Analiza wpływu na producentów i dystrybutorów – koordynator może przygotować mapę wpływu CRA na typowe produkty członków klastra (np. software, IoT, usługi chmurowe).**

2. **Wspólne warsztaty „Secure by Design" – koordynator może zorganizować praktyczne warsztaty: modelowanie zagrożeń, bezpieczny SDLC (ang. Software Development Life Cycle, tłum. cykl życia oprogramowania), procesy aktualizacji, minimum wymagań dla dokumentacji technicznej.**

3. **Grupowy dostęp do jednostek notyfikowanych – koordynator może ułatwić kontakt z jednostkami oceniającymi zgodność produktów z nowymi przepisami.**

4. **Szablony dokumentacji wymaganej przez CRA – koordynator może pomóc z przygotowaniu deklaracji zgodności, technicznej dokumentacji bezpieczeństwa, doradzać przy procedurze zgłaszania podatności.**

2.4 Certyfikaty i standardy

Oprócz regulacji prawnych istotną rolę w standaryzacji rynku cyberbezpieczeństwa odgrywają międzynarodowe normy i standardy. W niniejszym rozdziale poradniku zostaną omówione dwa najpopularniejsze związane z rodziną standardów ISO:

1. **ISO 27001** – to międzynarodowa norma dotycząca zarządzania bezpieczeństwem informacji.

49 Rozporządzenie Parlamentu Europejskiego i Radu UE 2024/2847 z dnia 23 października 2024 r. W sprawie horyzontalnych wymagań w zakresie cyberbezpieczeństwa w odniesieniu do produktów z elementami cyfrowymi oraz w sprawie zmiany rozporządzeń UE nr 168/2013 i UE 2019/1020 i dyrektywy UE 2020/1828 (akt o cyberodporności). Dostęp: https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng. (24 listopada 2025)

50 Na czas sporządzenia publikacji, tj. grudzień 2025, są one aktualne.

Zawiera zestaw zasad i procedur wspomagających budowanie systemu zarządzania bezpieczeństwem informacji (SZBI) w organizacji. ISO 27001 określa, jak powinien wyglądać system zarządzania bezpieczeństwem informacji, czyli spójny sposób organizowania polityk, procesów, procedur i zasobów, który zapewnia ochronę danych. Kluczowym elementem jest podejście oparte na ocenie ryzyka, czyli identyfikacja potencjalnych zagrożeń i wdrażanie odpowiednich zabezpieczeń. Ponadto organizacje mogą się certyfikować, potwierdzając w ten sposób, że stosują się do najlepszych praktyk w zakresie ochrony informacji[51].

Spośród najważniejszych obszarów które norma wskazuje jako najważniejsze w procesie zapewnienia bezpieczeństwa informacji organizacji znajdują się m.in.:

- politykę bezpieczeństwa informacji,
- bezpieczeństwo zasobów ludzkich,
- zarządzanie aktywami,
- kontrola dostępu,
- kryptografia,
- bezpieczeństwo fizyczne.

ISO 27001 to międzynarodowy, uznany również w Polsce standard, który na rynku postrzegany jest jako dobry benchmark pokazujący, że podmiot dba o dane swoich klientów i pracowników. Należy jednak oczywiście pamiętać, że samo posiadanie SZBI opartego o tą normę, czy nawet posiadania certyfikatu wdrożenia normy ISO 27001 nie gwarantuje sukcesu. W tym kontekście kluczowe jest zarządzanie systemem oraz jego ciągły monitoring i ulepszanie. Cyberzagrożenia ewoluują w szybkim tempie, dlatego też organizacje muszą dostosowywać i ulepszać swoje procedury, rozwiązania i techniki obrony, a także regularnie szkolić personel z zasad cyberhigieny.

2. **ISO 22301** – to międzynarodowy standard, który ustanawia wymagania dotyczące Systemu Zarządzanie Ciągłością Działania (SZCD). Norma ta pozwala przygotować się na sytuacje kryzysowe, takie jak awarie, katastrofy czy cyberataki. Stosowanie normy ma zapewnić, że firmy będą mogły kontynuować kluczowe działania nawet w trudnych warunkach[52].

   Norma ta w sposób naturalny uzupełnia normę ISO 27001 i powinna być szczególnie ważna dla podmiotów, w których przerwanie ciągłości pracy może doprowadzić do znacznych strat finansowych czy nawet zagrożenia zdrowia i życia ludzkiego (np. fabryki, dostawcy energii, szpitale). W porównaniu do normy ISO 27001 dotyczącej zarządzania bezpieczeństwem informacji, ISO 22301 skupia się w szczególności na planie ciągłości działania (ang. Business Continuity Plan, tłum. plan ciągłości Działania), analizie wpływu na biznes (ang. Business Impact Analysis, tłum. analiza wpływu na biznes), procedurach odtworzenia czy programie ćwiczeń.

Oczywiście nie jest to wyczerpujący katalog norm i standardów używanych w cyberbezpieczeństwa, natomiast dwie powyższe normy są najbardziej popularne. Wdrożenie tych norm w organizacji i stałe doskonalenie funkcjonujących polityk i zabezpieczeń może realnie przyczynić się do podnoszenia poziomu cyberbezpieczeństwa w organizacji.

51 ISO, „ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems – Requirements". Dostęp: https://www.iso.org/standard/27001. (24 listopada 2025)

52 ISO, „Security and resilience — Business continuity management systems — Requirements ISO/IEC 22301:2019". Dostęp: https://www.iso.org/standard/75106.html. (24 listopada 2025)

W kontekście norm i standardów koordynatorzy klastrów powinni być liderami i dostarczyć informację o standardach i normach swoim członkom. Ponadto koordynatorzy mogą, przy współpracy z ekspertami z tej dziedziny, zorganizować szkolenie dla swoich członków w temacie przygotowania się do wdrożenia normy ISO 27001 lub ISO 22301. Dzięki temu członkowie klastra mogą zapoznać się z ich wymaganiami i zdecydować czy wdrożenie danej normy jest zbieżne z ich celami biznesowymi.

2.5. Zarządzanie ryzykiem

Analizując krajobraz regulacji i standardów z obszaru cyberbezpieczeństwa można stwierdzić, że w obecnych czasach jednym z kluczowych procesów łączących akty prawne i standardy jest analiza ryzyka. W jej kontekście klastry pełnią szczególną rolę. Ich członkowie prowadzą działalność w jednym sektorze, więc zarówno potencjalne ryzyka i zagrożenia, jak i szanse z nich wynikające, w dużej mierze mogą być podobne dla wszystkich członków.

Ryzyko jest ogólnie definiowane jako kombinacja prawdopodobieństwa zmaterializowania się zagrożenia oraz konsekwencji skutków tego zdarzenia. Ryzyko można identyfikować na wiele sposób np. poprzez klasyczną analizę SWOT, burzę mózgów, listy kontrole, wywiady czy analizę PESTEL. W analizie ryzyka ważny jest również kontekst danej organizacji oraz wymagania regulacyjne, które mogą ciążyć na danej firmie.

Koordynator klastra może wspierać swoich członków w tym procesie poprzez udostępnienie szablonów i macierzy analizy ryzyka – pozwoli to na standaryzację podejścia do analizy ryzyka wśród członków klastra.

Poniżej zaprezentowano najważniejsze zagrożenia występujące **w polskiej cyberprzestrzeni**, które są **ukierunkowane na polskich przedsiębiorców**. Lista ta została opracowana **na podstawie raportu firmy DAGMA IT „Cyberportret polskiego biznesu"**[53].

1. **Ataki phishingowe:** jest to próba wyłudzenia poufnych informacji przez podszywanie się pod zaufaną instytucję, np. bank, za pomocą fałszywych e-maili lub SMS-ów, które zachęcają do kliknięcia linku lub podania danych[54].

2. **Atak na sieć Wi-Fi:** hakerzy próbują dostać się do bezprzewodowej sieci, np. zgadując hasło lub tworząc fałszywy punkt dostępu, aby przechwycić dane użytkowników lub infekować ich urządzenia[55].

3. **Ataki na aplikacje internetowe:** przestępcy włamują się do stron internetowych lub aplikacji online, by np. ukraść dane, zainfekować je złośliwym oprogramowaniem lub przeprowadzić inne ataki[56].

53 DAGMA Bezpieczeństwo IT, Raport „Cyberportret polskiego biznesu 2025". Dostęp: https://in.eset.pl/cyberportret-polskiego-biznesu. (24 listopada 2025)

54 US National Institute of Standards and Technology, „Phishing". Dostęp: https://www.nist.gov/itl/smallbusinesscyber/guidance-topic/phishing. (24 listopada 2025)

55 Checkpoint, „Wi-Fi Hacking: How It Works, and How to Stay Secure" [artykuł online]. Dostęp: https://www.checkpoint.com/cyber-hub/cyber-security/what-is-hacking/wi-fi-hacking-how-it-works-and-how-to-stay-secure/. (24.11.2025)

56 Akamai, „What Is a Web Application Attack" [artykuł online]. Dostęp: https://www.akamai.com/glossary/what-is-a-web-application-attack. (24.11.2025)

4. **Ataki DDoS:** systemy zasypują serwer ogromną liczbą fałszywych zapytań, czego skutkiem jest niedostępność strony lub usługi dla użytkowników[57].

5. **Spoofing:** podrabianie cyfrowych danych (np. adresów e-mail lub numerów telefonów), by oszukać odbiorcę i zdobyć jego zaufanie lub dane[58].

6. **Malware (np. trojan):** złośliwe oprogramowanie, które projektuje się w taki sposób, by infekować urządzenia, przejmować nad nimi kontrolę, kraść dane lub zakłócać ich działanie[59].

7. **Ataki na urządzenia mobilne:** zagrożenia skierowane na smartfony i tablety, np. malware, które kradnie dane lub blokuje dostęp do urządzenia[60].

8. **Ataki związane z usługami chmurowymi:** atak na serwery i usługi przechowujące dane i programy w chmurze, w celu wykradzenia danych lub zakłócenia działania usług[61].

9. **Socjotechnika:** manipulacja ludźmi, by zdradzili hasła lub wykonali niebezpieczne czynności[62].

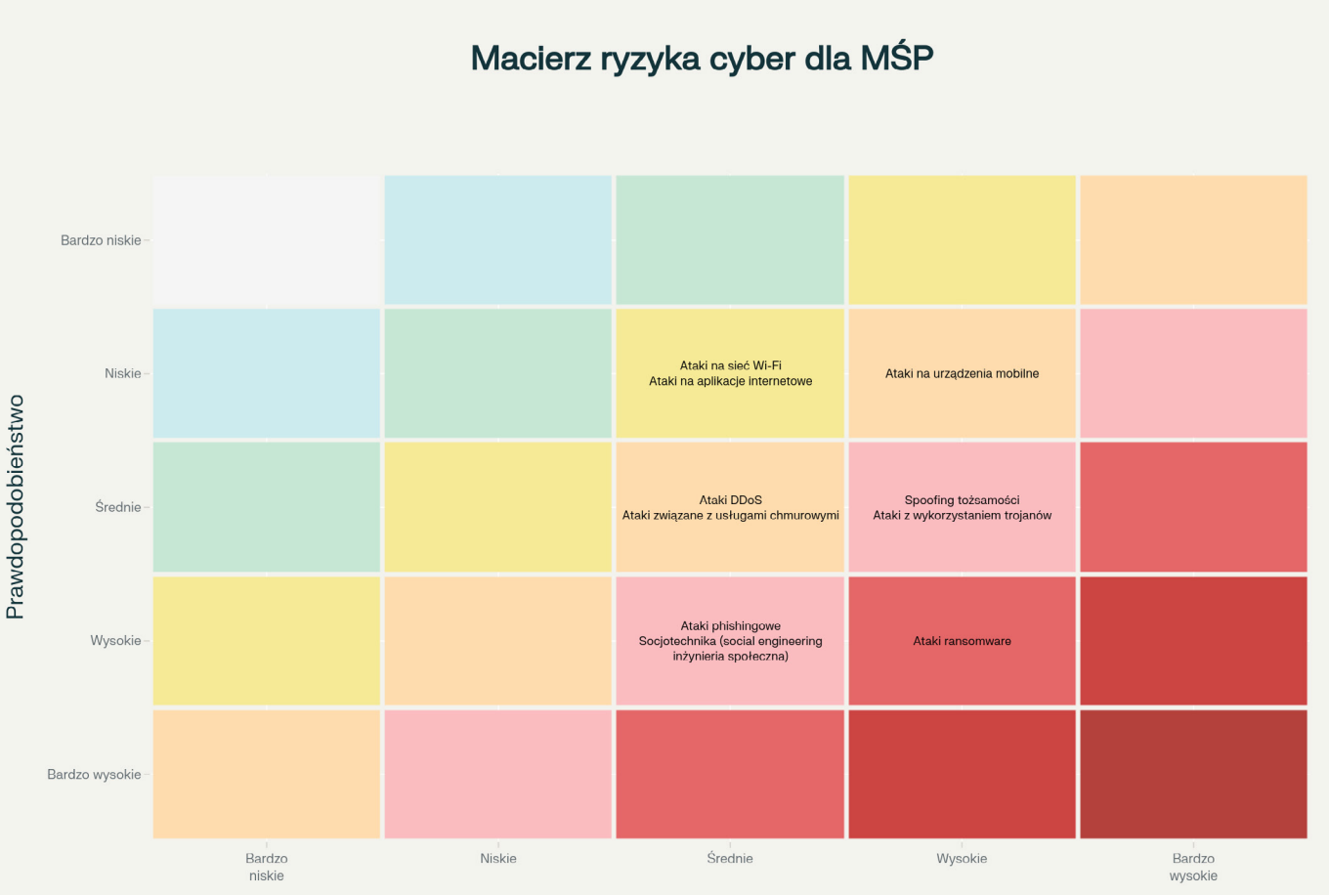
10. **Ransomware:** złośliwe oprogramowanie, które blokuje dostęp do plików i żąda okupu za ich odblokowanie[63].

Jako przykład realnego narzędzia, które może zostać udostępnione członkom klastra, na podstawie powyższej listy została opracowana przykładowa macierz ryzyka dla typowej firmy MŚP w Polsce[64].

Na macierzy znajdują się przykładowe rodzaje zagrożeń, umieszczone w osiach odpowiadających skutkom i prawdopodobieństwom. W zależności od oceny prawdopodobieństwa zmaterializowania się ryzyka oraz skutków zaistnienia takiego ryzyka, dany rodzaj zagrożeń został umieszczony w odpowiednim miejscu macierzy. Przykładowo: jeden z najbardziej szkodliwych rodzajów ataków tj. ransomware został oceniony jako ryzyko o dużym prawdopodobieństwie jego zmaterializowania ze względu na łatwość jego dostarczenia do systemów ofiary. Jednocześnie skutki zostały ocenione na wysokie, gdyż ten rodzaj ataku paraliżuje działalność podmiotu i w skrajnym przypadku może doprowadzić do upadku danego podmiotu.

57 Microsoft, „Co to jest atak DDos?" [artykuł online]. Dostęp: https://www.microsoft.com/pl-pl/security/business/security-101/what-is-a-ddos-attack. (24.11.2025)
58 Ministerstwo Cyfryzacji, „Czym jest spoofing? Jak go rozpoznać i nie dać się nabrać?" [artykuł online]. Dostęp: https://www.gov.pl/web/cyfryzacja/czym-jest-spoofing--jak-go-rozpoznac-i-nie-dac-sie-nabrac. (24.11.2025)
59 Ministerstwo Cyfryzacji, „Łagodzenie skutków ataków szkodliwego oprogramowania" [artykuł online]. Dostęp: https://www.gov.pl/web/baza-wiedzy/lagodzenie-skutkow-atakow-szkodliwego-oprogramowania. (24.11.2025)
60 F-secure, „Mobile Malware" [artykuł online]. Dostęp: https://www.f-secure.com/en/articles/mobile-malware. (24.11.2025)
61 Microsoft, „Wprowadzenie do bezpieczeństwa w chmurze" [artykuł online]. Dostęp: https://www.microsoft.com/pl-pl/security/business/security-101/what-is-cloud-security. (24.11.2025)
62 Trendmicro, „Czym jest social engineering?" [artykuł online]. Dostęp: https://www.trendmicro.com/pl_pl/what-is/social-engineering.html. (24.11.2025)
63 Ministerstwo Cyfryzacji, „Ransomware – jedno z najpoważniejszych zagrożeń w cyberprzestrzeni" [artykuł online]. Dostęp: https://www.gov.pl/web/baza-wiedzy/ransomware--jedno-z-najpowazniejszych-zagrozen-w-cyberprzestrzeni. (24 listopada 2025)
64 DAGMA Bezpieczeństwo IT, Raport „Cyberportret polskiego biznesu 2025", Dostęp: https://in.eset.pl/cyberportret-polskiego-biznesu. (24 listopada 2025)

Tabela 2.5 *Przykładowa macierz ryzyka cyberbezpieczeństwa dla MŚP.*



Źródło: Opracowanie własne.

Dodatkowe działania, które może podjąć koordynator klastra:

1. **Opracowanie wspólnego profilu zagrożeń, dostosowanego do branży reprezentowanej przez klaster.**
2. **Benchmarking dojrzałości cyberbezpieczeństwa – prosta skala oceny dojrzałości bezpieczeństwa, którą członkowie mogą stosować do samooceny i porównania z innymi podmiotami członkowskimiw klastrze.**

Przykłady powyższych narzędzi zostały zaprezentowane w rozdziale 5.

2.6. Ubezpieczenia od ryzyk cybernetycznych

Kolejnym tematem z obszaru cyberbezpieczeństwa i prawa, któremu warto poświęcić uwagę, są ubezpieczenia od ryzyk cybernetycznych.

Ubezpieczenia tego typu nie są w Polsce tak popularne jak w krajach anglosaskich, ale ostatnimi laty można zauważyć wzrost zainteresowania tym tematem. Wynika to z głównej mierze z rosnącej skali zagrożeń cyfrowych oraz wejściem w życie regulacji przewidujących kary finansowe (w tym możliwość nałożenia ich bezpośrednio na członków zarządów.)

Szkody potencjalnie objęte ubezpieczeniem mogą dotyczyć bezpośrednio strat wyrządzonych ubezpieczonemu podmiotowi (m.in. przerwa w działaniu systemów, utrata danych), jak i strat wyrządzonych osobom trzecim (m.in. wyciek danych osobowych, zainfekowanie systemów informatycznych i komputerów podmiotów trzecich). Zadaniem ubezpieczenia jest także zapewnienie ubezpieczonemu pomocy ekspertów, których celem jest przywrócenie systemów informatycznych i urządzeń do stanu przed awarią (atakiem), a także sfinansowanie pomocy prawnej w momencie, gdy osoby trzecie (firmy, osoby fizyczne, organy państwa) wysuwają roszczenia o odszkodowanie lub zadośćuczynienie[65].

Poniższa tabela prezentuje potencjalne rodzaje wsparcia, jakie koordynator klastra może udostępnić swoim członkom w obszarze ubezpieczeń od zagrożeń cybernetycznych.

Tabela 2.6 *Obszary wsparcia członków klastra w obszarze ubezpieczeń cybernetycznych*

Obszar	Działania koordynatora klastra	Wartość dla członków
Dostęp do informacji o rynku polis cyber	Przygotowanie porównania ofert ubezpieczycieli (zakres, wyłączenia, wymagania, limity odpowiedzialności).	Członkowie unikają błędnych decyzji i otrzymują rzetelny obraz dostępnych produktów.
Minimalne wymagania ubezpieczycieli	Opracowanie listy sprawdzającej zabezpieczeń wymaganych do zawarcia polisy (MFA, backupy, patching, monitoring).	Podmioty wiedzą, co muszą wdrożyć, aby uzyskać polisę lub poprawić zakres ochrony.
Negocjacje grupowe	Organizacja wspólnych negocjacji z ubezpieczycielami – model „polisy zbiorczej" lub preferencyjnych stawek.	Niższe składki, szerszy zakres ochrony, lepsze warunki zapisane w OWU.
Edukacja zarządów i działów prawnych	Szkolenia i krótkie materiały wyjaśniające różnice między typami polis.	Zarządy rozumieją ryzyko, odpowiedzialność osobistą oraz wiedzą, jak dobrać właściwą ochronę.
Wsparcie przy likwidacji szkód	Udostępnienie listy firm obsługujących incydenty i pracujących z ubezpieczycielami.	Skrócenie czasu reakcji, mniejsze straty i mniej formalnych błędów podczas składania roszczenia.
Weryfikacja OWU pod kątem realnych potrzeb członków	Analiza najczęściej spotykanych wyłączeń (błędy pracowników, brak aktualizacji, brak MFA).	Członkowie unikają polis, które „nie działają" w praktyce.
Ćwiczenia i testy wymagane przez ubezpieczycieli	Organizacja prostych „Table-Top Exercises" i dokumentowanie ich w formie raportu.	Raport podnosi wiarygodność firm i obniża koszt polisy.
Standaryzacja zgłoszeń incydentów	Stworzenie wzoru procedury zgłaszania incydentu zgodnej z wymaganiami polis cyber.	Firmy unikają odrzucenia roszczenia przez błędy proceduralne.

65 Findia, „Ubezpieczenia cyber". Dostęp: https://findia.pl/ubezpieczenie-cyber?gad_source=1&gad_campaignid=9889458441&gbraid=0AAAADb46qf7rIDzHtHg_OnW_6gv6mtIH&gclid=Cj0KCQiArOvIBhDLARIsAPwJXObfQ-GSSnMP7YRZNqPM8K7eM58s_OD7G1y_HtDlfoZJpL6MLWZex8jkaAo_GEALw_wcB. (24 listopada 2025)

Rozdział 3

Rola koordynatora klastra w budowaniu cyberodporności członków klastra

Poniższy rozdział przedstawia kluczową rolę koordynatora klastra w budowaniu cyberodporności podmiotów członkowskich. Omawia praktyczne metody diagnozy poziomu bezpieczeństwa, zarówno szybkie i skalowalne ankiety, jak i bardziej wymagające podejście proaktywne oparte na obserwacji. Wskazuje także, jak poprzez odpowiednią komunikację, edukację oraz tworzenie sieci ekspertów, dostawców i instytucji publicznych koordynator może wzmacniać świadomość oraz zdolność reagowania podmiotów na cyberzagrożenia. Rozdział przedstawia także koncepcję utworzenia ISAC klastra, którego celem jest wymiana informacji o incydentach i zagrożeniach wśród podmiotów członkowskich.

3.1 Praktyczne podejście do diagnozy cyberodporności wśród członków klastra

Skuteczne wspieranie cyberodporności podmiotów zrzeszonych w klastrze zaczyna się od rzetelnego rozpoznania ich potrzeb, poziomu dojrzałości, możliwości danej organizacji na wprowadzenie poszczególnych rozwiązań oraz identyfikację luk technologicznych, kompetencyjnych czy organizacyjnych. Koordynator klastra może pełnić rolę organizatora, moderatora oraz dostawcy narzędzi umożliwiających sprawną diagnozę cyberodporności organizacji. W tym celu koordynator klastra może skorzystać z poniższych narzędzi:

- diagnoza oparta na informacji od członków klastra – ankietowanie członków klastra i innych podmiotów,
- proaktywna diagnoza prowadzona przez koordynatora klastra jako obserwatora.

3.1.1. Ankietowanie członków klastra

Ankiety są jednym z najpopularniejszych narzędzi diagnozy cyberodporności, szczególnie wśród małych i średnich firm, które nie zawsze posiadają pracowników odpowiedzialnych za cyberbezpieczeństwo. Dzięki ankietom osoby zarządzające mogą uzyskać informację, jakie dobre praktyki i rozwiązania warto wprowadzić w firmie. Badania tego typu mają jednak istotne ograniczenia, które wpływają na jakość wyników i ich użyteczność dla podmiotu członkowskiego. Wady i zalety tego narzędzia przedstawia poniższa tabela:

Tabela 3.1 *Zalety i wady ankietowania podmiotów członkowskich w celu badania ich cyberodporności.*

Zalety ankietowania podmiotów	Wady ankietowania podmiotów
Szybkie i skalowalne pozyskanie informacji – koordynator klastra może dotrzeć do dużej liczby podmiotów jednocześnie, bez konieczności angażowania ekspertów.	**Subiektywność odpowiedzi** – podmioty często nie mają wiedzy, aby trafnie ocenić własny poziom bezpieczeństwa („nie wiemy, czego nie wiemy”). Prowadzi to do błędów typu zawyżania poczucia bezpieczeństwa, niedostrzeganie kluczowych luk, czy braku świadomości istnienia procesów, o które pyta ankieta.
Niskie koszty – przygotowanie ankiety i jej dystrybucja w formie online jest tanie oraz możliwe do realizacji w ramach codziennych zadań koordynatora klastra.	**Deklaratywność zamiast realnej diagnozy** – ankieta nie pokazuje: • jak podmiot faktycznie pracuje, • jak wygląda konfiguracja systemów, • jakie są zachowania pracowników, • jakie incydenty miały miejsce.

Zalety ankietowania podmiotów	Wady ankietowania podmiotów
Minimalny poziom ingerencji w działania członków – firmy samodzielnie wypełniają ankietę w dogodnym czasie, bez konieczności udostępniania infrastruktury, dokumentacji czy ustalania spotkań z pracownikami.	**Ryzyko zaniżania problemów** – członkowie mogą obawiać się, że negatywne odpowiedzi wpłyną na ich reputację w klastrze, nawet jeśli ankieta jest anonimowa.
Możliwość wstępnego zobrazowania świadomości członków – ankiety pokazują, jak członkowie same postrzegają swoje kompetencje, problemy i potrzeby, co może pomóc w planowaniu dalszych działań w budowaniu cyberodporności.	**Brak natychmiastowej wartości praktycznej** – ankieta sama w sobie nie poprawia cyberodporności organizacji. Podmiot często zostaje tylko z ogólnym „poczuciem, że coś trzeba zrobić", ale bez pomysłów i wiedzy, jakie działania może podjąć.
Porównywalność danych – ujednolicony zestaw pytań pozwala tworzyć raporty zbiorcze i porównywać podmioty zrzeszone w klastrze. Raporty mogą być wykorzystane na dalszym etapie do wymiany wiedzy i tworzenia dobrych praktyk wewnątrz klastra.	**Mała motywacja do wypełniania** – wielu przedsiębiorców traktuje ankiety jako biurokrację czy stratę czasu, co skutkuje niskim zaangażowaniem w jej wypełnienie, a zatem małą reprezentatywnością wyników.

Źródło: Opracowanie własne.

3.1.2 Proaktywne podejście obserwacyjne koordynatora klastra

Proaktywne podejście obserwacyjne koordynatora klastra polega na stałym monitorowaniu sytuacji cyberbezpieczeństwa w podmiotach członkowskich poprzez bezpośredni kontakt, analizę sygnałów z otoczenia i bieżące identyfikowanie potencjalnych problemów zanim przerodzą się one w incydenty. Nie opiera się ono wyłącznie na deklaracjach przedsiębiorstw i innych członków, lecz na praktycznej zewnętrznej obserwacji ich procesów, zachowań pracowników, komunikacji czy wykorzystywanych technologii. W ramach działań proaktywnych koordynator klastra może:

- podczas rozmowy z podmiotami zadawać pytania o aspekty związane z cyberbezpieczeństwem, zbierać sygnały ostrzegawcze i analizować nietypowe zdarzenia,
- obserwować zmiany w praktykach operacyjnych podmiotów i reagować na pojawiające się ryzyka,
- wspierać podmioty w identyfikacji luk poprzez informowanie ich o potencjalnych zagrożeniach,
- monitorować trendy zagrożeń w branży i przekładać je na rekomendacje dla członków klastra,
- wspierać członków przy potencjalnych wyborach wdrażanych technologii oraz ich konfiguracji w celu skutecznego wykorzystania,
- prowadzić działania edukacyjne i doradcze w odpowiedzi na zaobserwowane problemy,
- inicjować szybkie interwencje, gdy pojawią się sygnały dotyczące potencjalnych incydentów.

Podejście proaktywne pozwala koordynatorowi na lepsze wspieranie podmiotów członkowskich w ramach diagnozy ich cyberodporności poprzez bieżące śledzenie potencjalnych zagrożeń oraz zbieranie informacji bezpośrednio od członków klastra. Jest ono jednocześnie dużym obciążeniem kosztowym i osobowym dla koordynatora klastra, ze względu na konieczność posiadania wyspecjalizowanej kadry. Tak samo jak diagnoza

poprzez ankietowanie, proaktywne podejście niesie za sobą zarówno wiele zalet, jak i wad, które przedstawia poniższa tabela.

jako szybkie, wstępne narzędzie do zrozumienia poziomu świadomości i jako narzędzie edukacji członków klastra. Podejście proaktywne jest

Tabela 3.2 *Zalety i wady proaktywnego podejścia w badaniu cyberodporności podmiotów członkowskich.*

Zalety proaktywnego podejścia	Wady proaktywnego podejścia
Diagnoza oparta na faktach, nie deklaracjach – koordynator widzi realne praktyki, a nie ich deklaratywny opis. Pozwala to wychwycić m.in. błędne nawyki, potencjalne luki w procedurach czy niektóre problemy konfiguracyjne.	**Konieczność większej ingerencji w działania podmiotów członkowskich** – w niektórych przypadkach podejście proaktywne może wymagać większej ingerencji w organizację poprzez pokazanie sposobu jej pracy czy rozmowy z pracownikami w celu uzyskania lepszego oglądu działań.
Pozwala rozpoznać zagrożenia dotyczące wielu podmiotów – koordynator często widzi powiązania, których pojedyncze firmy nie dostrzegają: • problemy czy zagrożenia związane z wykorzystywaniem rozwiązań danego dostawcy, • kampanie cyberprzestępców nakierowane na daną branżę, • luki w specjalistycznym oprogramowaniu dla podmiotów członkowskich.	**Wymaganie kompetencji od koordynatora** – podejście proaktywne nie zadziała bez wiedzy specjalistycznej pracowników koordynatora klastra, doświadczenia w analizie procesów czy posiadania kompetencji technicznych.
Zwiększa skuteczność rekomendacji – rekomendacje pochodzą z realnego kontekstu, a nie z szablonów – przez co są bardziej adekwatne i chętniej wdrażane.	**Członkowie klastra mogą obawiać się:** • ujawnienia swoich słabych stron, • ingerencji w ich procesy, • naruszenia poufności.
Umożliwia tworzenie wspólnych rozwiązań – dzięki obserwacji koordynator może identyfikować wspólne potrzeby, inicjować projekty grupowe dla członków klastra (np. szkolenia, wspólny SOC (Security Operation Center), usługi prawne), czy standaryzować praktyki bezpieczeństwa wśród członków klastra.	**Trudniejsza skalowalność** – obserwacja wymaga czasu, trudniej objąć nią duże klastry (np. 100+ członków) bez podziału na priorytety.
Buduje zaufanie i relacje – regularna obecność koordynatora zwiększa otwartość członków w dzieleniu się problemami i zgłaszaniu incydentów.	**Ryzyko przeniesione na koordynatora** – ze względu na większe zaangażowanie w budowanie cyberodporności podmiotów członkowskich, mogą one stracić zaufanie, jeśli w czasie incydentu uznają, że koordynator klastra nie pomógł im wystarczająco.

Źródło: Opracowanie własne.

3.1.3 Porównanie narzędzi

Ze strony koordynatora klastra obie metody diagnozy cyberodporności posiadają zarówno wady, jak i zalety w ich realizacji. Ankiety sprawdzą się

znacznie skuteczniejsze w wykrywaniu faktycznych luk i zagrożeń, ale wymaga przygotowania i znacznie większych nakładów finansowych ze strony koordynatora. Próba połączenia obu podejść wraz z uwzględnieniem charakteru działal-

Tabela 3.3 *Podsumowanie porównawcze narzędzi diagnozy cyberodporności.*

Kryterium	Ankiety	Podejście obserwacyjne
Jakość danych	średnia, deklaratywna	wysoka, oparta na faktach
Koszty	niskie	wysokie
Zaangażowanie członków	minimalne	umiarkowane
Zaangażowanie klastra	niskie	wysokie
Potrzebna wiedza	niewielka	wyspecjalizowana
Skalowalność	wysoka	ograniczona
Wpływ na procesy w podmiotach członkowskich	niewielki	znaczący
Wartość diagnostyczna	ograniczona	bardzo wysoka
Budowa relacji	niska	wysoka
Identyfikacja zagrożeń międzyfirmowych	minimalna	wysoka

Źródło: Opracowanie własne.

ności danego klastra może przynieść najwięcej wartości dodanej dla podmiotów członkowskich.

3.2 Budowanie świadomości na temat cyberodporności wśród członków klastra

Świadomość cyberbezpieczeństwa wśród podmiotów członkowskich klastra jest podstawą skutecznej ochrony przed zagrożeniami. Nawet najlepsze procedury i technologie nie spełnią swojej roli, jeśli pracownicy i zarządy nie rozumieją ryzyk ani nie wiedzą, jak reagować w kryzysowych sytuacjach. Rolą koordynatora klastra może być prowadzenie jasnej i zrozumiałej komunikacji o cyberbezpieczeństwie i wprowadzenie mechanizmów zwiększających zaangażowanie członków.

W ramach dobrych praktyk koordynator klastra może regularnie komunikować się z podmiotami członkowskim np. poprzez wysyłanie informacji w formie newslettera lub w inny sposób wypracowany w klastrze. Pozwala to podmiotom członkowskim wyrobić nawyk systematycznego otrzymywania informacji i refleksji nad wiadomościami dotyczącymi cyberodporności.

Skuteczna komunikacja powinna spełniać kilka podstawowych zasad:

- unikać nadmiaru terminologii technicznej,
- skupiać się na tym, co jest istotne dla decydentów i pracowników (np. ryzyka biznesowe, aktualne regulacje prawne, którymi mogą zostać objęte podmioty członkowskie itp.),
- przedstawiać informacje w formie list sprawdzających, infografik, krótkich poradników, pozwalając na szybkie, a jednocześnie maksymalnie szerokie rozpoznanie tematu,

- pokazywać realne przypadki incydentów w branży lub w innych firmach – tzw. case study są jednym z najlepszych metod pokazywania sposobów reakcji oraz konsekwencji cyberataku,
- realizować cykliczne warsztaty, webinary i spotkania robocze w celu pogłębienia tematyki,
- dobrą praktyką jest także tworzenie zamkniętych grup w komunikatorach lub na platformach klastra, aby szybko dzielić się alertami, informacjami o zagrożeniach i dobrych praktykach.

Przykładowe tematy kampanii edukacyjnych koordynatora klastra mogą obejmować:

1. **Podstawy cyberbezpieczeństwa** – zasady tworzenia mocnych haseł, uwierzytelnianie wieloskładnikowe, podstawowe aktualizacje oprogramowania, uświadamianie w temacie rodzajów zagrożeń np. phishingu.

2. **Bezpieczeństwo danych i informacji** – tworzenie backup i przywracanie danych, przechowywanie dokumentów w chmurze, ochrona danych klientów i pracowników, legislacja w praktyce.

3. **Zarządzanie incydentami** – jak rozpoznać incydent, kto w podmiocie odpowiada za reakcję, podstawowe procedury na wypadek ataku ransomware lub wycieku danych.

4. **Zagrożenia technologiczne i trendy** – malware, ransomware, ataki na systemy OT/IoT, najnowsze techniki phishingowe, zagrożenia wynikające z korzystania z dostawców IT.

5. **Cyberhigiena i codzienne praktyki** – bezpieczne korzystanie z e-maili i komunikatorów, ograniczenie ryzyka w pracy zdalnej, zasady korzystania z nośników danych.

Jeśli koordynator klastra nie posiada odpowiednich kompetencji do przygotowania potrzebnych materiałów, warto nawiązać współpracę z lokalnymi firmami zajmującymi się cyberbezpieczeństwem. Współpraca z lokalnymi partnerami umożliwi szybsze organizowanie spotkań, takich jak konferencje czy warsztaty.

3.3 Budowanie sieci wsparcia cyberbezpieczeństwa w podmiotach członkowskich

Koordynator klastra powinien pełnić rolę centralnego punktu łączącego podmioty członkowskie z ekspertami oraz dostawcami produktów i usług z zakresu cyberbezpieczeństwa. Działanie to powinno opierać się na stworzeniu szerokiej sieci zaufanych ekspertów, dostawców i instytucji publicznych. W kontekście cyberbezpieczeństwa zadaniem koordynatora jest nie tylko identyfikacja potrzeb członków, ale również zapewnienie dostępu do odpowiednich ekspertów, technologii i instytucji, które mogą wspierać ich w podnoszeniu poziomu cyberodporności oraz reakcji na incydenty.

Systematyczne budowanie sieci kontaktów powinno być jednym z kluczowych zadań koordynatora klastra, który następnie udostępnia ją podmiotom członkowskim. Najskuteczniejszym sposobem rozwijania takiej sieci są spotkania bezpośrednie – warsztaty, konferencje, seminaria czy śniadania biznesowe. Ich forma sprzyja nawiązywaniu trwalszych, bardziej zaufanych relacji, które rzadko powstają jedynie poprzez kontakt mailowy.

Równocześnie niezwykle ważne jest posiadanie jednej, spójnej bazy informacji o współpracujących organizacjach, ich specjalizacjach i obszarach działania. Taka centralna lista ułatwia podmiotom członkowskim szybkie sprawdzenie dostępnych możliwości i efektywne korzystanie z zasobów sieci kontaktów rozwijanych przez koordynatora. Dzięki aktywnej roli koordynatora podmioty uzyskują dostęp do wiedzy, technologii oraz relacji,

Tabela 3.4 *Schematy nawiązywania relacji oraz realizacji współpracy z ekspertami, dostawcami produktów i usług oraz podmiotami administracji publicznej.*

Koordynator klastra		
Eksperci	**Dostawcy produktów i usług**	**Instytucje publiczne**
Nawiązywanie relacji z ekspertami pozwala na przekazywanie aktualnej i rzetelnej wiedzy członkom klastra na lepszych warunkach. Często ekspertami mogą zostać przedstawiciele członków, którzy posiadają stosowne doświadczenie lub rozbudowane działy cyberbezpieczeństwa.	Nawiązywanie relacji z dostawcami produktów i usług pozwala na przekazywanie aktualnej wiedzy członkom klastra ze strony podmiotów działających w branży. Dodatkowym atutem może być możliwość skorzystania z dedykowanej oferty dla wszystkich członków na rozwiązania i usługi danej organizacji partnerskiej.	Nawiązywanie relacji z podmiotami administracji publicznej w zakresie cyberbezpieczeństwa jest kluczowe pod kątem przekazywania istotnych informacji w dół drabiny informacyjnej. Podmioty takie jak Ministerstwo Cyfryzacji, NASK-PIB, CERT Polska czy sektorowe CSIRTy prowadzą szereg działań informacyjnych, które mogą okazać się znaczące dla członków klastra.
Rodzaje poszukiwanej wiedzy wśród wskazanych podmiotów:		
Wśród ekspertów powinny znaleźć się osoby z doświadczeniem w: • audytach i ocenie cyberodporności, • testach penetracyjnych i weryfikacji bezpieczeństwa systemów, • zarządzania incydentami i reagowania na ataki, • zgodności z regulacjami prawnymi (np. RODO, NIS2), • edukacji i szkoleń pracowników.	Wśród dostawców produktów i usług powinny znaleźć się organizacje z ofertą: • systemów zabezpieczeń IT i OT, • rozwiązań chmurowych, backupowych, antywirusowych, MDM, MFA, EDR, • systemy monitorowania sieci, SIEM, SOC, • platformy edukacyjne i szkoleniowe dla pracowników, • organizacje realizujące audyty, testy penetracyjne oraz sprawdzające zgodności z regulacjami.	Wśród instytucji publicznych powinny znaleźć się organizacje realizujące takie działania jak: • wsparcie przy reakcji na incydenty – CERT Polska, CSIRT sektorowy pasujący do danej branży lub CSIRT MON, GOV, NASK, • instytucje udzielające grantów i dofinansowań na poprawę cyberbezpieczeństwa jak PARP, ARP, MRiT, NCC-PL, CPPC, • tworzące sieci kontaktów branżowych i inicjatyw wspólnych dla MŚP – klastry, organizacje branżowe, izby gospodarcze itp.
Możliwe formy współpracy z poszczególnymi organizacjami:		
• organizacja webinarów, szkoleń, warsztatów lub spotkań doradczych dla członków klastra • tworzenie grup doradczych lub konsultacyjnych dostępnych dla członków klastra, • koordynację wspólnych działań edukacyjnych dla pracowników podmiotów członkowskich,	• negocjowanie preferencyjnych warunków współpracy, licencji lub wsparcia technicznego, • dzielenie się doświadczeniami dostawców produktów i usług z innymi członkami klastra, • inicjowanie pilotaży rozwiązań w wybranych firmach, • wspólne testowanie narzędzi dla całego klastra.	• utworzenie kanałów komunikacji w przypadku incydentów z odpowiednimi instytucjami, • informowanie członków klastra o aktualnych programach wsparcia, • inicjowanie wspólnych wniosków grantowych dla grupy, podmiotów z klastra, • ułatwianie kontaktów i pośrednictwo w procesie aplikacyjnym,

Możliwe formy współpracy z poszczególnymi organizacjami:		
• w przypadku wystąpienia incydentu możliwość szybkiego połączenia stosownych ekspertów i poszkodowanej firmy.		• monitorowanie przepisów i przekazywanie ich w formie przystępnych komunikatów.

Źródło: Opracowanie własne.

których samodzielne wypracowanie wymagałoby znacznie więcej czasu i zasobów. W rezultacie cały klaster staje się lepiej przygotowany na wyzwania i zagrożenia w obszarze cyberbezpieczeństwa.

3.4 Wymiana informacji o zagrożeniach – ISAC klastrowy

Efektywne zwiększanie cyberodporności klastra wymaga nie tylko diagnozy i edukacji, ale także szybkiego dostępu do informacji o zagrożeniach i incydentach. W tym celu koordynator może utworzyć ISAC (ang. Information Sharing and Analysis Center, tłum. Centrum Udostępniania i Analizowania informacji) klastrowy, który umożliwia członkom klastra współdzielenie wiedzy o cyberzagrożeniach w bezpieczny i zorganizowany sposób.

ISAC, czyli centrum wymiany i analizy informacji, jest to sektorowe partnerstwo publiczno-prywatne (PPP), non-profit, którego celem jest gromadzenie, analiza i bezpieczna wymiana informacji o zagrożeniach cybernetycznych między instytucjami publicznymi i prywatnymi[66]. W kontekście klastra, ISAC może pełnić rolę:

- centralnego punktu gromadzenia i dystrybucji informacji o zagrożeniach,
- platformy współpracy w zakresie reagowania na incydenty,
- narzędzia budującego świadomość o ryzykach branżowych i technologicznych,
- sposobu wspólnego podnoszenia poziomu cyberodporności całej grupy członków klastra.

Koordynator klastra w celu sprawnego działania ISAC powinien pozyskiwać informacje z takich źródeł jak:

- raporty krajowych i międzynarodowych zespołów CERT (ang. Computer Emergency Response Team, tłum. zespół monitorujący, analizujący i reagujący na incydenty cyberbezpieczeństwa),
- raporty sektorowych zespołów CSIRT (ang. Computer Security Incident Response Team, tłum. zespół reagujący na incydenty bezpieczeństwa w organizacji),
- biuletyny informacyjne oraz rekomendacje publikowane przez Ministerstwo Cyfryzacji,
- informacje od dostawców technologii i producentów oprogramowania,
- raporty branżowe,
- media branżowe i portale dotyczące cyberbezpieczeństwa,
- incydenty i sygnały od członków klastra,
- alerty regulatorów i instytucji nadzorczych.

Zebrane dane powinny być następnie dostosowywane do poziomu i potrzeb członków klastra, aby były zrozumiałe i możliwe do szybkiego zastosowania.

66 Wrzosek, Magdalena, NASK, (2019) „ISAC, czyli centra wymiany i analizy informacji" [artykuł online]. Dostęp: https://cyberpolicy.nask.pl/isac-centra-wymiany-analizy-informacji/. (17 listopada 2025)

Rysunek 3.1 *Schemat roli koordynatora klastra w ISAC klastrowym.*

Facylitacja wymiany informacji

Tworzenie bezpiecznych kanałów komunikacji (np. zamknięte platformy online, dedykowane grupy, newslettery alertowe) oraz zachęcanie członków klastra do raportowania incydentów i podejrzanych działań.

Analiza i weryfikacja informacji

Selekcja, weryfikacja i klasyfikacja otrzymanych danych, pozwalająca na wychwycenie dezinformacji oraz unikanie przesyłania nieistotnych informacji. Na podstawie zebranych informacji koordynator przygotowuje rekomendacje i wskazówki praktyczne dla podmiotów członkowskich.

Koordynacja reakcji na zagrożenia

Wspieranie podmiotów w przygotowaniu reakcji na wykryte zagrożenia lub przekazanie kontaktu do odpowiedniego eksperta lub dostawcy produktów/usług z sieci kontaktów koordynatora klastra.

Budowanie zaufania i kultury współpracy

Celem ISAC jest stworzenie ekosystemu zaufania wśród podmiotów członkowskich do wymiany istotnych informacji dla ich cyberodporności. Zapewnienie poufności informacji i określenie zasady wymiany danych pomiędzy firmami w ramach ISAC. Ponadto promowanie dzieleniem się doświadczeniami bez obawy przed utratą reputacji.

Źródło: Opracowanie własne.

ISAC klastra może być skutecznym narzędziem koordynatora klastra do stworzenia zbiorowej prewencyjnej ochrony przed cyberzagrożeniami. Dzięki centralnej wymianie informacji, analizie incydentów i rekomendacjom dla podmiotów członkowskich pozwala on na szybką reakcję na pojawiające się zagrożenia, budowanie zaufania i współpracy wśród członków klastra. W efekcie prowadzi to do zwiększenia odporności całego ekosystemu klastra. W celu sprawnego utworzenia własnego ISAC można wzorować się na aktualnie działających centrach takich jak:

- ISAC GIG – https://isac.gig.eu/,
- ISAC Kolej – https://isac-kolej.pl/.

Tabela 3.5 *Zalety oraz wady ISAC klastra.*

Zalety ISAC	Wady ISAC
Umożliwia szybką wymianę informacji o zagrożeniach i incydentach.	Istnieje ryzyko nieumyślnego ujawnienia wrażliwych danych.
Podnosi świadomość bezpieczeństwa wśród podmiotów członkowskich.	Różny poziom zaangażowania może ograniczać skuteczność współpracy.
Wspiera współpracę i budowanie zaufania w klastrze.	Wymaga zasobów organizacyjnych i finansowych.
Pozwala szybciej reagować na zagrożenia.	Wymaga wypracowania wysokiego poziomu zaufania między podmiotami członkowskimi.

Źródło: Opracowanie własne.

Rozdział 4

Cyberbezpieczeństwo koordynatora klastra

W rozmowie o cyberbezpieczeństwie trzeba pamiętać o bezpieczeństwie samego koordynatora klastra. Koordynator zarządza dużą liczbą danych i korzysta z zaufania członków klastra. Dlatego powinien dbać również o własne bezpieczeństwo cyfrowe.

4.1 Główne zagrożenia cyberbezpieczeństwa w kontekście koordynatora klastra

Specyfika działalności koordynatora klastra wpływa na rodzaje zagrożeń, na które może być narażony. Atakujący może być zainteresowany przede wszystkim uzyskaniem danych członków klastra, jakie przechowuje koordynator, skompromitowaniem strony internetowej lub podszyciem się pod komunikację mailową w celu wyłudzenia informacji. Atrakcyjnym celem hakerów może być także wspólny dorobek B+R wytworzony przez klaster.

Znamy już rodzaje zagrożeń cyberbezpieczeństwa, które szczegółowo omówiono w rozdziale 1. Poniżej przedstawiamy konkretne przykłady, pokazujące jak dane zagrożenia może zostać wykorzystane w kontekście klastra oraz jakie konsekwencje może nieść dla członków.

Należy pamiętać, że koordynator klastra jest częścią łańcucha dostaw swoich członków na wielu poziomach. Dotyczy to zarówno usług, portalu członka, wspólnej platformy zakupowej, czy dzielonej infrastruktury laboratoryjnej i produkcyjnej.

Tabela 4.1 *Rodzaje ataków i ich konsekwencje dla klastra.*

Rodzaj ataku	Przykład	Konsekwencje
Phishing (w tym spear phishing przy użyciu AI)	Atakujący wysyła spreparowaną wiadomość e-mail do koordynatora wykorzystując wizerunek jednego z członków klastra lub instytucji zaufania publicznego, celem zmuszenia ofiary do wykonania czynności (np. podanie danych uwierzytelniających), która w konsekwencji prowadzi do wycieku danych, zaszyfrowania systemu lub kradzieży tożsamości bądź pieniędzy. Co odróżnia phishing od spoofingu to skala, gdyż zwykle wysyłany jest masowo[a]. Jednym z rodzajów ataków phishingowych jest spear phishing. Atakujący przed przeprowadzaniem ataku wykonują wnikliwą analizę wywiadowczą ofiary, aby uzyskać jak najwięcej informacji i w konsekwencji podszyć się pod osoby lub organizację znane ofierze, w celu zwiększenia skuteczności ataku. Obecnie coraz większą popularnością cieszą się ataki phishingowe tworzone z wykorzystaniem sztucznej inteligencji.	Utrata dostępu do skrzynki mailowej, ryzyko przelewu na fałszywe konta, wyciek danych osobowych i wrażliwych, utrata wiarygodności u członków i partnerów publicznych.

a Makowiec, Paweł, (2025) „Cyberatak na gminy. Sprawcy podszywają się pod ministerstwo" [artykuł online]. Dostęp: https://cyberdefence24.pl/cyberbezpieczenstwo/cyberatak-na-gminy-sprawcy-podszywaja-sie-pod-ministerstwo. (28 listopada 2025)

Rodzaj ataku	Przykład	Konsekwencje
	Atakujący używają narzędzi AI celem tworzenia bardziej ukierunkowanych i wiarygodnych fałszywych wiadomości tekstowych lub nawet klonując głos sławnych osób[b].	
Ataki na sieć Wi-Fi	Atakujący tworzą fałszywy punkt dostępu do Wi-Fi np. w miejscach publicznych (lotnisko, kawiarnia) i w ten sposób uzyskują dane do logowania od nieświadomych ofiar. Atakujący może stworzyć fałszywą sieć Wi-Fi w miejscu, gdzie klaster udostępnia swoją infrastrukturę, np. w laboratorium, centrum testowym lub hali prototypowej. Jeżeli członkowie klastra lub pracownicy koordynatora przypadkowo połączą się z taką siecią, haker może przechwycić ich loginy, hasła lub dane techniczne przesyłane podczas pracy[c].	Podglądanie ruchu, dokumentów czy haseł, przejęcie kontroli nad urządzeniami w biurze, możliwość podszycia się pod koordynatora w komunikacji.
Ataki na aplikacje internetowe	Hakerzy uzyskują dostęp do strony internetowej koordynatora lub aplikacji online (CRM, portal członka) poprzez phishing lub wykorzystanie podatności w systemie lub inny rodzaj ataku (np. SQL Injection)[d].	Podmiana treści strony koordynatora celem wyłudzania danych odwiedzających, wyciek danych członków klastra, zniszczenie lub usunięcie treści i dokumentów.
Ataki DDoS	Atakujący zasypują serwer hosta strony internetowej koordynatora co w konsekwencji powoduje niedostępność strony. Atak ten może również odwracać uwagę od innego wektora ataku, z którego korzystają atakujący[e].	Czasowe wyłączenie strony i platform projektowych, brak możliwości rejestracji na wydarzenia, utrudniona komunikacja z członkami.
Spoofing	Atakujący podszywa się pod domenę członka Klastra i podszywając się pod niego wysyła e-maila do koordynatora z prośbą o dostęp do platformy, wykonanie przelewu bądź podanie danych na spreparowanej wcześniej stronie.	Wyciek danych, straty finansowe, chaos informacyjny (np. fałszywe zmiany w harmonogramie projektów), spadek zaufania do koordynatora klastra.

b Przykład ataku spear phishing: Olszewska, Monika, (2025) „Natalia Sikora oszukana „na Anthony'ego Hopkinsa!" 39-letnia wokalistka straciła mnóstwo pieniędzy" [artykuł online]. Dostęp: https://tvn.pl/gwiazdy/natalia-sikora-ofiara-oszustwa-na-anthony-ego-hopkinsa-wokalistka-myslala-ze-dostala-zyciowa-szanse-st8752674. (28 listopada 2025)

c Przykład ataku na sieć Wi-Fi: Makowiec, Paweł, (2024), „Wyłudzał dane logowania od pasażerów samolotów. Wszystko dzięki Wi-Fi" [artykuł online]. Dostęp: https://cyberdefence24.pl/cyberbezpieczenstwo/wyludzal-dane-logowania-od-pasazerow-samolotow-wszystko-dzieki-wi-fi. (28 listopada 2025)

d Przykład ataku na aplikacje internetowe: Pentest Tools Blog, (2024) „Breaking down the 5 most common SQL injection attacks" [artykuł online]. Dostęp: https://pentest-tools.com/blog/sql-injection-attacks. (28 listopada 2025)

e Przykład ataku DDoS: Makowiec, Paweł, (2025) „Kolejny atak DDoS na system BLIK" [artykuł online]. Dostęp: https://cyberdefence24.pl/cyberbezpieczenstwo/kolejny-atak-ddos-na-system-blik. (28 listopada 2025)

Rodzaj ataku	Przykład	Konsekwencje
	W spoofingu mamy do czynienia z techniką maskowania tożsamości i ukrycia źródła tożsamości i zwykle kierowany jest do konkretnej ofiary[f].	
Malware	Wykorzystując phishing/spoofing lub podatności w systemie atakujący wysyła złośliwe oprogramowanie, które nieświadomie uruchamiana jest przez ofiarę. Malware rozprzestrzenia się w systemie dając atakującemu uprawnienia, która wykorzystuje np. do kradzieży danych osobowych[g].	Kradzież dokumentów, faktur, danych członków, rozprzestrzenienie się infekcji na urządzenia pracowników.
Ataki na urządzenia mobilne	Scenariusz ataku jest podobny jak w przypadku malware, z tą różnicą, że nakierowany jest na urządzenia mobilne używane w firmie[h].	Przejęcie poczty i komunikatorów, wyciek danych kontaktowych, nieautoryzowane logowanie do systemów klastra, nieautoryzowane przelewy.
Ataki na chmurę	Atakujący uzyskuje nieuprawniony dostęp do danych logowania chmury pracowników koordynatora (lub je omija), następnie pobiera wszystkie pliki, wysyła je na swój serwer, tworzy dodatkowe konta administracyjne[i].	Utrata dostępu do plików, nieautoryzowane udostępnianie zasobów koordynatora, usuwanie lub modyfikacja dokumentacji projektowej.
Socjotechnika	Przykładem socjotechniki jest spoofing i phishing, ale w zbiór tej kategorii wchodzi więcej technik opierających się na psychicznej manipulacji pracownikiem, np. presja pośpiechu, strach przed przełożonym[j].	Przekazanie dostępu do systemu osobom nieuprawnionym, ujawnienie danych członków i partnerów, błędne decyzje administracyjne na podstawie zmanipulowanych danych.
Ransomware	Zwykle za pomocą phishingu atakujący dostarcza złośliwe oprogramowanie do systemów firmowych, który po uruchomieniu szyfruje pliki i rozprzestrzenia się do sieci biurowej.	Przerwanie ciągłości działania, wysokie koszty odbudowania systemu, brak możliwości realizacji projektów i komunikacji z członkami.

f Przykład spoofingu: Bochyńska, Nikola, (2022) „Walka ze spoofingiem w Polsce. Komendant CBZC: „Kampania przygotowana pod znane osoby i spersonalizowana" [artykuł online]. Dostęp: https://cyberdefence24.pl/armia-i-sluzby/walka-ze-spoofingiem-w-polsce-komendant-cbzc-kampania-przygotowana-pod-znane-osoby-i-spersonalizowana. (28 listopada 2025)

g Przykłady rodzajów malware: Baker, Kurt, (2023) „The 12 Most Common Types of Malware" [artykuł online}. Dostęp: https://www.crowdstrike.com/en-us/cybersecurity-101/malware/types-of-malware/. (28 listopada 2025)

h Przykład ataku na urządzenia mobilne: Rogalewicz, Mikołaj, (2025) „Nowy malware na Androida. Jest w stanie naśladować człowieka" [artykuł online]. Dostęp: https://cyberdefence24.pl/cyberbezpieczenstwo/nowy-malware-na-androida-jest-w-stanie-nasladowac-czlowieka. (28 listopada 2025)

i Przykład ataku na chmurę: Komunikat Zespołu Bezpieczeństwa Informacji Wrocławskiego Centrum Sieciowo-Superkomputerowego. Dostęp: https://di.pwr.edu.pl/aktualnosci/ostrzezenie-o-atakach-na-konta-ms365-115.html. (28 listopada 2025)

j Przykład socjotechniki: Palczewski, Szymon, (2025) „Oszustwo na PKO BP. Wschodni akcent w słuchawce" [artykuł online]. Dostęp: https://cyberdefence24.pl/cyberbezpieczenstwo/oszustwo-na-pko-bp-wschodni-akcent-w-sluchawce. (28 listopada 2025)

Rodzaj ataku	Przykład	Konsekwencje
	Atakujący za odblokowanie dostępu żąda okupu (zwykle w kryptowalutach), grożąc często ujawnieniem danych[k].	

Źródło: Opracowanie własne.

k Przykład ataku ransomware: Klimczuk, Oskar, (2025) „Atak na Urząd Miasta w Wadowicach. Wysokie ryzyko kradzieży danych" [artykuł online]. Dostęp: https://cyberdefence24.pl/cyberbezpieczenstwo/atak-na-urzad-miasta-w-wadowicach-wysokie-ryzyko-kradziezy-danych. (28 listopada 2025)

Atak wymierzony w koordynatora może być tylko sposobem dostępu do członków i partnerów klastra. Ataki na łańcuch dostaw stały się w ostatnich czasach bardzo popularne – atakujący wykorzystują podatności i słabości podwykonawców, dostawców i partnerów, aby dostać się do lepiej zabezpieczonych systemów swojej docelowej ofiary. Specyficzna rola koordynatora klastra – ściśle współpracującego z dużą grupą przedsiębiorstw i pełniącego funkcję zaufanej strony – sprawia, że musi on zapewnić co najmniej podstawowy poziom zabezpieczeń cyfrowych w swojej organizacji.

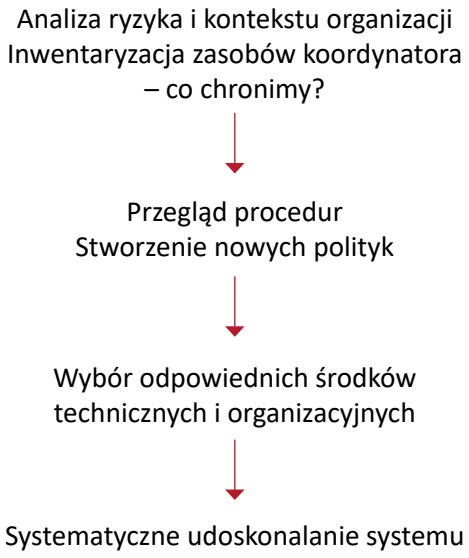
Warto również wyraźnie zaznaczyć, że w obecnych czasach cyberbezpieczeństwo nie powinno być rozpatrywane wyłącznie jako kwestia technologiczna dla działów IT. Powinno być nierozerwalną częścią procesów biznesowych w każdej organizacji. Wyciek danych, zakłócenie ciągłości działania, kompromitacja domeny, to nie tylko straty finansowe, ale także wizerunkowe. W przypadku koordynatora klastra zaufanie i wiarygodność to podstawa, dlatego cyberbezpieczeństwo należy traktować nie jako koszt, lecz jako inwestycję w stabilność i wiarygodność klastra.

Cyberbezpieczeństwo jest procesem, dlatego oprócz odpowiedniego przygotowania się do wdrożenia odpowiednich procedur czy narzędzi nie można zapominać o ciągłym doskonaleniu systemu. Zagrożenia w cyberprzestrzeni stale się zmieniają. Sama specyfika klastra, w której członkowie zmieniają się dynamicznie, a koordynator realizuje kilka dużych projektów na raz, wymusza ciągłe podnoszenie odporności. W zakresie ciągłego doskonalenia systemu bezpieczeństwa warto wymienić m.in.:

- regularne szkolenia personelu,
- okresowe przeglądy i audyty polityk i procedur,
- testy penetracyjne infrastruktury,
- śledzenie krajobrazu zagrożeń,
- aktualizacje oprogramowania,
- szacowanie ryzyka, w tym stron trzecich.

4.2. Dobre praktyki budowania cyberodporności u koordynatora klastra

Znając już rodzaje zagrożeń, matrycę ryzyka oraz ramy regulacyjne cyberbezpieczeństwa, koordynator może w pierwszym kroku przeprowadzić analizę ryzyka i kontekstu swojej organizacji. Następnie kluczowy będzie przegląd istniejących procesów lub stworzenie nowych polityk, odpowiadających potrzebom danego koordynatora. Kolejnym etapem jest wybór odpowiednich rozwiązań, a następnie zarządzanie i udoskonalanie procesu. Uproszczony proces budowania systemu cyberbezpieczeństwa koordynatora klastra można przedstawić następująco:



W budowie systemu cyberbezpieczeństwa koordynatora klastra można korzystać z wielu różnych podejść. W zależności od skali działalności klastra i specyfiki sektora można uwzględnić podstawowe zagadnienia cyber-higieny, a także posiłkować się regulacjami (np. Art 8 UKSC2 mówiący o środkach technicznych i organizacyjnych) lub sięgnąć po normy takiej, jak ISO 27001, czy ISO 22301.

Normy ISO w szczególności pomagają zbudować zestaw polityk i procedur związanych z cyberbezpieczeństwem. Poniżej przedstawimy najbardziej popularny zbiór polityk i procedur, które wspierają procesy związane z budowaniem ogólnej polityki bezpieczeństwa informacji w firmie:

- role i odpowiedzialności,
- polityka analizy i zarządzania ryzykiem,
- polityka kontroli dostępu,
- procedura ciągłości działania,
- procedura obsługi i zarządzania incydentem,
- polityka bezpieczeństwa fizycznego,
- procedury audytu i kontroli zgodności z normami/regulacjami[67].

Poniżej prezentujemy zbiór podstawowych zasad cyberhigieny oraz przykłady najlepszych praktyk i list sprawdzających związanych z polityką haseł i procedurą kopii zapasowych, których stosowanie w spółce koordynatora klastra może znacząco zmniejszyć skutki cyberataku. Wartym podkreślenia jest fakt, że zdecydowana większość poniższych wskazówek jest darmowa – koordynator nie musi ponosić wysokich kosztów lub są one minimalne.

Cyberhigiena

Rysunek 4.1 *Główne zasady cyberhigieny.*

Źródło: Opracowanie własne.

67 Na podstawie normy ISO/IEC 27001:2022.

Polityka haseł

Poniżej zostały zaprezentowane zagadnienia, które mogą stanowić podstawowy wzór polityki haseł dla koordynatora klastra oraz dla małej organizacji:

1. Hasła organizacji powinny składać się z co najmniej 16 znaków, uwzględniających co najmniej jedną cyfrę oraz jeden znak specjalny.

2. Użytkownik powinien stosować różne hasła do różnych systemów.

3. Hasła nie powinny uwzględniać łatwych do odgadnięcia ciągów znaku np. daty urodzenia, imienia i nazwiska, nazwy organizacji.

4. Każdy użytkownik zobowiązany jest do używania wdrożonego w firmie managera haseł.
   Przykłady managerów haseł:
   - Manager haseł Google[68],
   - KeePass[69],
   - PercPass[70].

5. Użytkownik zobowiązany jest do zmiany hasła w momencie otrzymania informacji o wycieku danych z serwisów, w których ma utworzone konto.

6. Użytkownik zobowiązany jest do stosowania uwierzytelniania wieloskładnikowego wdrożonego w organizacji.
   Przykład aplikacji uwierzytelniających:
   - Microsoft Authenticator,
   - Google Authenticator.

7. Używanie konta administracyjnego powinno służyć tylko do wykonywania czynności administracyjnych.

8. Użytkownik powinien unikać zapisywania haseł w notatnikach na biurku lub wywieszania ich w widocznym miejscu w biurze. Jeżeli hasła są zapisywane, to powinny być trzymane dyskretnie pod kluczem a najlepiej przechowywawane w managerze haseł.

Wskazówka dla koordynatora: rekomenduje się regularne odwiedzanie strony https://haveibeenpwned.com/, która analizuje czy podany adres e-mail znajdował się w jednym z wielu monitorowanych przez nich wycieków danych.

Polityka tworzenia kopii zapasowych[71]

1. **Cel polityki**
   Polityka określa zasady tworzenia, przechowywania i testowania kopii zapasowych danych organizacji. Celem jest zapewnienie ciągłości działania firmy, ograniczenie skutków awarii, błędów ludzkich i ataków cybernetycznych (w tym ransomware).

2. **Zakres**
   Polityka obejmuje:
   - dane pracowników,
   - dokumenty firmowe,
   - pocztę elektroniczną,
   - systemy biznesowe (ERP/CRM/Bazy danych),
   - komputery i urządzenia mobilne,
   - serwery lokalne i wirtualne,
   - konfiguracje urządzeń sieciowych.

68 Strona internetowa narzędzie Manager haseł Google. Dostęp: https://passwords.google.com/intro. (28 listopada 2025)
69 Strona internetowa narzędzia KeePass. Dostęp: https://keepass.info/. (28 listopada 2025)
70 Strona internetowa narzędzia Percpass. Dostęp: https://percpass.com/. (28 listopada 2025)
71 Na podstawie: Xopero Software, „Plan Backupu. Jak go stworzyć aby był skuteczny i niezawodny". Dostęp: https://xopero.com/pl/dokumenty/backup-plan/. (28 listopada 2025)

3. Zasady backupu (Model 3-2-1)

Organizacja stosuje zasadę 3-2-1:

- 3 kopie danych,
- 2 różne nośniki lub środowiska,
- 1 kopia poza lokalizacją firmy (offsite lub chmura).

4. Harmonogram backupu

- backup codzienny: pliki, dokumenty, skrzynki pocztowe,
- backup tygodniowy pełny (full): systemy biznesowe, serwery,
- backup przyrostowy: między pełnymi backupami,
- kopia offline/offsite: minimum 1 raz dziennie.

5. Retencja

Dane przechowywane są minimum:

- 30 dni – standard,
- 90 dni – dla systemów krytycznych,
- do 12 miesięcy – dla danych istotnych z punktu widzenia zgodności i audytów.

6. Przechowywanie i zabezpieczenia

- kopie szyfrowane w trakcie przesyłu i w spoczynku,
- nośniki fizyczne przechowywane w miejscu zabezpieczonym przed dostępem osób nieuprawnionych,
- kopie chmurowe przechowywane w środowisku posiadającym backup geograficzny,
- dostęp do systemu backupowego ograniczony do wyznaczonych osób.

7. Odpowiedzialności

Właściciel procesu backupu – wyznaczona osoba (IT lub osoba odpowiedzialna za operacje). Odpowiada za monitorowanie backupów, reagowanie na błędy, plan testów i aktualizację listy danych objętych backupem.

8. Testowanie kopii zapasowych

- Test przywracania wybranych danych – raz na kwartał.
- Test pełnego odtwarzania systemu (Disaster Recovery Test) – raz do roku.
- Wyniki testów dokumentowane i raportowane właścicielowi firmy lub zarządowi.

9. Procedury awaryjne

Plan w punktach:

1. W przypadku utraty danych lub incydentu cyber: zgłosić incydent do osoby odpowiedzialnej,
2. Ocenić zakres utraty danych,
3. Odtworzyć dane zgodnie z instrukcją Disaster Recovery,
4. Dokonać analizy przyczyny incydentu,
5. Wprowadzić działania naprawcze (patch, zmiana hasła, dodatkowa kopia offline).

10. Przegląd polityki

Polityka backupu jest przeglądana raz w roku lub po istotnym incydencie bezpieczeństwa.

Powyższe zasady związane z procesem budowy systemu cyberbezpieczeństwa, mogą mieć zastosowanie również w małej i średniej firmie członkowskiej klastra. Zachęcamy do dzielenia się tą wiedzą ze swoimi członkami i partnerami.

Listy kontrole związane z budowaniem cyberbezpieczeństwa w organizacji znajdują się w rozdziale 5 niniejszego podręcznika.

Rozdział 5

Praktyczne sposoby wsparcia członków klastra przez koordynatora

Budowanie odporności cyfrowej w klastrze nie polega jedynie na dostarczaniu pojedynczych usług czy szkoleń, ale na stworzeniu trwałego systemu wsparcia, który pozwala wszystkim członkom, niezależnie od ich wielkości i poziomu dojrzałości cyfrowej, funkcjonować w bezpiecznym i świadomym środowisku biznesowym. Koordynator klastra pełni tutaj kluczową rolę jako inicjator działań, organizator współpracy oraz strażnik standardów funkcjonowania ekosystemu.

Poniższy rozdział stanowi zbiór praktycznych metod i gotowych do wdrożenia narzędzi, które koordynator może wykorzystać, aby efektywnie podnieść ogólną odporność cyfrową całego ekosystemu klastra.

5.1 Ocena poziomu cyberbezpieczeństwa członków klastra oraz benchmarking

Zanim koordynator podejmie decyzję o wdrożeniu konkretnych narzędzi lub szkoleń, niezbędna jest diagnoza – zrozumienie, gdzie aktualnie znajdują się członkowie klastra w kontekście swojej dojrzałości cybernetycznej. Metodyka powinna być prosta, aby nie zniechęcać MŚP do udziału, a jednocześnie dawać użyteczny obraz całości.

Ocena poziomu cyberbezpieczeństwa pozwala koordynatorowi:

- zrozumieć dojrzałość cyfrową członków klastra,
- zidentyfikować największe ryzyka dla łańcucha wartości,
- przygotować dedykowane działania, takie jak szkolenia, doradztwo, warsztaty,
- uzyskać argumenty do pozyskania finansowania na działania klastrowe,
- budować kulturę bezpieczeństwa jako wspólny standard współpracy biznesowej.

W przeciwieństwie do pełnych audytów zgodnych z ISO 27001 czy NIST, uproszczona samoocena poziomu dojrzałości (ang. Maturity Assessment, tłum. ocena dojrzałości) jest szybka, tania i możliwa do przeprowadzenia nawet w podmiotach, które nie mają własnych zespołów IT. Może przybrać formę ankiety lub listy kontrolnej, która pozwoli podmiotowi ocenić wewnętrzne procesy i technologie. Jest to uproszczony model, który sprawdzi się w ogólnej ocenie stanu cyberbezpieczeństwa, zwłaszcza w mikro i małych przedsiębiorstwach. Dla firm zaawansowanych technologicznie lub podlegających regulacjom (np. NIS2), stanowi on jedynie wstęp do pełnego audytu bezpieczeństwa zgodnego z normami takimi jak np. ISO 27001. Poniżej propozycja krótkiego kwestionariusza w modelu PPT (ang. People-Processes--Technology, tłum. ludzie-procesy-technologia).

Przykład konstrukcji kwestionariusza (Model PPT)

Filar	Pytania kluczowe dla członka klastra	Skala oceny
Ludzie (Świadomość)	1. Czy wszyscy pracownicy przechodzą obowiązkowe szkolenie z cyberbezpieczeństwa co najmniej raz w roku? 2. Czy przeprowadzane są regularne, niespodziewane symulacje phishingu?	0 (Nie) 1 (Częściowo) 2 (Tak, Systematycznie)
Procesy (Zarządzanie)	1. Czy podmiot posiada aktualny plan awaryjny (Business Continuity Plan – BCP)?	0 (Nie) 1 (Tak, nie testowano) 2 (Tak, jest testowana)

Filar	Pytania kluczowe dla członka klastra	Skala oceny
	2. Czy istnieje udokumentowana procedura tworzenia i weryfikacji kopii zapasowych (backup)? 3. Czy istnieje formalna procedura weryfikacji dostawców (due diligence)? 4. Czy istnieje procedura zgłaszania incydentów?	
Technologia (Zabezpieczenia)	1. Czy uwierzytelnianie wieloskładnikowe (MFA) jest wdrożone dla poczty i zdalnych dostępów? 2. Czy stosowane jest regularne łatanie (patching) luk w oprogramowaniu? 3. Czy kluczowe dane są szyfrowane na dyskach i w ruchu? 4. Czy wszystkie komputery w firmie/organizacji mają aktualny system operacyjny?	0 (Nie) 1 (Częściowo) 2 (Tak, dla wszystkich systemów)

Co powinno cechować proces wdrażania ankiety?

1. **Anonimizacja i poufność** – kluczowe jest zapewnienie organizacjom członkom klastra pełnej anonimowości i poufności danych. Koordynator nie powinien znać wyników poszczególnych podmiotów, a jedynie ich zagregowaną średnią. To buduje zaufanie i zachęca do szczerej odpowiedzi.

2. **Kanał i format** – ankieta powinna być krótka (maksymalnie 15-20 pytań zamkniętych, punktowanych). Ankiety można przeprowadzić za pomocą prostych, bezpłatnych narzędzi online (np. Google Forms, SurveyMonkey) lub użyć dedykowanych narzędzi np. stworzonych przez koordynatora klastra w ramach swoich działań. Użycie darmowych rozwiązań jest dobrym pomysłem przy ankietach ogólnych, niezawierających informacji dotyczących zabezpieczeń.

3. **Wsparcie** – do każdej ankiety należy dołączyć krótki przewodnik definiujący pojęcia (np. co to jest MFA, EDR – słownik dołączony jest również do niniejszego podręcznika), aby zapewnić jednolity sposób interpretacji pytań.

4. **Komunikacja** – podczas prowadzenia badania koordynator przekazuje podmiotom członkowskim cel oceny, czas trwania całego procesu, sposób przeprowadzenia, deklarację poufności oraz wskazuje na korzyści, jakie może przynieść udział w badaniu.

Po zebraniu danych, koordynator przetwarza je na użyteczną formę, tj. przygotowuje krótki raport np. w formie prezentacji w programie MS Powerpoint, w której zawarta zostanie:

1. **Agregacja danych** – wyniki są sumowane dla każdego z trzech filarów (ludzie, procesy, technologia) i uśredniane.

2. **Wizualizacja** – prezentacja wyników nie powinna polegać na pokazywaniu, kto jest najsłabszy, lecz na identyfikacji obszarów ryzyka dla całego klastra. Wyniki są wizualizowane w postaci wykresu radarowego lub prostego słupkowego, wskazując:

   » mocne strony klastra: (np. filar ludzie – wysoka świadomość, 80% podmiotów przeszkolonych),

Obszar	Pytania	Skala	Wynik obszaru
Ludzie	1. Czy wszyscy pracownicy przechodzą obowiązkowe szkolenie z cyberbezpieczeństwa co najmniej raz w roku? 2. Czy przeprowadzane są regularne, niespodziewane symulacje phishingu? 3. Czy pracownicy mieli możliwość zapoznania się z procedurą reakcji na incydent? 4. Czy pracownicy mieli możliwość zapoznania się z polityką bezpieczeństwa informacji	0 – Nie 1 – Częściowo 2 – Tak	0–2 = „0” 3–5 = „1” 6–8 = „2”
Procesy	1. Czy podmiot posiada aktualny plan awaryjny (BCP)? 2. Czy istnieje udokumentowana procedura backupu? 3. Czy istnieje formalna procedura weryfikacji dostawców (due diligence)? 4. Czy istnieje procedura zgłaszania incydentów?	0 – Nie 1 – Tak, ale nie testowano 2 – Tak, testowana	0–2 = „0” 3–5 = „1” 6–8 = „2”
Technologia	1. Czy MFA jest wdrożone? 2. Czy prowadzony jest regularny patching? 3. Czy dane są szyfrowane? 4. Czy wszystkie komputery mają aktualny system?	0 – Nie 1 – Częściowo 2 – Tak, w pełni	0–2 = „0” 3–5 = „1” 6–8 = „2”

» obszary krytyczne/luki: (np. filar technologia – tylko 15% podmiotów stosuje MFA; filar procesy – brak planu ciągłości działania).

3. **Dostosowanie wsparcia** – raport końcowy służy do uzasadnienia dalszych działań. Jeśli wskaźnik wskaże, że największą luką jest brak BCP (plan ciągłości działania), koordynator wie, że pierwszym priorytetem jest zorganizowanie warsztatów na temat tworzenia prostych BCP i udostępnienie szablonów.

Ocena poziomu dojrzałości członków klastra może być podstawą do stworzenia cyklicznego benchmarkingu klastra oraz pomysłem na projekt rozwojowy opisywany szerzej w rozdziale 8 (Projekt C4AM).

Dysponując odpowiedziami z powyższej ankiety koordynator klastra może stworzyć benchmark, czyli raport całościowy z analizy poziomu cyberbezpieczeństwa swoich członków.

Wynik końcowy i poziomy dojrzałości

Przyjmując ujednoliconą skalę, gdzie za każdy obszar podmiot może otrzymać od 0 do 2 punktów można zastosować poniższą matrycę celem interpretacji wyników.

Na podstawie danych z ankiet koordynator może stworzyć benchmarking oceniający stopień dojrzałości swoich członków. Taki benchmark pozwoli ocenić jaki jest poziom cyberbezpieczeństwa członków i danego sektora i będzie stanowił doskonałą okazję do stworzenia mapy rozwoju usług i projektów wspierających wspierających członków klastra. Koordynator może wykorzystać benchmark w kilku produktach:

Wynik	Poziom dojrzałości	Interpretacja
0–1	Bardzo niski	Brak podstawowych zabezpieczeń. Wysokie ryzyko incydentu.
2–3	Niski	Podmiot działa punktowo, brak procesów.
4–5	Średni	Istnieją procesy, technologia częściowo wdrożona.
6	Wysoki	Podmiot posiada dojrzałe zabezpieczenia i stabilne procesy.

a. Raport roczny klastra

- rozkład wyników członków klastra – heatmapy (wizualizacja danych, która używa kolorów do przedstawienia intensywności lub gęstości zjawiska w określonym obszarze), wykresy,
- średnia dojrzałość w każdym filarze,
- porównanie z poprzednim rokiem,
- najczęściej wskazywane braki (np. brak BCP, testów phishingowych).

b. Indywidualne karty wyników dla członków

Każdy podmiot otrzymuje:

- wynik globalny,
- wyniki filarowe,
- krótkie rekomendacje „first steps" (np. MFA, backup, szkolenie roczne).

c. Benchmark branżowy

Klaster może zestawiać wyniki:

- producenci vs. logistyka vs. usługi,
- firmy duże vs. mikro,
- nowe organizacje vs. długoletni członkowie.

W kontekście budowania ankiet ewaluacyjnych czy benchmarkingów, a także tworząc matrycę ryzyka (zaprezentowaną w rozdziale 2) warto wziąć pod uwagę profil zagrożeń danego sektora. Rodzaj i częstotliwość pojawiania się zagrożeń będą znacznie różniły się od sektora, w którym operuje dany klaster – z innymi wyzwaniami będzie zmagał się sektor opieki zdrowotnej, a z innym sektor nastawiony na produkcję czy przemysł ciężki. Na następnych stronach zaprezentowana została infografika pokazująca specyfikę zagrożeń w danym sektorze, w którym operują polskie Krajowe Klastry Kluczowe.

Praktyczne wskazówki dla koordynatora:

Użyj zasady anonimowości jako narzędzia marketingowego. Komunikat powinien brzmieć: „Im więcej podmiotów weźmie udział, tym dokładniej klaster wskaże luki i tym lepsze, dopasowane do waszych realnych potrzeb szkolenia i usługi zaoferujemy".

Warto skorzystać już z gotowych, darmowych narzędzi przygotowanych np. przez NASK[72], PFR (Polski Fundusz Rozwoju)[73], czy PARP (Polska Agencja Rozwoju Przedsiębiorczości) w ramach inicjatywy AI4SME[74] oraz PARP4digital[75]. Jest to dobre rozwiązania dla członków klastra, którzy chcieliby mocniej skupić się na analizie swojego poziomu cyfryzacji i indywidualnie podejść do tematu.

72 Samodzielna ocena poziomu jakości i bezpieczeństwa usług cyfrowych dostępna na stronie internetowej NASK. Dostęp: https://firmabezpiecznacyfrowo.pl/diagnoza/. (24 listopada 2025)

73 Test Dojrzałości Cyfrowej dostępny na stronie internetowej PRF. Dostęp: https://pfr.pl/test-dojrzalosci-cyfrowej. (24 listopada 2025)

74 Test AIMIND (określa poziom dojrzałości przedsiębiorstwa w obszarze wdrażania i wykorzystania sztucznej inteligencji) dla AI4SME. Dostępny na stronie internetowej PARP. Dostęp: https://ai4msp.pl/test-aimind/. (24 listopada 2025)

75 Zestaw narzędzi do samooceny poziomu cyfryzacji w przedsiębiorstwie dostępny jest na stronie internetowej PARP. Dostęp: https://www.parp.gov.pl/component/site/site/4digital. (24 listopada 2025)

Rysunek 5.1

Lotnictwo

Dolina Lotnicza, Śląski Klaster Lotniczy

⚠ Krytyczne

58,4% wszystkich cyberataków na transport

Ransomware Łańcucha Dostaw
Szyfrowanie systemów dostawców krytycznych dla lotnictwa

Manipulacja Systemami Odprawy
MUSE System Collins – powrót do obsługi manualnej

Fałszowanie Sygnałów GPS (Spoofing)
Podszywanie się pod sygnały satelitarne, przekierowanie trasy

Luki w Systemach Autonomicznych
Ataki na systemy autopilota i kontroli lotu

Motoryzacja

Polska Grupa Motoryzacyjna, Silesia Automotive

⚠ Krytyczne

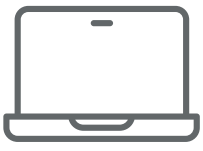
Zagrożenia technologią autonomiczną

Podatności Typu Zero-Day
Niezidentyfikowane luki w systemach sterowania pojazdem

Ataki na Systemy OT (Operational Technology)
Manipulacja systemami sterowania silnikiem i podwoziem

Fałszywe Aktualizacje Over-The-Air
Zainfekowana aktualizacja wysłana do pojazdów bezpośrednio

Kradzież IP Technologii Autonomicznej
Własność intelektualna i algorytmy sztucznej inteligencji



ICT/Technologia

Mazowiecki Klaster ICT, Pomorski Klaster ICT

⚠ Wysoka

32% MŚP doświadczenia phishingu

Phishing Kampanie
Ataki na dyrektorw IT (whaling) w celu uzyskania dostępu

Ataki APT (Advanced Persistent Threat)
Zaawansowane grupy szpiegowskie (GRU od 2022)

Kradzież Źródła Kodu
Własność intelektualna, technologie, algorytmy

Wycieki Danych i Baz Kodów
Wyciek numerów PESEL, serii dowodów, poufnych danych

Medycyna/LifeScience

MedSilesia, NUTRIBIOMED, Klaster LifeScience Kraków

⚠ Krytyczne

Wysokie wartości okupu za dane pacjentów

Ransomware na Dane Pacjentów
Szyfrowanie danych i szantaż ekstorcyjny

Wycieki Poufnych Informacji Zdrowotnych
200k+ rekordów pacjentów = miliardowe straty i reputacyjne

Ataki na Bazy Danych Medycznych
Dane pacjentów s cennym towarem dla cyber-przestępców

Przerwanie Usług Medycznych
Bezpośrednie zagrożenie dla zdrowia i życia pacjentów

Produkcja Zaawansowana

Obróbka Metali, NANO, Kompozyty

⚠ Krytyczne

Colonial Pipeline*: 4,4M$ okupu

Ataki OT/SCADA/ICS
Manipulacja parametrami produkcji

Niezabezpieczone Systemy
Stare, nieaktualizowane oprogramowanie

Uszkodzenia Maszyn CNC
Fizyczne zniszczenia infrastruktury

Wstrzymanie Produkcji
2M$ strat za 4 godziny w fabryce

Transport/Logistyka

Drugie miejsce ataków w UE – 20,8% incydentów

⚠ Wysoka

87,6% DDoSów na transport to hacktywizm

DDoS Ataki (Distributed Denial of Service)
Grupy hacktywistyczne – 87,6% ataków na transport

Phishing Kampanie
Kradzież poświadczeń dostępu do systemów logistyki

Fałszowanie Sygnałów GPS (Spoofing)
Zmiana tras pojazdów w systemach nawigacji

Ataki na Niezabezpieczone Połączenia
Włamania do systemów zarządzania flotą

* Colonial Pipeline Company to amerykańska firma, która przesyła ropę i paliwa ropopochodne z Teksasu do Nowego Jorku oraz wielu innych stanów. W 2021 roku firma ta została zaatakowana przez ransomware, który spowodował zatrzymanie prac. Podczas procesu nadzorowanego przez FBI firma zapłaciła okup w wysokości ok. 4.4 mln $ w zamian za narzędzie deszyfrujące.

Źródło: Opracowanie własne.

5.2 Bezpieczeństwo łańcucha dostaw

Tak jak zostało wspomniane w rozdziale pierwszym, atak na łańcuch dostaw jest jednym z największych zagrożeń dla klastrów. Rolą koordynatora jest dostarczenie członkom prostych metod na zarządzanie ryzykiem (szerzej omówione w rozdziale drugim), które pochodzi od ich dostawców, partnerów i podwykonawców.

W rozdziale drugim przedstawiona została macierz ryzyka cyber dla MŚP w oparciu o najczęściej występujące cyberzagrożenia, a poniżej macierz, którą można wykonać dla każdej zidentyfikowanej krytycznej relacji w łańcuchu dostaw. W przypadku zidentyfikowania krytycznego ryzyka, koordynator powinien zalecić członkom wdrożenie przykładowych mechanizmów, które zostały opisane poniżej.

Przykładowa prosta matryca oceny ryzyka w łańcuchu dostaw

Pytanie	Ocena Ryzyka (Skala 1-3)	Uzasadnienie
Jakie jest prawdopodobieństwo ataku na systemy dostawcy?	[1 – Niskie, 2 – Średnie, 3 – Wysokie]	[np. Dostawca IT nie ma MFA i stosuje słabe hasła, co podnosi prawdopodobieństwo.]
Jaki jest skutek wystąpienia takiego ataku?	[1 – Mały, 2 – Znaczący, 3 – Katastrofalny]	[np. Niedostępność systemów tego dostawcy paraliżuje całą produkcję na więcej niż 48h, co jest katastrofalne.]
Jaki jest priorytet działania?	[Wynik iloczynu (mnożymy określony poziom prawdopodobieństwa ataku oraz skutków awarii, jeżeli wynik jest pomiędzy 6, a 9, to ryzyko określić na poziomie krytycznym]	[Wymaga natychmiastowej uwagi.]

Koordynator powinien pomóc podmiotom członkowskim w identyfikacji krytycznych relacji w łańcuchu dostaw. Nie chodzi o listę wszystkich dostawców, ale o tych, którzy:

1. Uzyskują dostęp do wewnętrznych systemów podmiotów (np. dostawca usług IT, zewnętrzny serwisant systemów OT).
2. Uzyskują dostęp do kluczowych danych (np. księgowość, HR, projekty techniczne).
3. Dostarczają kluczowy komponent/usługę, której awaria sparaliżuje całą organizację (np. dostawca chmury, jedyny producent specjalistycznego komponentu itd.).

Wymogi kontraktowe i SLA

SLA (ang. Service Level Agreement, tłum. umowa o poziomie usług) to umowa o poziomie świadczenia usług między dostawcą usług, a klientem, która określa oczekiwany poziom jakości, dostępności i wydajności usługi. Można w niej zdefiniować konkretne mierzalne parametry, według których oceniana jest jakość świadczonych usług oraz określić konsekwencje niespełnienia tych standardów. Zawarcie wspomnianej umowy niesie ze sobą wiele korzyści związanych przede wszystkim z możliwością określenia jasnych oczekiwań, dotyczących jakości usług oraz minimalizacją ryzyka związanego z niedostateczną ich jakością. Jednak podczas tworzenia dokumentu warto zwrócić uwagę

m.in. uwagę na możliwość dostosowania SLA do zmieniających się warunków (np. wynikających ze zmian w przepisach prawnych), czy zapewnienie przejrzystości w raportowaniu oraz precyzyjne określenie właściwych i mierzalnych wskaźników[76].

Przykładowe zapisy, jakie można uwzględnić w umowie:

- **Obowiązek stosowania MFA** – wszelki zdalny dostęp do systemów członka klastra musi być chroniony uwierzytelnianiem wieloskładnikowym.

- **Wymóg powiadamiania o incydencie** – dostawca musi natychmiast, w ciągu określonego czasu (np. 24h), powiadomić o każdym naruszeniu bezpieczeństwa lub incydencie, który może mieć wpływ na systemy klienta. Jest to wymóg kluczowy w kontekście regulacji RODO i NIS2/UKSC2.

- **Prawo do audytu** – w przypadku incydentu, klient (podmiot członkowski) ma prawo zlecić zewnętrzny audyt bezpieczeństwa procesów dostawcy.

Zarządzanie dostępem uprzywilejowanym (Least Privilege)

Nawet najbardziej zaufany dostawca powinien mieć dostęp wyłącznie do niezbędnych zasobów i usług. Koordynator powinien promować zasadę najmniejszego przywileju (ang. Principle of Least Privilege), to jest:

- **Ograniczyć uprawnienia** – dostawca powinien mieć dostęp tylko do tych systemów i funkcji, które są mu niezbędne do pracy. Przykładowo, serwisant strony internetowej nie potrzebuje dostępu do serwera ERP.

- **Kontrola dostępu zdalnego** – wszelki dostęp zdalny dostawców powinien być realizowany poprzez bezpieczne, monitorowane systemy (np. rozwiązania PAM – Privileged Access Management) i automatycznie wygasać po zakończeniu prac.

- **Dedykowane konta** – zamiast używania kont wspólnych, każdy zewnętrzny specjalista powinien mieć własne, unikalne konto, aby możliwe było śledzenie jego działań w razie incydentu.

5.3 Analiza ryzyka i kontekstu działalności klastra oraz jego członków

Koordynator klastra może pełnić rolę „tłumacza" pomiędzy językiem technicznym cyberbezpieczeństwa, a rzeczywistością biznesową konkretnych branż. Analiza ryzyka i kontekstu powinna zaczynać się od odpowiedzi na pytanie: co jest najważniejsze dla organizacji w naszym klastrze, jakie procesy, dane i systemy? Inaczej wygląda to w klastrze przemysłowym, inaczej w usługowym, a jeszcze inaczej w kreatywnym, czy medycznym.

Praktyczną metodą jest przygotowanie krótkiej „mapy ryzyka sektorowego" dla klastra. Koordynator identyfikuje typowe procesy (np. produkcja, logistyka, sprzedaż online, projektowanie, obsługa klienta) i przypisuje do nich typowe zagrożenia, jak np. ransomware blokujące produkcję, phishing w dziale finansowym, wyciek dokumentacji projektowej, przejęcie konta w systemie e-commerce itd. Taka mapa nie musi mieć formy skomplikowanej matrycy – ważne, by była zrozumiała dla właściciela danej organizacji i pokazywała zależność „proces → zagrożenie → sposób zapobiegania".

76 Więcej na temat umów SLA można znaleźć na stronie internetowej nFlo. Dostęp: https://nflo.pl/slownik/service-level-agreement/. (25 listopada 2025)

Przykład analizy sektorowej

Sektor	Krytyczne Aktywa (Co chronić?)	Dominujące Zagrożenie	Proponowane Działanie Klastra
Produkcja/OT	M.in. systemy sterowania (SCADA/PLC), maszyny, formuły techniczne.	M.in. sabotaż (przerwanie produkcji), szpiegostwo przemysłowe, ransomware na stacjach roboczych.	Warsztaty: Bezpieczna segmentacja sieci IT/OT
Finanse/Usługi	M.in. dane klientów, systemy transakcyjne, poczta elektroniczna.	M.in. Business Email Compromise, phishing zaawansowany, ataki na aplikacje webowe.	Szkolenia: procedury weryfikacji zleceń przelewu (zapewnienie drugiej pary oczu).
IT/Software	M.in. kod źródłowy, repozytoria, procesy DevOps.	M.in. atak na łańcuch dostaw (np. skompromitowanie kodu), wyciek własności intelektualnej.	Utworzenie wspólnego repozytorium bezpiecznych praktyk deweloperskich.

Dlaczego kontekst sektorowy jest kluczowy?

1. **Typologia zagrożeń** – w sektorze finansowym dominują ataki ukierunkowane na kradzież pieniędzy i danych (np. Business Email Compromise – to rodzaj przestępstwa, w którym za pomocą spreparowanej wiadomości e-mail oszuści starają się najczęściej nakłonić kogoś do wysłania pieniędzy lub ujawnienia poufnych informacji finansowych[77]). W sektorze produkcyjnym i energetycznym głównym celem jest sabotaż lub szpiegostwo przemysłowe, a wektorem ataku są często systemy OT (Operational Technology). Rozpoznanie sektora będzie miało wpływ na późniejsze zidentyfikowanie potencjalnych zagrożeń.

2. **Priorytet ochrony** – np. dla firmy IT, krytycznym zasobem jest własność intelektualna, dla szpitala – ciągłość działania i dane pacjentów.

3. **Regulacje** – organizacja podlegająca pod DORA (finanse) nie zawsze będzie podlegała też pod dyrektywę CER (infrastruktura krytyczna).

Ważne: Warto zaznaczyć, że podane w tabeli zagrożenia są tylko przykładami, wiele z nich np. phishing, czy ransomware może dotknąć podmiotu działającego w każdej branży.

5.4 Budowanie sieci zaufanych dostawców

Budowa sieci zaufanych dostawców to jedno z najskuteczniejszych narzędzi, jakie ma w ręku koordynator klastra. W praktyce wiele podmiotów ma problem z wyborem rzetelnego partnera w obszarze cyberbezpieczeństwa, czy IT – nie wiedzą, jak oceniać oferty, czego wymagać ani jak nie uzależnić się od jednego dostawcy. Klaster może pełnić rolę „filtra", który pomaga uporządkować rynek i wskazać sprawdzonych partnerów.

Pierwszym krokiem jest ustalenie kryteriów weryfikacji dostawców. Obok ceny, zakresu usług i referencji powinny znaleźć się elementy związane bezpośrednio z obszarem bezpieczeństwa: stosowane standardy (np. zgodność z normą ISO 27001), doświadczenie w danej branży, podejście

77 Na podstawie: Ministerstwo Cyfryzacji, (2023) „Oszustwa typu BEC" [artykuł online]. Dostęp: https://www.gov.pl/web/cyfryzacja/oszustwa-typu-bec. (2 grudnia 2025)

do aktualizacji oprogramowania i reagowania na incydenty, jasne zapisy umowne dotyczące odpowiedzialności za dane i ciągłość usług. Wiele dobrych praktyk wskazuje także na konieczność oceny kultury bezpieczeństwa po stronie dostawcy – jego transparentności, gotowości do audytu, sposobu komunikacji o incydentach.

Koordynator może stworzyć „białą listę" dostawców spełniających minimalne kryteria, z którymi klaster ma doświadczenia lub których kompetencje zostały pozytywnie zweryfikowane. Ważne, by unikać sytuacji monopolu. Rekomendowane jest oferowanie kilku alternatywnych firm dla podobnych usług, co pozwala uniknąć uzależnienia od jednego podmiotu i zachęca dostawców do utrzymywania jakości. Takie podejście jest zgodne z rekomendacjami w obszarze zarządzania ryzykiem dostawców i łańcucha dostaw.

Wskazane jest także, by klaster wypracował wspólną politykę due diligence[78] dostawców, np. w formie ankiety oceniającej standardy bezpieczeństwa, zakres podwykonawstwa i procedury reagowania na incydenty. Europejskie i krajowe przewodniki dla MŚP podkreślają, że aktywne zarządzanie dostawcami, zwłaszcza tymi mającymi dostęp do danych lub systemów, jest jednym z filarów dojrzałego cyberbezpieczeństwa. Koordynator może tu odegrać rolę moderatora procesu, ułatwiając podmiotom członkowskim zadawanie właściwych pytań i interpretowanie odpowiedzi. W ramach niniejszego podręcznika przygotowaliśmy przykładową listę sprawdzającą, którą udostępnić może koordynator klastra swoim podmiotom członkowskim, dzięki której możliwe będzie sprawdzenie zarówno „twardych" wymagań, jak i kultury bezpieczeństwa dostawcy.

Lista dot. weryfikacji dostawcy IT/cyberbezpieczeństwa

1. Podstawowe informacje o dostawcy

- Dostawca działa na rynku co najmniej X lat (np. 3–5).
- Posiada doświadczenie w obsłudze organizacji o podobnym profilu / w tej samej branży.
- Może przedstawić referencje (min. 2–3) z ostatnich lat.
- Ma jasno zdefiniowany zakres odpowiedzialności (umowy, regulaminy, OWU).

2. Zgodność ze standardami i regulacjami

- Posiada wdrożony system zarządzania bezpieczeństwem informacji (np. zgodny z ISO 27001 lub innymi uznanymi standardami).
- Ma formalne procedury ochrony danych osobowych (RODO) i może je przedstawić.
- Regularnie przeprowadza wewnętrzne lub zewnętrzne audyty bezpieczeństwa.
- Posiada polityki zarządzania dostępem, haseł, backupów, aktualizacji.

3. Techniczne środki bezpieczeństwa

- Stosuje aktualne oprogramowanie zabezpieczające (antymalware, firewall, systemy monitoringu).
- Zapewnia szyfrowanie danych w spoczynku (np. szyfrowanie dysków) i w ruchu (np. TLS).
- Stosuje uwierzytelnianie wieloskładnikowe (MFA) do dostępu administracyjnego i paneli klienckich.
- Ma zdefiniowaną politykę aktualizacji (łatki bezpieczeństwa instalowane w określonym czasie).
- Posiada mechanizmy ograniczonego dostępu do danych (nie każdy pracownik ma dostęp do wszystkiego).

78 Due diligence (ang. należyta staranność) w kontekście sprawdzania dostawcy usług IT/cyber oznacza działanie z „należytą starannością" przy wyborze podmiotu i późniejszym nadzorze

4. Kopie zapasowe i ciągłość działania

- Wykonuje regularne kopie zapasowe (z określoną częstotliwością – np. dziennie/tygodniowo).
- Przechowuje kopie w odseparowanej lokalizacji (fizycznie/osobna chmura/kopia offline).
- Określił parametry RPO/RTO (jak dużo danych można stracić, ile czasu trwa przywrócenie usług).
- Regularnie testuje odtwarzanie kopii zapasowych (nie tylko deklaruje ich istnienie).
- Posiada plan ciągłości działania (BCP) i plan awaryjny (DRP) – choćby w uproszczonej formie.

5. Reagowanie na incydenty

- Posiada formalną procedurę reagowania na incydenty bezpieczeństwa.
- Wyznaczył zespół/osoby odpowiedzialne za obsługę incydentów (24/7 lub w ustalonych godzinach).
- Określa i komunikuje maksymalne czasy reakcji (SLA) w przypadku awarii lub ataku.
- Zobowiązuje się w umowie do niezwłocznego informowania klienta o incydentach, które dotyczą jego danych/systemów.
- Po incydencie przygotowuje raport wskazujący na przyczyny i podjęte działania naprawcze, który udostępnia klientowi.

6. Zarządzanie podwykonawcami i łańcuchem dostaw

- Jasno wskazuje, czy i jakich podwykonawców używa (hosting, chmura, serwis zdalny itd.).
- Zawiera z podwykonawcami umowy obejmujące wymagania bezpieczeństwa i ochrony danych.
- Ma możliwość wskazania lokalizacji (kraj/region) przetwarzania danych.
- Określa zasady zmiany podwykonawców i informowania o tym klientów.
- Aktywnie ocenia ryzyko związane z własnymi dostawcami (np. ma minimalne kryteria bezpieczeństwa).

7. Organizacja, ludzie i kultura bezpieczeństwa

- Prowadzi regularne szkolenia z cyberbezpieczeństwa dla swoich pracowników.
- Ma procedury nadawania, odbierania i przeglądania uprawnień (np. przy zatrudnieniu/odejściu pracownika).
- Stosuje zasadę minimalnych uprawnień (dostęp tylko tam, gdzie to konieczne).
- Prowadzi rejestry dostępu i logi działań administracyjnych oraz przechowuje je przez określony czas.
- Jest gotów poddać się audytowi klienta (w rozsądnym zakresie) lub udostępniać raporty z audytów.

8. Umowy, odpowiedzialność i przejrzystość

- Umowy jasno regulują odpowiedzialność za naruszenia bezpieczeństwa i dane.
- Warunki rozwiązania umowy uwzględniają bezpieczne przekazanie/wymazanie danych.
- Dostawca deklaruje maksymalny czas przechowywania danych po zakończeniu współpracy.
- Warunki SLA (dostępność, czas reakcji, czas naprawy) są konkretne i mierzalne.
- Dostawca ma jasną politykę informowania o zmianach w usługach, cenach i warunkach bezpieczeństwa.

Po uzupełnieniu listy sprawdzającej o odpowiedzi TAK/CZĘŚCIOWO/NIE należy zliczyć konkretne odpowiedzi, a także przypisać wagę do wybranych pytań krytycznych (np. kopie zapasowe, incydenty, podwykonawcy) – będą one inne dla każdego podmiotu ze względu na zróżnicowany charakter działalności. Po przeliczeniu odpowiedzi można zaklasyfikować dostawcę jako:

- niskie ryzyko – spełnione większość kryteriów, brak czerwonych flag,
- umiarkowane ryzyko – część braków, możliwa współpraca przy planie poprawy,
- wysokie ryzyko – poważne luki (brak backupów, brak procedur, brak przejrzystości).

5.5 Propozycja wsparcia: gotowe pomysły na usługi i działania koordynatora

Samodzielne wdrożenie zaawansowanych mechanizmów obrony, takich jak np. całodobowe monitorowanie systemów, jest dla większości MŚP finansowo nieosiągalne. Klaster jako platforma współpracy może rozwiązać ten problem, umożliwiając członkom zbiorowy zakup technologii w ramach współdzielonych usług. Taka kooperacja minimalizuje koszty jednostkowe, jednocześnie maksymalizując efektywność obrony. Zamiast budować drogie kompetencje od zera, członkowie klastra inwestują w wspólną tarczę ochronną, która zapewnia aktywny monitoring i szybką, skoordynowaną reakcję na incydenty.

5.5.1 Wspólny SOC

Security Operations Center (SOC; tłum. Centrum Bezpieczeństwa Operacji) to wykwalifikowany zespół specjalistów, którego zadaniem jest monitorowanie i zapewnienie bezpieczeństwa informacji, przy wykorzystaniu mechanizmów wykrywania, analizowania i reagowania na incydenty związane z bezpieczeństwem. SOC to propozycja bardzo zaawansowanego modelu kolektywnej obrony w klastrze, który byłby inwestycją na poziomie całego ekosystemu. Utworzenie i utrzymanie własnego, całodobowego SOC jest dla większości MŚP nierealne z uwagi na ogromne koszty zatrudnienia wysoko wykwalifikowanych specjalistów oraz drogich narzędzi do monitorowania.

Dzięki modelowi współdzielonemu, klaster staje się dużym klientem zbiorowym, który:

- **Dzieli koszty i ryzyko:** klaster negocjuje jedną, zbiorową umowę na narzędzia do monitorowania (np. platformy SIEM/XDR) oraz na zespół analityków SOC. Koszty stałe zostają rozłożone na kilkanaście lub kilkadziesiąt podmiotów, co czyni usługę dostępną dla MŚP.

- **Zyskuje efekt skali (odporność stadna):** zespół SOC, monitorując kilkadziesiąt organizacji jednocześnie, ma znacznie szerszy ogląd zagrożeń. Jeśli atakujący wypróbują nową technikę phishingu na organizacji A, SOC może wdrożyć reguły detekcji i prewencji na serwerach pocztowych organizacji B, C i D, zanim atak je dosięgnie.

- **Zapewnia ciągły monitoring 24/7:** członkowie zyskują dostęp do aktywnego nadzoru bezpieczeństwa, co jest kluczowe, ponieważ większość zaawansowanych ataków jest prowadzona poza godzinami pracy.

5.5.2 Cyber Threat Intelligence (CTI)

Proces pozyskiwania i przetwarzania danych o zagrożeniach cybernetycznych (ang. Cyber Threat Intelligence, tłum. wywiad dotyczący zagrożeń

cybernetycznych) polega na systematycznym zbieraniu, analizie i udostępnianiu informacji o aktualnych i nadchodzących cyberzagrożeniach, które mogą dotknąć wszystkich w klastrze. Z perspektywy pojedynczego podmiotu śledzenie tego typu informacji jest mało realne – brakuje czasu, kompetencji analitycznych i dostępu do specjalistycznych źródeł. Dzięki modelowi współdzielonemu klaster może kupić dostęp do profesjonalnych źródeł CTI lub współpracować z partnerem, który będzie filtrował informacje i przekładał je na praktyczne rekomendacje dla członków. W efekcie organizacje nie dostają „lawiny technicznych alertów", tylko zrozumiałe komunikaty:

- jakie kampanie phishingowe właśnie krążą w ich sektorze,
- jakie podatności wymagają pilnej aktualizacji,
- jakie typy ataków są obserwowane w regionie i jak się na nie przygotować.

CTI może więc być radarem klastra, który pozwala wcześniej zobaczyć nadchodzące zagrożenia i zawczasu dostosować zabezpieczenia, zamiast reagować dopiero po incydencie.

5.5.3 Opracowanie wspólnego profilu zagrożeń

Wspólny profil zagrożeń stanowi opis najważniejszych ryzyk cybernetycznych charakterystycznych dla danego klastra, uwzględnia on branże jego członków, typowe procesy biznesowe, używane technologie oraz zależności w łańcuchu dostaw. Zamiast określania zagrożeń przez każdą organizację z osobna, klaster może wspólnie z ekspertami przygotować ujednolicony dokument pokazujący:

- które rodzaje ataków są najbardziej prawdopodobne,
- jakie mogą mieć skutki,
- jakie środki ochronne są priorytetem.

Dla MŚP i innych podmiotów stanowi to ogromne ułatwienie, ponieważ otrzymują one gotową mapę ryzyka dostosowaną do ich realiów, a nie ogólny katalog zagrożeń. W praktyce, profil zagrożeń może stanowić podstawę do planowania szkoleń, wspólnych ćwiczeń, zakupu narzędzi oraz wymagań wobec dostawców. Koordynator klastra aktualizuje taki dokument co najmniej raz w roku lub po istotnych zmianach technologicznych i regulacyjnych.

5.5.4 Doradztwo prawne

Obszar cyberbezpieczeństwa jest coraz mocniej regulowany, od RODO, przez NIS2 i sektorowe przepisy branżowe, aż po umowy z dostawcami IT i kwestie odpowiedzialności za incydenty. Pojedyncze MŚP rzadko ma dostęp do wyspecjalizowanego prawnika od zagadnień cyber i ochrony danych, a pojedyncze konsultacje bywają kosztowne. Klaster może negocjować wspólną usługę doradczą, np. ryczałtową pulę godzin miesięcznie u wyspecjalizowanej w tematyce kancelarii, z której usług członkowie będą korzystać na preferencyjnych warunkach. W takim modelu podmioty mogą uzyskać wsparcie przy przygotowaniu lub weryfikacji polityk bezpieczeństwa, umów z dostawcami IT, procedur reagowania na incydenty, czy realizacji obowiązków notyfikacyjnych, a koszt usługi rozkłada się na cały ekosystem. Koordynator może pełnić w tym podejściu rolę operatora usługi, zbierać typowe problemy, pomagać priorytetyzować tematy, a także dbać o tworzenie wspólnych wzorów dokumentów, które można następnie adaptować w poszczególnych organizacjach.

5.5.5 Obsługa incydentów

Profesjonalna obsługa incydentów (Incident Response) wymaga wiedzy technicznej, narzędzi śledczych i doświadczenia w zarządzaniu kry-

zysowym – zasobów, których większości MŚP brakuje. W modelu współdzielonym klaster może zapewnić swoim członkom dostęp do „grupy szybkiego reagowania" – zespołu specjalistów, który w razie ataku ransomware, wycieku danych czy przejęcia konta pomoże szybko opanować sytuację. W praktyce może to oznaczać potrzebę zawarcia stałej umowy z zewnętrznym zespołem specjalistów lub zbudowanie hybrydowego zespołu opartego o ekspertów podmiotów członkowskich. Kluczową wartością jest tu czas. Podmioty członkowskie nie muszą w panice szukać pomocy „na rynku"w momencie wystąpienia zagrożenia, ale korzystają z ustalonych wcześniej procedur, kontaktów i pakietów usług. Koordynator klastra może ponadto prowadzić rejestr incydentów (anonimizowany na poziomie raportów zbiorczych), co pozwala na wyciąganie wniosków dla całego ekosystemu i planowanie działań zapobiegawczych.

5.5.6 Licencja na szkolenia cyber i testy anty-phishingowe

Budowanie świadomości pracowników pozostaje jednym z najskuteczniejszych i jednocześnie najbardziej opłacalnych środków obrony przed atakami. Problemem MŚP jest jednak brak czasu na tworzenie własnych materiałów oraz wysokie koszty komercyjnych platform szkoleniowych. Klaster może negocjować wspólną licencję na sprawdzoną platformę do szkoleń z cyberbezpieczeństwa i testów anty-phishingowych oraz udostępnić ją podmiotom członkowskim w modelu „per użytkownik" lub w pakietach. Dzięki temu nawet małe przedsiębiorstwa zyskują dostęp do nowoczesnych, regularnie aktualizowanych treści i automatycznych kampanii phishingowych, które mierzą poziom czujności pracowników. Koordynator może dodatkowo przygotowywać wspólne harmonogramy kampanii (np. „miesiąc phishingu w klastrze") oraz raporty zbiorcze pokazujące postępy, oczywiście bez wskazywania wyników konkretnych podmiotów członkowskich.

5.5.7 EDR w pakiecie dla podmiotów członkowskich

Rozwiązania klasy EDR (Endpoint Detection and Response – nazwa rozwiązań, które stale monitorują i reagują na potencjalne cyberzagrożenia) to narzędzia monitorujące komputery i inne urządzenia końcowe w czasie zbliżonym do rzeczywistego, pozwalające wykrywać i blokować zaawansowane ataki, które omijają tradycyjne antywirusy. Dla wielu MŚP są one jednak zbyt drogie lub skomplikowane do samodzielnego wdrożenia i obsługi. Klaster może wynegocjować pakietową ofertę EDR dla swoich członków z uproszczoną konfiguracją, wspólnym wsparciem technicznym i lepszą ceną jednostkową. W bardziej zaawansowanym wariancie EDR może być zintegrowany ze wspólnym SOC, co pozwala na centralne monitorowanie zagrożeń i skoordynowaną reakcję. Taki model znacząco podniesie poziom ochrony w podmiotach członkowskich, a jednocześnie pozostanie osiągalny finansowo dzięki efektowi skali. Rolą koordynatora mogłoby być zebranie potrzeb, wybór dostawcy i wsparcie przy wdrożeniu minimalnych standardów.

5.5.8 Matchmaking, brokering z dostawcami rozwiązań cyber

Nie każda potrzeba cyberbezpieczeństwa musi być realizowana przez usługi współdzielone. Często chodzi o to, aby dany podmiot trafił do właściwego dostawcy, który naprawdę rozumie jego skalę i branżę. Koordynator klastra może pełnić rolę brokera i „matchmakera" między organizacjami członkowskimi a rynkiem rozwiązań cyber. Oznacza to m.in. prowadzenie „białej listy" zweryfikowanych dostawców, organizowanie dni

demo i sesji przeglądu rozwiązań, wspólne testy pilotażowe, a także wsparcie w negocjowaniu warunków umów. Dzięki temu podmioty klastrowe nie muszą samodzielnie przeczesywać rynku i oceniać setek ofert – korzystają z filtrowania i doświadczeń całego klastra. Taki model zmniejsza ryzyko wyboru nieodpowiedniego partnera, ogranicza zjawisko uzależnienia się od jednego dostawcy i wzmacnia pozycję negocjacyjną członków klastra, które mogą występować jako grupa, a nie pojedyncze podmioty.

Rozdział 6

Finansowanie działań z zakresu cyberbezpieczeństwa dla koordynatora klastra oraz podmiotów członkowskich

Efektywne funkcjonowanie klastra oraz rozwój jego członków w dążeniu do cyberodporności w dużej mierze zależą od dostępu do odpowiednich źródeł finansowania oraz umiejętnego wykorzystania dostępnych programów wsparcia. Dynamicznie zmieniające się otoczenie technologiczne i rosnące wymagania w zakresie cyberbezpieczeństwa wymagają stabilnych, dobrze zaplanowanych mechanizmów inwestycyjnych, które umożliwią rozwój kompetencji, wdrażanie innowacji oraz wypracowywanie przewag konkurencyjnych bazujących na cyberodporności organizacji.

Celem niniejszego rozdziału jest przedstawienie kompleksowego przeglądu obecnych i przyszłych krajowych i europejskich instrumentów finansowania, wraz ze wskazaniem potencjalnych korzyści dla członków. Ponadto w rozdziale przedstawiono kompleksowe zestawienie usług świadczonych w Polsce z ramienia EDIHów (European Digital Innovation Hub – więcej w rozdziale 6.2) oraz możliwości skorzystania z usług dofinansowanych ze środków publicznych przez członków klastra.

Zebrane informacje mają na celu umożliwić koordynatorom klastrów oraz ich członkom świadome planowanie rozwoju z wykorzystaniem dostępnych środków na rozwój cyberbezpieczeństwa.

6.1 Źródła finansowania cyberodporności członków klastra

W poniższym rozdziale przedstawiono różne rodzaje dostępnych programów, z których członkowie klastra mogą korzystać w celu zwiększenia swojej cyberodporności. Głównym zadaniem koordynatora klastra powinno być śledzenie programów konkursowych oraz wybieranie takich, z których mogą skorzystać członkowie klastra. Usługi doradcze i konsultacyjne związane z możliwościami skorzystania z funduszy publicznych są wysoce cenione przez członków klastra.

6.1.1. Fundusze unijne w obecnej perspektywie – FENG oraz FERC

Od 2021 r. w Unii Europejskiej działa nowa perspektywa finansowa na lata 2021-2027. Jednym z jej programów jest FENG, który oferuję szerokie formy wsparcia dla firm z różnych branż i regionów. Program ten ma przede wszystkim pomagać przedsiębiorstwom w realizacji nowatorskich projektów i rozwoju nowych technologii.

Fundusze Europejskie dla Nowoczesnej Gospodarki (FENG)

W lutym 2023 r. rozpoczął się nabór do programu FENG, który jest kontynuacją wcześniejszych Programów Operacyjnych: Innowacyjna Gospodarka 2007-2013 oraz Inteligentny Rozwój 2014-2020. FENG ma na celu:

- wzmacnianie potencjału firm w obszarze badań, innowacji i nowoczesnych technologii,
- zwiększenie konkurencyjności małych i średnich przedsiębiorstw,
- rozwój umiejętności związanych z inteligentnymi specjalizacjami i transformacją przemysłową,
- wspieranie Przemysłu 4.0 i ekologicznych technologii.

Budżet FENG to ok. 10 mld euro. Środki te są przekazywane w formie dotacji, pożyczek, inwestycji kapitałowych, gwarancji finansowych lub mieszanego wsparcia, łączącego dotacje i finansowanie zwrotne. O dofinansowanie mogą ubiegać się firmy, jednostki naukowe, konsorcja oraz partnerstwa firm z organizacjami badawczymi lub instytucjami wspierającymi biznes. Dofinansowania w ramach FENG są zatem szeroko dostępne dla firm zrzeszonych w klastrze.

W ramach programu dostępna jest m.in. Ścieżka SMART, której założeniem jest realizacja modułu obligatoryjnego we wniosku obejmującego:

- **Moduł B+R** na realizację prac badawczo-rozwojowych prowadzących do wytworzenia innowacji produktowej lub procesowej w skali kraju.

- **Moduł wdrożenia innowacji** obejmujący wdrożenie w przedsiębiorstwie wyników prac B+R, zrealizowanych przez wnioskodawcę lub będących efektem realizacji komponentu B+R. Wyniki działań B+R muszą zakończyć się wprowadzeniem innowacji produktowej lub procesowej co najmniej na poziomie krajowym.

Po spełnieniu wymagań obligatoryjnych wnioskodawca może uzyskać dodatkowo wsparcie w ramach jednego z pięciu modułów fakultatywnych. Jednym z nich jest wsparcie na cyfryzację przedsiębiorstwa, w tym na działania związane z transformacją cyfrową i np. wdrożenie rozwiązań z zakresu cyberbezpieczeństwa. Kolejne nabory w ramach Ścieżki SMART odbędą się[79]:

- w lutym oraz IV kwartale 2026 dla pojedynczych MŚP,
- w marcu oraz III kwartale dla konsorcjów przedsiębiorstw wraz z organizacjami badawczymi lub NGO.

Ścieżka SMART pomimo tego, iż nie jest dedykowana zwiększeniu poziomu cyberbezpieczeństwa w organizacjach, poprzez posiadanie komponentu fakultatywnego, może wpłynąć skutecznie na jego zwiększenie. Bieżące informacje nt. aktualnych projektów w ramach FENG można znaleźć na stronie: https://www.nowoczesnagospodarka.gov.pl/.

Kolejnym działaniem w ramach FENG, w którym klastry mogą zwiększyć poziom cyberbezpieczeństwa swoich podmiotów członkowskich jest działanie 2.17 – rozwój oferty klastrów dla firm. Celem działania jest rozwój innowacyjnej oferty usługowej dla podmiotów członkowskich w zakresie B+R+I świadczonej przez koordynatora klastra, w obszarach takich jak transformacja cyfrowa, gospodarka obiegu zamkniętego, gospodarka niskoemisyjna czy nowoczesna edukacja. Przykładowe usługi, które mogłyby zostać uwzględnione we wniosku wskazano w rozdziale 5. Z dofinansowania mogą skorzystać koordynatorzy Krajowych Klastrów Kluczowych (KKK) oraz Ponadregionalnych Klastrów Wzrostowych (PKW). Kolejny nabór w ramach działania 2.17 zaplanowany jest na luty 2026[80].

W FENG zaplanowano także kolejne nabory w działaniu 5.1 – fundusz wsparcia technologii krytycznych. Jest to działanie nakierowane na wsparcie projektów przedsiębiorców realizujących inicjatywy w ramach STEP (Platformy na rzecz Technologii Strategicznych dla Europy). Nabory będą dedykowane przedsiębiorstwom, konsorcjom przedsiębiorców, w tym z organizacjami badawczymi lub NGO. Nabory odbędą się w maju oraz czerwcu 2026[81]. Program zostanie podzielony na dwie ścieżki:

- **Ścieżka A** – innowacyjne technologie krytyczne, której celem jest realizacja innowacyjnego, najnowocześniejszego lub przełomowego elementu o znaczącym potencjale gospodarczym. Do realizacji wniosku należy spełnić co najmniej 2 z 3 warunków.

- **Ścieżka B** – strategiczna niezależność UE, której celem jest ograniczenie lub zwalczenie

79 Portal informacyjny dotyczący Funduszy Europejskich dla Nowoczesnej Gospodarki. Dostęp: https://www.nowoczesnagospodarka.gov.pl/. (20 listopada 2025)

80 Strona informacyjna archiwalnego naboru do konkursu „Rozwój oferty klastrów dla firm – nabór dla koordynatorów Krajowych Klastrów Kluczowych" (2025). Dostęp: https://www.parp.gov.pl/component/grants/grants/rozwoj-oferty-klastrow-dla-firm-nabor-dla-koordynatorow-krajowych-klastrow-kluczowych. (28 listopada 2025)

81 Tamże.

strategicznej zależności UE. Projekt w Ścieżce B powinien przyczyniać się do uzyskania czołowej pozycji Unii w dziedzinie przemysłu i technologii, wnieść wkład w infrastrukturę krytyczną na szczeblu europejskim, zwiększyć zdolności produkcyjne i bezpieczeństwo dostaw lub korzystnie wpłynąć na rynek wewnętrzny. Do realizacji wniosku należy spełnić co najmniej 2 z 5 warunków.

W projekcie STEP wprost wskazano projekty z zakresu cyberbezpieczeństwa jako jedne z głównych technologii cyfrowych w komponencie DIGITAL[82]. Ze środków FENG działają także takie programy jak:

1. **Kredyt technologiczny** – dotacja dla przedsiębiorstw sektora MŚP, które wdrażają innowacyjną technologię i na jej podstawie rozpoczynają produkcję towarów lub świadczenie usług. W ramach kredytu można wdrożyć innowacje technologiczne, których celem jest rozpoczęcie produkcji towarów / świadczenia usług, które są nowe lub znacząco ulepszone na podstawie. Zrealizować można to poprzez zakup i wdrożenie nowej technologii lub wdrożenie własnej nowej technologii[83].

2. **DIG.IT** – projekt skierowany do MŚP z sektora przetwórstwa przemysłowego oraz usług produkcyjnych. Jego celem jest wsparcie wdrażania nowoczesnych technologii cyfrowych w procesach wytwórczych, automatyzacji procesów, a także implementacji rozwiązań opartych na big data, sztucznej inteligencji i cyberbezpieczeństwie. W ramach dofinansowania firmy mogą otrzymać od 150 000–850 000 zł

w formie pomocy de minimis, co stanowi 50% kosztów kwalifikowanych w projekcie. Przedsiębiorcy mogą w ramach projektu nabyć i wdrożyć gotowe technologie cyfrowe lub zlecić wykonanie prac programistycznych w celu opracowania danej technologii[84].

6.1.2 Digital Europe Programme (DEP)

DEP to unijny program finansowania na lata 2021–2027, który ma na celu przyspieszenie wdrażania dojrzałych technologii cyfrowych w Europie oraz wspieranie transformacji cyfrowej gospodarek i społeczeństw UE. Jednymi z głównych filarów wspieranych przez program są aspekty m.in. cyberbezpieczeństwa i zaawansowanych kompetencji cyfrowych, czy wsparcia użycia technologii cyfrowych w gospodarce i społeczeństwie[85]. Cyberbezpieczeństwo jest jednym z głównych obszarów w Digital Europe. W ramach programu finansowane jest m.in:

82 Portal informacyjny Inicjatywy STEP. Dostęp: https://www.parp.gov.pl/component/site/site/step#konkursy. (26 listopada 2025)
83 Portal informacyjny dotyczący Kredytu Technologicznego. Dostęp: https://www.bgk.pl/produkty/kredyt-technologiczny/. (20 listopada 2025)
84 Portal informacyjny archiwalnego naboru do konkursu „Dig.IT". Dostęp: https://digit.arp.pl/. (20 listopada 2025)
85 Portal informacyjny Programu „Cyfrowa Europa". Dostęp: https://digital-strategy.ec.europa.eu/pl/activities/digital-programme. (20 listopada 2025)

Europejskie Centrum Kompetencji Cyberbezpieczeństwa (ECCC), które odpowiada za zarządzanie znaczną częścią działań DEP w obszarze cyberbezpieczeństwa[86]. W programie prac ECCC na lata 2025–2027 zapowiedziano inwestycje na ok. 390 mln euro w projekty cyberbezpieczeństwa. ECCC na lata 2026-2027 zaplanowało kilka konkursów dedykowanych dla MŚP[87]:

- Wzmacnianie zdolności cyberbezpieczeństwa europejskich MŚP z wykorzystaniem cyberbezpiecznych rozwiązań AI („Strengthening cybersecurity capacities of European SMEs with cybersecure AI-powered solutions"). Program ma zwiększyć odporność cyfrową europejskich MŚP poprzez rozwój i wdrażanie innowacyjnych opartych na sztucznej inteligencji narzędzi cyberbezpieczeństwa. Jego celem jest automatyzacja kluczowych procesów bezpieczeństwa (ocena ryzyka, wykrywanie zagrożeń, reagowania na incydenty), wspieranie przyjmowania zaawansowanych technologii przez firmy o ograniczonych zasobach oraz poprawa przygotowania organizacji do cyberataków. Program kierowany jest dla MŚP, startupów, jednostek badawczych i akademickich, podmiotów objętych dyrektywą NIS2 oraz sektora publicznego. Nabór planowany jest na 2026 rok.

- Wdrażanie innowacyjnych rozwiązań z zakresu cyberbezpieczeństwa dla MŚP („Uptake of innovative cybersecurity solutions for SMEs"). Program ma zwiększyć gotowość rynkową i technologiczną MŚP do spełnienia wymogów europejskich regulacji cyberbezpieczeństwa (m.in. Cyber Resilience Act, NIS2, Cybersecurity Act). Ma zapewnić dostęp do innowacyjnych narzędzi wspierających zgodność z prawem, raportowanie incydentów, poprawę bezpieczeństwa sieci i systemów oraz zwiększenie odporności łańcucha dostaw. Program dedykowany jest dla MŚP, podmiotów publicznych i prywatnych wdrażających NIS2 i Cyber Resilience Act oraz jednostek naukowo-badawczych. Program zaplanowano na 2027 rok.

ECCC zostało także głównym operatorem konkursów ze środków z programu Horyzont Europa. Zgodnie z programem roboczym, wszystkie działania związane z celem „Increased Cybersecurity" będą przekazywane do realizacji przez ECCC. Na 2026 rok w ramach programu zaplanowano 4 konkursy[88]:

1. Approaches and tools for security in software and hardware development and assessment (including open source).
2. Enhancing the Security and Robustness of AI Models and Systems (SecureAI).
3. Post-quantum cryptography RIA.
4. Emerging challenges: Human aspects of Cybersecurity.

Na 2027 rok zostały zaplanowane takie konkursy jak:

1. AI for Cybersecurity applications.
2. Privacy Enhancing Technologies.
3. Secure Computing Continuum (IoT, Edge, Cloud, Dataspaces).

86 Directorate-General for Communications Networks, Content and Technology, (2025) „ECCC to finance EUR 390 million in cybersecurity projects under Digital Europe Programme for 2025-2027". Dostęp: https://cybersecurity-centre.europa.eu/news/eccc-finance-eur-390-million-cybersecurity-projects-under-digital-europe-programme-2025-2027-2025-03-28_en. (26 listopada 2025)

87 Portal informacyjny Programu „Cyfrowa Europa". Dostęp: https://digital-strategy.ec.europa.eu/en/activities/work-programmes-digital. (26 listopada 2025)

88 Horizon Europe – Work Programme 2026-2027 Civil Security for Society. Dostęp: https://sciencebusiness.net/sites/default/files/inline-files/HORIZON-CL3-2026-2027_02_13_2025_draft_v1.pdf?utm. (4 grudnia 2025)

4. Emerging challenges: Human aspects of Cybersecurity.
5. Post-quantum cryptography.

W celu śledzenia programów oraz bieżącego kontaktu odnośnie do możliwości w ramach DEP oraz programu Horyzont Europa, koordynator klastra powinien nawiązać relację z lokalnym instytucją działającą w ramach ECCC – w tym przypadku NCC-PL (Krajowe Centrum Kompetencji Cyberbezpieczeństwa). NCC-PL odpowiedzialne jest za budowanie potencjału krajowego w dziedzinie cyberbezpieczeństwa, w tym obsługę i wsparcie w ramach programów realizowanych w ramach DEP.

6.1.3. Krajowy Plan Odbudowy (KPO)

W zatwierdzonym przez Komisję Europejską polskim Planie Odbudowy (KPO) uwzględniono działania mające na celu zwiększenie cyberodporności Polski. Zakładają one wsparcie transformacji cyfrowej oraz podnoszenie poziomu cyberbezpieczeństwa. Jednym z zaplanowanych przedsięwzięć jest Projekt Funduszu Bezpieczeństwa i Obronności (FBiO), który obejmuje m.in. inwestycje w cyberbezpieczeństwo. Na ten cel przewidziano około 2,46 mld zł, które zostaną przeznaczone na zwiększenie bezpieczeństwa i niezawodności infrastruktury cyfrowej odpowiedzialnej za gromadzenie danych oraz wspieranie zarządzania kluczowymi elementami otoczenia, takimi jak: systemy ujęć wody, instalacje kanalizacyjne, transport publiczny, sieci energetyczne i paliwowe. Pierwsze nabory w ramach tego projektu planowane są na drugą połowę 2026 roku[89].

Zakres konkursów ani dokładny harmonogram FBiO nie zostały jeszcze doprecyzowane. Bazując na poprzednich konkursach z zakresu cyberbezpieczeństwa realizowanych ze środków z KPO tj.: Cyberbezpieczny Rząd[90], Cyberbezpieczny Samorząd[91] oraz Cyberbezpieczne Wodociągi[92], oraz biorąc pod uwagę aktualne zapisy wydatkowania środków, można założyć bardzo podobną grupę docelową podmiotów, które otrzymają dofinansowanie. Zaleca się zatem bieżące śledzenie konkursów w ramach KPO, ze względu na możliwość wykorzystania tych środków ze strony podmiotów członkowskich.

6.1.4 Regionalne Programy Operacyjne (RPO)

Regionalny Program Operacyjny jest to dokument planistyczny określający działania oraz obszary ich podejmowania, jakie organy samorządu województwa podejmują lub mają zamiar podjąć na rzecz wspierania rozwoju województwa lub regionu. W Polsce każde województwo posiada swoje dedykowane RPO dostosowane do lokalnych potrzeb. W wielu przypadkach w ramach finansowania realizowane są projekty związane ze zwiększaniem cyberodporności lokalnych przedsiębiorstw oraz instytucji. Kompleksową mapę dotacji w Polsce z uwzględnieniem lokalnych RPO można znaleźć na stronie: https://mapadotacji.gov.pl/. Dobrą praktyką ze strony koordynatora klastra

89 Portal informacyjny o Krajowym Planie Odbudowy, Aktualności, [artykuł online]. Dostęp: https://www.kpo.gov.pl/strony/aktualnosci/projekt-ustawy-o-funduszu-bezpieczenstwa-i-obronnosci-fbio-w-sejmie/. (20 listopada 2025)

90 Centrum Projektów Polska Cyfrowa, Ogłoszenie naboru do działania: „Inwestycja C3.1.1. Konkurs Grantowy–Cyberbezpieczny Rząd". Dostęp: https://www.gov.pl/web/cppc/inwestycja-c-311-konkurs-grantowy-cyberbezpieczny-rzad. (20 listopada 2025)

91 Centrum Projektów Polska Cyfrowa, Ogłoszenie naboru do działania: „Cyberbezpieczny Samorząd". Dostęp: https://www.gov.pl/web/cppc/cyberbezpieczny-samorzad. (20 listopada 2025)

92 Serwis Rzeczpospolitej Polskiej, „Cyberbezpieczny Wodociąg założenia nowego konkursu grantowego ze środków KPO" [artykuł online]. Dostęp: https://www.gov.pl/web/baza-wiedzy/cyberbezpieczny-wodociag-zalozenia-nowego-konkursu-grantowego-ze-srodkow-kpo. (20 listopada 2025)

jest śledzenie lokalnych dofinansowań oraz nawiązanie relacji z jednostką ich udzielających w celu sprawnej wymiany informacji o planowanych inicjatywach.

6.1.5 Lista sprawdzająca dofinansowania z zakresu cyberbezpieczeństwa

Wartościową usługą dla członków klastra ze strony koordynatorów jest bieżące śledzenie możliwości poszczególnych programów finansowania oraz przekazywanie informacji członkom klastrów. Podmioty członkowskie ze względu na ilość obowiązków, nie śledzą na bieżąco wszystkich dostępnych programów, zatem wsparcie w tym zakresie ze strony koordynatora klastra może być kluczowe. Pomocnym narzędziem może być lista sprawdzająca do cyklicznego sprawdzania dofinansowań:

- Sprawdzenie aktualnych konkursów na stronie FENG: https://www.nowoczesnagospodarka.gov.pl/.
- Sprawdzenie aktualnych konkursów na stronie KPO: https://www.kpo.gov.pl/strony/o-kpo/wsparcie/nabory-dla-przedsiebiorcow/#target_12.
- Sprawdzenie aktualnych konkursów w ramach RPO: https://mapadotacji.gov.pl/.
- Sprawdzenie aktualnych konkursów na stronie Centrum Projektów Polska Cyfrowa (uwzględnia także nabory w ramach DEP z zakresu cyberbezpieczeństwa): https://www.gov.pl/web/cppc/cppc-nabory.
- Sprawdzenie aktualnych konkursów na stronie PARP: https://www.parp.gov.pl/component/grants/grantss?sort=default&term%5B%5D=1&term%5B%5D=2&text_search=.
- Sprawdzenie Social Mediów organizacji promujących oraz realizujących programy wsparcia:
  - PARP – https://www.linkedin.com/company/polska-agencja-rozwoju-przedsiebiorczosci/posts/?feedView=all,
  - PFR – https://www.linkedin.com/company/pfr/posts/?feedView=all,
  - ARP – https://www.linkedin.com/company/agencja-rozwoju-przemyslu/,
  - CPPC – https://www.linkedin.com/company/centrum-projekt%C3%B3w-polska-cyfrowa/posts/?feedView=all,
  - NCC-PL – https://www.linkedin.com/company/ncc-pl/posts/?feedView=all,
  - ECCC – https://www.linkedin.com/company/cybersec-eccc/posts/?feedView=all,
  - BGK – https://www.linkedin.com/company/bank-gospodarstwa-krajowego/posts/?feedView=all.

6.2. Sposoby finansowania cyberodporności poprzez współpracę podmiotów członkowskich oraz współpracę z European Digital Innovation Hubs (EDIH)

Współpraca pomiędzy podmiotami członkowskimi uwzględniająca wspólne finansowanie działań z zakresu cyberbezpieczeństwa oraz wykorzystywanie aktualnie dostępnych darmowych narzędzi może wnieść znaczące korzyści do działań całego klastra. W poniższym podrozdziale omówiono dwa główne podejścia do finansowania cyberodporności: współpraca podmiotów członkowskich w ramach klastra oraz współpraca z EDIHami, które w Polsce oferują szeroką gamę usług wspierających bezpieczeństwo cyfrowe przedsiębiorstw.

6.2.1 Współpraca podmiotów członkowskich w celu wspólnego finansowania usług cyberbezpieczeństwa

Przedsiębiorstwa coraz częściej poszukują efektywnych metod zwiększania swojej cyberodporności przy jednoczesnym ograniczeniu kosztów. Jednym z efektywnych rozwiązań jest współpraca podmiotów członkowskich w ramach klastra

w celu wspólnego finansowania usług związanych z cyberbezpieczeństwem.

Model ten opiera się na utworzeniu wspólnego budżetu, z którego środki przeznaczane są na realizację działań mających na celu podniesienie poziomu bezpieczeństwa cyfrowego wszystkich podmiotów działających przy tym projekcie. Budżet taki może być zasilany proporcjonalnie do wielkości firmy, zakresu korzystania z usług lub innych uzgodnionych kryteriów, co pozwala na sprawiedliwy podział kosztów i zapewnia dostęp do wysokiej jakości usług nawet dla mniejszych podmiotów. Zalecanym rozwiązaniem jest równomierny podział kosztów oraz umożliwienie z korzystania z danej usługi dla każdego zaangażowanego podmiotu w tym samym stopniu.

Koordynator klastra odgrywa w tym modelu kluczową rolę. Jego zadaniem jest zarówno zarządzanie wspólnym budżetem, jak i koordynacja realizacji usług cyberbezpieczeństwa dla członków klastra zaangażowanych w dany projekt. Przykładowe pomysły usług, które mogłyby być współfinansowane w ramach klastra wskazano w rozdziale 5. Natomiast w rozdziale 8 wskazano przykładowe struktury oraz modele współpracy.

Taki model współpracy pozwala nie tylko obniżyć koszty jednostkowe usług cyberbezpieczeństwa, ale również buduje spójny system ochrony w całym klastrze. Wspólne finansowanie usług w ramach klastra staje się zatem zarówno narzędziem optymalizacji kosztów, jak i sposobem systemowego podnoszenia cyberodporności uczestniczących podmiotów.

Dodatkowo podmioty członkowskie w celu optymalizacji budżetu powinny korzystać z darmowych usług i szkoleń dostępnych na rynku jak np.:

- Akademia PARP, która oferuje liczne szkolenia, w tym z zakresu cyberbezpieczeństwa[93],
- szkolenia realizowane przez Ministerstwo Cyfryzacji z zakresu cyberbezpieczeństwa dla podmiotów krajowego systemy cyberbezpieczeństwa[94].

6.2.2 Współpraca podmiotów członkowskich z European Digital Innovation Hubs

EDIHy są ośrodkami wspierającymi MŚP oraz administrację publiczną w procesie transformacji cyfrowej. Ich zadaniem jest ułatwienie wdrażania nowych technologii takich, jak np. AI, cyberbezpieczeństwo, automatyzacja czy rozwiązań chmurowych poprzez[95]:

- doradztwo technologiczne,
- testowanie rozwiązań typu test before invest,
- szkolenia i podnoszenie kompetencji cyfrowych,
- wsparcie w pozyskiwaniu finansowania,
- łączenie firm z ekosystemem innowacji.

EDIHy świadczą usługi na podstawie pomocy de minimis dla mikro, małych i średnich przedsiębiorstw. Duże przedsiębiorstwa mogą skorzystać z usług odpłatnie, zgodnie z cennikiem zaproponowanym w projekcie. Wszystkie EDIHy w Europie tworzą wspólną sieć, której celem jest jak najlepsze dopasowanie danej usługi pod oczekiwania przedsiębiorcy. Zgłaszając zatem potrzeby do lokalnego EDIHa, w momencie, kiedy nie jest

93 Polska Agencja Rozwoju Przedsiębiorczości, Kursy online. Dostęp: https://www.parp.gov.pl/component/site/site/kursy-online. (28 listopada 2025)

94 Serwis Rzeczypospolitej Polskiej, „Informacja o szkoleniach dla podmiotów krajowego systemu cyberbezpieczeństwa" [artykuł online]. Dostęp: https://www.gov.pl/web/baza-wiedzy/harmonogramszkolen. (28 listopada 2025)

95 Krajowe Centrum Kompetencji Cyberbezpieczeństwa, „Europejskie huby innowacji cyfrowych (European Digital Innovation Hub, EDIH)" [artykuł online]. Dostęp: https://www.gov.pl/web/cyber-nccpl/europejskie-huby-innowacji-cyfrowych-european-digital-innovation-hub-edih. (20 listopada 2025)

on w stanie wyświadczyć wskazanej usługi, dana firma zostanie przekierowana do innego regionalnego lub nawet zagranicznego EDIHa w celu wyświadczenia poszukiwanej usługi[96].

Dla koordynatorów klastrów EDIHy są idealnymi partnerami, gdyż we współpracy z nimi mogą oferować swoim członkom dostęp do wyspecjalizowanych usług z zakresu cyberbezpieczeństwa (oraz wielu innych podnoszących poziom cyfryzacji danej organizacji). Współpraca na linii koordynator klastra–EDIH pozwala stworzyć efektywny system wsparcia członków i ich cyberodporności oraz w sposób bezkosztowy (na podstawie pomocy de minimis), wesprzeć daną organizację.

Z uwagi na powyższe informacje zaleca się, aby każdy koordynator klastra był w bieżącym kontakcie z co najmniej jednym lokalnym EDIHem w celu ułatwiania dostępu do usług EDIH swoich członkom.

W Polsce powstało 7 EDIHów, które mają w swojej ofercie usługi z zakresu cyberbezpieczeństwa:

EDIH Cybersec jest specjalistycznym EDIHem skupionym jedynie na usługach z zakresu cyberbezpieczeństwa. W projekcie świadczone są takie usługi jak[97]:

- audyt w obszarze bezpieczeństwa teleinformatycznego,
- techniczna ocena cyberbezpieczeństwa,
- test penetracyjny infrastruktury sieciowej,
- audyt bezpieczeństwa aplikacji mobilnej,
- rekomendacje inwestycyjne podnoszące poziom dojrzałości cyberbezpieczeństwa,
- ocena stanu bezpieczeństwa sieci przemysłowych (e-audyt infrastruktury IT),
- wdrożenie testowe systemu monitorowania sieci przemysłowych,
- SOC ad hoc,
- wsparcie procesów zarządczych,
- implementacja systemów zarządzania bezpieczeństwem informacji oraz infrastrukturą IT,
- warsztaty z Inwentaryzacji zasobów IT,
- szkolenia audytorów,
- pakiet konsultacji eksperckich oraz audyty, ciągłe doskonalenie systemów zarządzania,
- wdrożenie i doskonalenie RODO,
- usługi przetwarzania informacji niejawnych,
- szkolenie z ochrony przed atakami socjotechnicznymi,
- budowanie świadomości i szkolenia w zakresie cyberbezpieczeństwa oraz bezpieczeństwa informacji,
- implementacja bezpiecznego cyklu życia oprogramowania,
- szkolenie z bezpiecznego programowania,
- poligon cybernetyczny CDeX,
- wirtualne Laboratorium Testowe.

EDIH hub4industry jest EDIHem nakierowanym na firmy przemysłowe, które chcą wprowadzić do swoich fabryk rozwiązania przemysłu 4.0. W projekcie świadczone są usługi z zakresu cyberbezpieczeństwa takie, jak[98]:

- audyt i doradztwo w zakresie zaprojektowania i wykorzystania bezpiecznych sieci kampusowych,
- analizy i audyty cyberbezpieczeństwa sieci IT,
- analizy i audyty cyberbezpieczeństwa sieci teleinformatycznych (sieci przemysłowe LAN/WAN, SDN i OT),
- PoC w zakresie audytu bezpieczeństwa sieci teleinformatycznej i używanych aplikacji,

96 Polska Agencja Rozwoju Przedsiębiorczości, „Europejskie Centra Innowacji Cyfrowych (EDIH)" [artykuł online]. Dostęp: https://www.parp.gov.pl/component/site/site/edih#mapa. (28 listopada 2025)
97 Strona informacyjna dotycząca EDIH-u Cybersec. Dostęp: https://cyber-sec.net.pl. (21 listopada 2025)
98 Strona informacyjna dotycząca EDIH-u Hub4Industry. Dostęp: https://hub4industry.pl/. (21 listopada 2025)

- wdrożenie testowe rozwiązań SD-LAN/WAN – Next-gen Connectivity,
- wdrożenie testowe sieci IT/OT/Cybersec.

EDIH Silesia Smart Systems – wspiera przedsiębiorstwa przemysłowe, które chcą przeprowadzić transformację cyfrową z wykorzystaniem technologii Przemysłu 4.0 lub rozważają zmianę modelu biznesu i wdrożenie inteligentnych produktów z wykorzystaniem technologii cyfrowych. W projekcie świadczone są takie usługi z zakresu cyberbezpieczeństwa, jak[99]:

- praktyczne warsztaty z zakresu silnego uwierzytelniania ze szczególnym uwzględnieniem metod i systemów biometrycznych,
- testowanie jakości transmisji danych w cyfrowych systemach komunikacji bezprzewodowej w symulowanym środowisku elektromagnetycznym,
- ochrona stacji końcowych zgodnie z NIS 2,
- dedykowany proces zarządzania podatnościami zgodnie z NIS 2,
- pierwsze kroki po certyfikat Common Criteria dla własnego produktu informatycznego – szkolenie.

EDIH WRO4digITal to EDIH utworzony przez konsorcjum 22 instytucji oferujących kompleksowe wsparcie w procesie transformacji cyfrowej. W projekcie świadczone są takie usługi z zakresu cyberbezpieczeństwa takie, jak[100]:

- szkolenie Security Awareness – bezpieczny pracownik, bezpieczna firma,
- cyberbezpieczny pracownik – praktyczne przygotowanie uczestników do rozpoznawania i reagowania na zagrożenia IT,
- cyberbezpieczne rozwiązania – jak je projektować i utrzymywać?,
- jak rozpoznać hakera? Metody obrony przed cyberatakami,
- bezpieczna firma – wprowadzenie do zarządzania cyberbezpieczeństwem,
- jak zwiększyć poziom dojrzałości swojego Systemu Zarządzania Bezpieczeństwem Informacji? Szkolenie z zakresu cyberbezpieczeństwa,
- audyt bezpieczeństwa infrastruktury, aplikacji internetowej,
- audyt poziomu dojrzałości firmy w obszarze wdrożonych środków bezpieczeństwa przed cyberzagrożeniami,
- audyt bezpieczeństwa cybernetycznego,
- analiza procesowa w zakresie RODO dla MŚP,
- dedykowany program świadomości cybernetycznej.

Re_d-rethink digital hub EDIH – koordynowany przez Łódzką Specjalną Strefę Ekonomiczną. W projekcie świadczone są takie usługi z zakresu cyberbezpieczeństwa, jak[101]:

- cyberbezpieczeństwo i nowe technologie dla MŚP,
- bezpieczne technologie przyszłości z uwzględnieniem cyfrowej transformacji,
- cybersecurity 4.0. Venture Building,
- AI & Data Driven Identity and Access Management,
- e-audyt cyberbezpieczeństwa dla infrastruktury.

Technopark Kielce Digital Innovation Hub. Grupą docelową TKDIH są przedsiębiorstwa z województwa świętokrzyskiego, należące do sektora MŚP z branż zgodnych ze specjalizacjami Regionalnej Strategii Innowacji Województwa Świę-

99 Strona informacyjna dotycząca EDIH-u Silesian Smart Systems. Dostęp: https://www.silesiasmartsystems.pl/start--3836?lang_id=10. (21.11.2025)

100 Strona informacyjna dotycząca EDIH-u Wro4digITal. Dostęp: https://www.technologpark.pl/edih/. (21 listopada 2025)

101 Strona informacyjna dotycząca EDIH-u rethink digital hub. Dostęp: https://re-d.pl/#uslugi. (21 listopada 2025)

tokrzyskiego. W projekcie świadczone są takie usługi z zakresu cyberbezpieczeństwa, jak:

- analiza w zakresie cyberbezpieczeństwa.

WAMA EDIH – głównym celem projektu jest wzrost konkurencyjności polskich, lokalnych firm (ze szczególnym uwzględnieniem MŚP zlokalizowanych w województwie warmińsko-mazurskim i mazowieckim). W projekcie świadczone są takie usługi z zakresu cyberbezpieczeństwa, jak[102]:

- Network Sentinel (monitorowanie ruchu sieciowego w systemach automatyki przemysłowej),
- CyberLab – rekomendacje zwiększające cyberbezpieczeństwo.

102 Strona informacyjna dotycząca EDIH-u Koalicja dla Innowacji. Dostęp: https://koalicjadlainnowacji.pl/wama-edih/wyszukiwarka-uslug/. (21 listopada 2025)

Rozdział 7

Działania zbiorowe i budowanie odporności cyfrowej klastra jako całości

Sama wiedza teoretyczna o zagrożeniach i regulacjach prawnych cyberbezpieczeństwa nie wystarczy, by zabezpieczyć ekosystem klastra przed realnym atakiem. Odporność cyfrowa (ang. cyber resilience) nie jest stanem, lecz ciągłym procesem, który wymaga planowania, regularnego sprawdzania gotowości oraz aktywnej współpracy. Tylko takie podejście pozwoli utrzymać zdolność organizacji do nieprzerwanego działania w obliczu zagrożeń cyfrowych.

W niniejszym rozdziale przedstawiamy, jak koordynator klastra może stworzyć prostą, lecz skuteczną strategię bezpieczeństwa, organizować ćwiczenia symulacyjne oraz jak wykorzystać potencjał sieciowania do wymiany doświadczeń z innymi klastrami.

7.1 Tworzenie strategii odporności cyfrowej klastra

Stworzenie strategii odporności cyfrowej klastra nie musi oznaczać setek stron dokumentacji ani korzystania z kosztownego wsparcia doradców. Jest to mit, który często paraliżuje działania, ponieważ w rzeczywistości, dla organizacji takich jak klaster wystarczy jasna, zrozumiała i możliwa do wdrożenia strategia, która będzie drogowskazem, a nie biurokratycznym obciążeniem. Skuteczna strategia odporności cyfrowej powinna opierać się na czterech filarach:

- misji,
- celach,
- miernikach,
- partnerstwach.

Taki dokument powinien chronić zasoby klastra, utrzymać ciągłość działania, reputację i konkurencyjność. Jasny plan sprzyja lepszej komunikacji oraz umożliwia ocenę działań z perspektywy całego ekosystemu klastra, co jest kluczowe w obliczu rosnącej liczby ataków na podmioty gospodarcze.

Choć w polskich i zagranicznych klastrach trudno znaleźć gotowe przykłady takich strategii, w tym podręczniku przedstawiamy propozycję, która może stać się inspiracją do stworzenia dokumentu dostosowanego do potrzeb konkretnego klastra.

7.1.1 Misja

Strategia musi zaczynać się od odpowiedzi na pytanie „dlaczego?". Dla klastra, misją w obszarze cyberbezpieczeństwa nie jest „ochrona serwerów", ale zapewnienie ciągłości biznesowej i budowanie zaufania w łańcuchu wartości. Przykładowy zapis misji może brzmieć: „Celem strategii jest stworzenie środowiska, w którym członkowie klastra mogą bezpiecznie wymieniać dane i realizować wspólne projekty, minimalizując ryzyko przestojów operacyjnych spowodowanych incydentami cyfrowymi". Tak jak w powyższym przykładzie misja może koncentrować się na zapewnieniu bezpieczeństwa ekosystemu, wsparciu członków Klastra, czy stworzeniu bezpiecznego środowiska wymiany wiedzy i najlepszych praktyk.

7.1.2 Cele strategiczne i operacyjne

Aby strategia nie pozostała martwym dokumentem, koordynator powinien podzielić cele na dwa poziomy: strategiczny (długoterminowy, określający kierunek na 2-3 lata) oraz operacyjny (krótkoterminowy, konkretne zadania na najbliższe np. 12 miesięcy). Poniżej przedstawiamy przykładowy zestaw celów, który jest uniwersalny dla większości klastrów, niezależnie od branży i opiera się na budowaniu podstawowej higieny cyfrowej.

- **Poziom Strategiczny (horyzont 2-3 lat)**
  Cele strategiczne definiują stan docelowy, do którego dąży klaster. Powinny one wspierać misję biznesową klastra (np. tę określoną w Strategii Rozwoju) i budować przewagę kon-

kurencyjną oraz zaufanie wśród potencjalnych nowych członków klastra. Poniżej propozycja celów strategicznych:

» **Cel Strategiczny nr 1: budowa kultury odporności** – dążenie do stanu, w którym cyberbezpieczeństwo jest naturalnym elementem działalności każdego członka klastra, a świadomość zagrożeń (np. phishingu) jest powszechna wśród pracowników wszystkich szczebli, nie tylko w działach IT.

» **Cel Strategiczny nr 2: zapewnienie ciągłości i minimalizacja ryzyka systemowego (awaria całego systemu, a nie tylko poszczególnych jego elementów)** – stworzenie mechanizmów, które w przypadku ataku na jednego z członków uchronią pozostałych przed efektem domina i pozwolą na szybkie przywrócenie procesów biznesowych.

» **Cel Strategiczny nr 3: wiarygodność jako partnera w łańcuchu dostaw** – pozycjonowanie klastra jako bezpiecznego ekosystemu, co ułatwi podmiotom członkowskim spełnianie wymogów bezpieczeństwa stawianych przez dużych kontrahentów oraz regulacji (takich jak np. NIS2).

- **Poziom Operacyjny (horyzont 12 miesięcy)**
  Cele operacyjne muszą być mierzalne i realizowane we względnie krótkim czasie. Są to konkretne kroki, które koordynator i członkowie podejmą, aby zrealizować misję oraz przybliżyć się do realizacji celów strategicznych. Stosując metodę SMART (technika wyznaczania celów oparta na akronimie od pięciu angielskich słów: Specific (konkretny), Measurable (mierzalny), Achievable (osiągalny), Relevant (istotny) i Time-bound (określony w czasie)) w wyznaczaniu celów, proponujemy przykładowe:

» **Cel Operacyjny A (Edukacja) – podniesienie kompetencji kadr:**
  * *Działanie:* organizacja cyklu 4 kwartalnych webinarów/szkoleń dla członków klastra dotyczących aktualnych zagrożeń (np. „Jak rozpoznać fałszywą fakturę?").
  * *Miernik:* przeszkolenie minimum 30% członków do końca konkretnego roku.

» **Cel Operacyjny B (Zabezpieczenie klastra) – wdrożenie standardów w biurze koordynatora:**
  * *Działanie:* wdrożenie Uwierzytelniania Wieloskładnikowego (MFA) na wszystkich kontach służbowych (poczta, chmura, social media) oraz weryfikacja procesu wykonywania kopii zapasowych (backup).
  * *Miernik:* 100% kont służbowych zabezpieczonych MFA w ciągu 3 miesięcy od przyjęcia strategii.

» **Cel Operacyjny C (Diagnoza) – ocena stanu bezpieczeństwa członków:**
  * *Działanie:* Przeprowadzenie prostej ankiety samooceny (bazującej na narzędziu zaproponowanym w podręczniku) wśród członków, aby zidentyfikować najsłabsze obszary wymagające wsparcia.
  * *Miernik:* Uzyskanie wypełnionych ankiet od co najmniej 50% członków klastra.

» **Cel Operacyjny D (Reagowanie) – utworzenie kanału komunikacji kryzysowej:**
  * *Działanie:* Opracowanie i przetestowanie prostej procedury informowania o incydentach (np. dedykowana grupa na komunikatorze lub lista mailingowa „Cyber-Alert"), służącej wyłącznie do ostrzegania przed atakami.
  * *Miernik:* Przeprowadzenie jednego testu łączności (próby generalnej) do końca roku.

Tak sformułowane cele są realistyczne nawet dla klastrów bez dużego budżetu, a ich wdrożenie może w znaczący sposób wpłynąć na bezpieczeństwo wszystkich członków.

7.1.3 Mierniki Sukcesu (KPI)

Aby skutecznie zarządzać cyberbezpieczeństwem, niezbędne jest systematyczne mierzenie jego poziomu. Strategia powinna zawierać proste wskaźniki efektywności – KPI (ang. Key Performance Indicators), które umożliwiają ocenę skuteczności działań zarządczych Wskaźniki te nie powinny mieć charakteru technicznego (np. liczba zablokowanych wirusów), lecz odnosić się do poziomu zarządzania cyberbezpieczeństwem. Dobre mierniki dla klastra to:

- **Poziom pokrycia szkoleniami:** odsetek członków, które wzięły udział w co najmniej jednym webinarze o cyberbezpieczeństwie.
- **Czas reakcji:** średni czas od zgłoszenia incydentu koordynatorowi do przekazania informacji pozostałym członkom (np. ostrzeżenie o fali phishingu).
- **Poziom pokrycia samooceną ryzyka:** liczba członków, które przeprowadziły podstawową samoocenę ryzyka (według ankiety zaproponowanej w podręczniku).

KPI powinny oczywiście zostać dobrane odpowiednio do postawionych sobie celów i być adekwatne do możliwości ich realizacji. Nawet jeżeli nie zostaną one spełnione w założonej liczbie to kolejnym krokiem powinna być weryfikacja takiego stanu rzeczy oraz zidentyfikowanie barier, które to uniemożliwiły. Jest to również ważne w kontekście rzetelnej samooceny oraz wyciągania wniosków na przyszłość, które pozwolą w kolejnym etapie zaplanować bardziej realne cele oraz mierniki sukcesu.

7.1.4 Partnerstwa Strategiczne

Istotnym elementem strategii są partnerstwa. Zbudowanie odporności cyfrowej we współpracy z konkretnymi wyspecjalizowanymi jednostkami jest dużo bardziej efektywne. Nawiązanie kontaktu z uczelniami, firmami technologicznymi, centrami kompetencji, jednostkami administracji publicznej, ekspertami branżowymi, czy innymi klastrami znacząco może podnieść jakość podejmowanych działań. Partnerstwa mogą wspierać koordynatora w obszarach, które wymagają specjalistycznej wiedzy, np. w przypadku audytu, analizy zagrożeń, szkoleniach, czy opracowywaniu procedur reagowania na zagrożenia. Nawet jeżeli partnerstwa nie będą sformalizowane, mogą również przybrać formę jednorazowych konsultacji lub regularnej wymiany dobrych praktyk. Warto uwzględnić je w strategii i opisać potencjalne zasady takiej współpracy, podać przykładowy zakres wymiany danych oraz częstotliwość wspólnych działań, o ile jest możliwy do określenia. Wtedy nie będą one partnerstwem strategicznym, a tylko doraźną współpracą, niemniej warto również o tym wspomnieć w tym punkcie.

Wspomniane relacje warto nawiązać z następującymi podmiotami:

- Uczelnią, która funkcjonuje w obrębie województwa, w którym działa koordynator klastra i posiada kierunek/katedrę cyberbezpieczeństwa.
- Z CSIRT NASK lub CSIRT (Computer Security Incident Response Team (pol. Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego) sektorowym – jeżeli istnieje stosowny do sektora, w którym działa klaster, np. CSIRT KNF – Komisji Nadzoru Finansowego (utworzony w celu prowadzenia koordynacji działań i wsparcia obsługi incydentów bezpieczeństwa w podmiotach rynku finansowego uznanych

za Operatorów Usług Kluczowych w UKSC2), CSIRT CEZ – Centrum E-Zdrowia (utworzony w celu prowadzenia koordynacji działań i wsparcia obsługi incydentów bezpieczeństwa w podmiotach Sektora Zdrowia uznanych za Operatorów Usług Kluczowych w UKSC2.

- innymi klastrami działającymi w tym obszarze, np.
  - » w Polsce: Polski Klaster Cyberbezpieczeństwa #CyberMadeInPoland[103], Pomorski Klaster ICT[104], Łódzki Klaster ICT[105] itd.
  - » w Europie: Cyber Ireland[106], Hague Security Delta[107], LSEC – Leaders In Security[108], CyberLur[109], Cyber Security Cluster of Excellence[110] oraz Euroklastry, np. Silicon Europe[111], SUSTAIN Eurocluster[112], AEC EUROCLUSTER[113] itd[114].

- stowarzyszeniami branżowymi, zrzeszeniami przedsiębiorców, instytucjami otoczenia biznesu, np.
  - » w Polsce: ISSA Polska[115], Polska Izba Informatyki i Technologii[116], Polska Platforma Bezpieczeństwa Wewnętrznego[117], CSO Council[118], ZIPSEE Cyfrowa Polska[119] itd.
  - » w Europie: European Cybersecurity Organisation (ECSO)[120], European Digital SME Alliance[121], Cyber Threat Alliance[122], Cybersecurity Advisors Network (CyAN)[123] itd.

Praktyczna wskazówka dla koordynatora: Nie twórz strategii w izolacji. Powołaj małą grupę roboczą (np. 2-3 osoby, w tym jedną, która posiada doświadczenie w zakresie cyberbezpieczeństwa), aby w ciągu jednego/dwóch spotkań warsztatowych omówić i spisać punkty w formie zwięzłego szkicu. Następnie przygotuj cały dokument i przedstaw członkom klastra – warto rozważyć zebranie opinii od przedstawicieli podmiotów członkowskich – ich doświadczenie może być cenne w wypracowaniu najbardziej adekwatnego dokumentu.

7.2 Ćwiczenia i symulacje

Jednym z najskuteczniejszych sposobów budowania odporności cyfrowej są ćwiczenia i symu-

103 Strona internetowa Klastra #CyberMadeInPoland. Dostęp: https://cybermadeinpoland.pl/. (26 listopada 2025)
104 Strona internetowa Pomorskiego Klastra ICT. Dostęp: https://interizon.pl/pl/. (26 listopada 2025)
105 Strona internetowa Łódzkiego Klastra ICT. Dostęp: https://ictcluster.pl/. (26 listopada 2025)
106 Strona internetowa Klastra Cyber Ireland. Dostęp: https://cyberireland.ie/. (26 listopada 2025)
107 Strona internetowa Klastra The Dutch Security Cluster. Dostęp: https://securitydelta.nl/. (26 listopada 2025)
108 Strona internetowa Klastra LSEC. Dostęp: https://www.digitalsecuritycatalyst.com/. (26 listopada 2025)
109 Strona internetowa Klastra CyberLur. Dostęp: https://cyberlur.es/aei-home. (26 listopada 2025)
110 Strona internetowa Klastra Cyscoe. Dostęp: https://cyscoe.ro/. (26 listopada 2025)
111 Strona internetowa Euroklastra Silicon Europe. Dostęp: https://www.silicon-europe.eu/home/. (26 listopada 2025)
112 Strona internetowa Euroklastra Sustain. Dostęp: https://www.sustaineurocluster.com/. (26 listopada 2025)
113 Strona internetowa Euroklastra SGG. Dostęp: https://www.sgg.si/eng-aec-eurocluster/. (26 listopada 2025)
114 Więcej Euroklastrów można znaleźć na stronie internetowej European Cluster Collaboration Platform. Dostęp: https://www.clustercollaboration.eu/euroclusters (26 listopada 2025)
115 Strona internetowa ISSA Polska. Dostęp: https://issa.org.pl/. (26 listopada 2025)
116 Strona internetowa PIIT. Dostęp: https://piit.org.pl/. (26 listopada 2025)
117 Strona internetowa PPBW. Dostęp: https://ppbw.pl/. (26 listopada 2025)
118 Strona internetowa CSO Council. Dostęp: https://csoc.pl/. (26 listopada 2025)
119 Strona internetowa Cyfrowa Polska. Dostęp:https://cyfrowapolska.org/. (26 listopada 2025)
120 Strona internetowa ECSO. Dostęp: https://ecs-org.eu/. (26 listopada 2025)
121 Strona internetowa Digitalsme. Dostęp: https://www.digitalsme.eu/. (26 listopada 2025)
122 Strona internetowa Cyber Threat Alliance. Dostęp: https://www.cyberthreatalliance.org/. (26 listopada 2025)
123 Strona internetowa Cybersecurity Advisors Network. Dostęp: https://cybersecurityadvisors.network/. (26 listopada 2025)

lacje incydentów, oparte na realnych scenariuszach i dostosowane do możliwości uczestników. Dobrze zorganizowane ćwiczenia pomagają członkom nie tylko zrozumieć, jak wyglądają prawdziwe ataki, ale także przetestować procedury, ocenić czas reakcji oraz zidentyfikować luki organizacyjne i techniczne. Założenie wykonywania takich ćwiczeń, np. raz w roku można uwzględnić również w strategii opisanej w poprzednim podrozdziale.

Pierwszym krokiem jest wybór scenariusza ćwiczenia. Powinien on odpowiadać typowym zagrożeniom dla członków klastra. Może to być atak phishingowy, awaria dostawcy usług chmurowych, próba przejęcia konta pracownika, incydent ransomware, wyciek danych lub zakłócenie działania systemu ERP (ang. Enterprise Resource Planning, tłum.oprogramowania do kompleksowego zarządzania zasobami przedsiębiorstwa).

W środowisku klastrowym, gdzie zasoby są ograniczone efektywną formą mogą być ćwiczenia w formule „Table Top Exercises (TTX)". Są to warsztaty dyskusyjne, podczas których uczestnicy (np. zarządy firm, koordynator) omawiają swoje reakcje na hipotetyczny scenariusz ataku, bez ingerencji w rzeczywiste systemy IT. Jest to również metoda stosowana przez agencję ENISA pod nazwą Cyber Europe[124], a także przez polskie Ministerstwo Cyfryzacji oraz Fundację Bezpieczną Cyberprzestrzeń – ostatnia edycja odbyła się w 2024 roku pod nazwą KSC-EXE 2024[125].

7.2.1 Table Top Exercises

Scenariusz ćwiczenia TTX musi być realistyczny i dotyczyć większości członków. Dla klastrów najlepszym wyborem mógłby być: atak na łańcuch dostaw (Supply Chain Attack) lub ransomware paraliżujący wspólny projekt.

Przykład: „Firma X, będąca członkiem klastra i dostawcą komponentów dla trzech innych firm, została zainfekowana oprogramowaniem ransomware. Hakerzy grożą publikacją wykradzionych projektów technicznych, które są własnością intelektualną całego klastra. Co robimy?".

Przebieg ćwiczeń (krok po kroku)

Organizacja ćwiczeń w klastrze powinna przebiegać w trzech fazach:

1. **Faza wstępna:** koordynator zaprasza przedstawicieli członków (osoby decyzyjne, nie tylko informatyków). Spotkanie trwa max. 2-3 godziny.

2. **Symulacja (rozgrywka):** moderator (może to być ekspert zewnętrzny lub przeszkolony reprezentant koordynatora) przedstawia scenariusz i wprowadza „wstawki" (ang. injects), czyli nowe informacje, które komplikują sytuację (np. „Media właśnie dowiedziały się o wycieku", „Systemy pocztowe przestały działać"). Uczestnicy muszą odpowiedzieć na pytania: *Kogo zawiadamiamy? Kto ma prawo podejmować decyzje o okupie? Jak komunikujemy się z klientami?*

124 Ministerstwo Cyfryzacji, (2024) „Udział Ministerstwa Cyfryzacji w ćwiczeniach Cyber Europe 2024" [artykuł online]. Dostęp: https://www.gov.pl/web/cyfryzacja/udzial-ministerstwa-cyfryzacji-w-cwiczeniach-cyber-europe-2024. (26 listopada 2025).

125 Serwis Rzeczypospolitej Polskiej, (2024) „KSC-EXE 2024: ćwiczenia krajowego systemu cyberbezpieczeństwa 2024" [artykuł online]. Dostęp: https://www.gov.pl/web/baza-wiedzy/ksc-exe-2024-cwiczenia-krajowego-systemu-cyber-bezpieczenstwa. (26 listopada 2025)

3. **Faza wniosków (ang. debriefing):** to najważniejsza część. Po zakończeniu scenariusza grupa omawia, co zadziałało, a co nie. Często okazuje się, że brakuje aktualnych list kontaktowych, procedur awaryjnych lub wiedzy prawnej.

4. **Faza wprowadzania zmian i poprawek:** w trakcie ćwiczenia ważne jest prowadzenie obserwacji i dokumentacji, aby móc później określić, które działania zadziałały lub mają opracowaną procedurę, a które wymagają poprawy. Kluczowe są również wnioski końcowe, ponieważ to one stanowią podstawę do wprowadzania zmian organizacyjnych, które powinny zostać uwzględnione w działalności podmiotu.

Koordynator klastra może przygotować wspólny raport, zawierający najważniejsze lekcje, rekomendacje oraz działania, które warto wdrożyć w skali klastra. W załączniku nr 1 przygotowana została przykładowa karta pracy, której wzór może zostać wykorzystany do organizacji ćwiczeń.

Dlaczego ćwiczenia TTX? Ponieważ większość błędów podczas incydentów cybernetycznych to błędy komunikacyjne i decyzyjne, a nie techniczne. Ćwiczenia te budują „pamięć mięśniową" organizacji i pozwalają przetestować procedury w bezpiecznych warunkach („na sucho"), zanim wystąpi realne zagrożenie.

Praktyczna wskazówka dla koordynatora: Nie bój się, że nie masz wiedzy technicznej, by prowadzić ćwiczenia. Twoją rolą jest zadawanie pytań biznesowych: „Czy wiemy, jak skontaktować się z wszystkimi członkami, jeśli e-maile nie działają?", „Kto jest upoważniony do kontaktu z mediami w imieniu klastra?". To są kluczowe kwestie zarządcze. Jeżeli budżet na to pozwoli, można zatrudnić doświadczonego eksperta, który przeprowadzi takie ćwiczenie.

7.2.2 Cyber Range

Kolejnym testem, ale tym razem dla zespołów IT członków klastra może być Cyber Range, czyli zaawansowana, w pełni wirtualna i izolowana platforma symulacyjna, która wiernie odwzorowuje sieć komputerową i środowisko IT firmy lub całego klastra. Jest to bezpieczne laboratorium, w którym można prowadzić realistyczne, dynamiczne ćwiczenia. Zamiast dyskutować o ataku, uczestnicy (głównie specjaliści IT z podmiotów członkowskich) aktywnie bronią symulowanej sieci przed kontrolowanym, żywym atakiem.

Dlaczego warto zorganizować Cyber Range?

- Testuje gotowość techniczną i pozwala weryfikować, czy zespoły IT potrafią naprawdę wykryć, zablokować i usunąć intruza, sprawdzając skuteczność narzędzi i procedur technicznych, np. reakcję firewalla (system bezpieczeństwa, który działa jako bariera między zaufaną siecią, a niezaufaną (np. internetem), monitorując i kontrolując ruch sieciowy na podstawie ustalonych reguł), czy systemów detekcji (system bezpieczeństwa, który monitoruje sieć i urządzenia w poszukiwaniu złośliwych działań i podejrzanych wzorców).

- Umożliwia ćwiczenia zespołowe, podczas których klaster może symulować atak na łańcuch dostaw, w którym systemy Firmy A muszą izolować Firmę B, a Firmy C i D wspólnie wymieniają się informacjami w czasie rzeczywistym.

- Buduje kompetencje, ponieważ jest jedną z najskuteczniejszych form praktycznego szkolenia dla administratorów systemów IT, pozwalająca na popełnianie błędów bez ryzyka dla rzeczywistej infrastruktury produkcyjnej.

Praktyczna wskazówka dla koordynatora: Wdrożenie własnego Cyber Range może być zbyt kosztowne. Dlatego koordynator klastra powinien szukać partnerstwa z ośrodkami akademickimi (politechnikami) lub firmami z branży cyberbezpieczeństwa (np. zrzeszonymi w klastrze, które oferują taką usługę). Można negocjować dostęp do platformy na preferencyjnych warunkach w ramach wspólnych projektów szkoleniowych dla członków.

7.3 Wymiana doświadczeń między klastrami

Skuteczna wymiana doświadczeń między klastrami wymaga uporządkowanego podejścia, opartego na stałych strukturach, jasno określonych zasadach i narzędziach, które umożliwiają systematyczne dzielenie się wiedzą. W praktyce najlepiej sprawdzają się modele współpracy wzorowane na europejskich ISAC-ach, w których uczestnicy regularnie analizują zagrożenia, wymieniają się informacjami o incydentach i tworzą wspólne zasoby. W środowisku klastrów oznacza to konieczność stworzenia mechanizmu, który pozwoli na bieżąco gromadzić, filtrować i przekazywać wiedzę w sposób bezpieczny i zrozumiały dla różnych branż.

Podstawą jest utworzenie struktury wymiany wiedzy, która porządkuje przepływ informacji i jasno określa, jakie treści trafiają do koordynatorów, podmiotów członkowskich oraz partnerów zewnętrznych. Taka struktura może obejmować trzy poziomy.

Takie uporządkowanie wymiany informacji sprawia, że każdy klaster może uczestniczyć na poziomie, który odpowiada jego aktualnym potrzebom i zasobom. Jednocześnie ułatwia koordynatorom budowanie trwałego systemu współpracy z innymi klastrami, niezależnie od branży. W sytuacji, kiedy wymiana wiedzy jest prowadzona z zagranicznymi klastrami pozwala na porównanie sytuacji w cyberprzestrzeni w różnych krajach – z jakimi problemami się borykają.

01 Pierwszy z nich to operacyjna wymiana informacji o incydentach i alertach, która koncentruje się na analizie bieżących zagrożeń, kampanii phishingowych, podatności w popularnych narzędziach, atakach na konkretne branże czy interpretacji komunikatów CERT Polska i ENISA.

02 Drugi poziom to wymiana praktyk technicznych i organizacyjnych, obejmująca dokumenty takie jak listy sprawdzające, standardy minimum dla łańcucha dostaw, scenariusze ćwiczeń czy wymiana dobrych praktyk w zakresie cyberhigieny.

03 Trzeci poziom to wymiana strategiczna, ukierunkowana na długoterminowe inicjatywy – wspólne projekty, wdrażanie standardów branżowych, prace nad strategią odporności, a także rozwój kompetencji wśród podmiotów członkowskich.

Aby usprawnić pracę, warto stworzyć stałe grupy robocze, które działają w zakresie ustalonych tematów i celów.

Przykładowy podział:

- Grupa „Incydenty i reagowanie” – dzielenie się scenariuszami incydentów, procedurami, lekcjami po ćwiczeniach i realnych zdarzeniach.
- Grupa „Dostawcy i łańcuch dostaw” – listy sprawdzające, wzory due diligence, białe listy dostawców i dobre praktyki w tworzeniu umów z dostawcami.
- Grupa „Ludzie i świadomość” – materiały szkoleniowe, kampanie edukacyjne, scenariusze testów phishingowych.

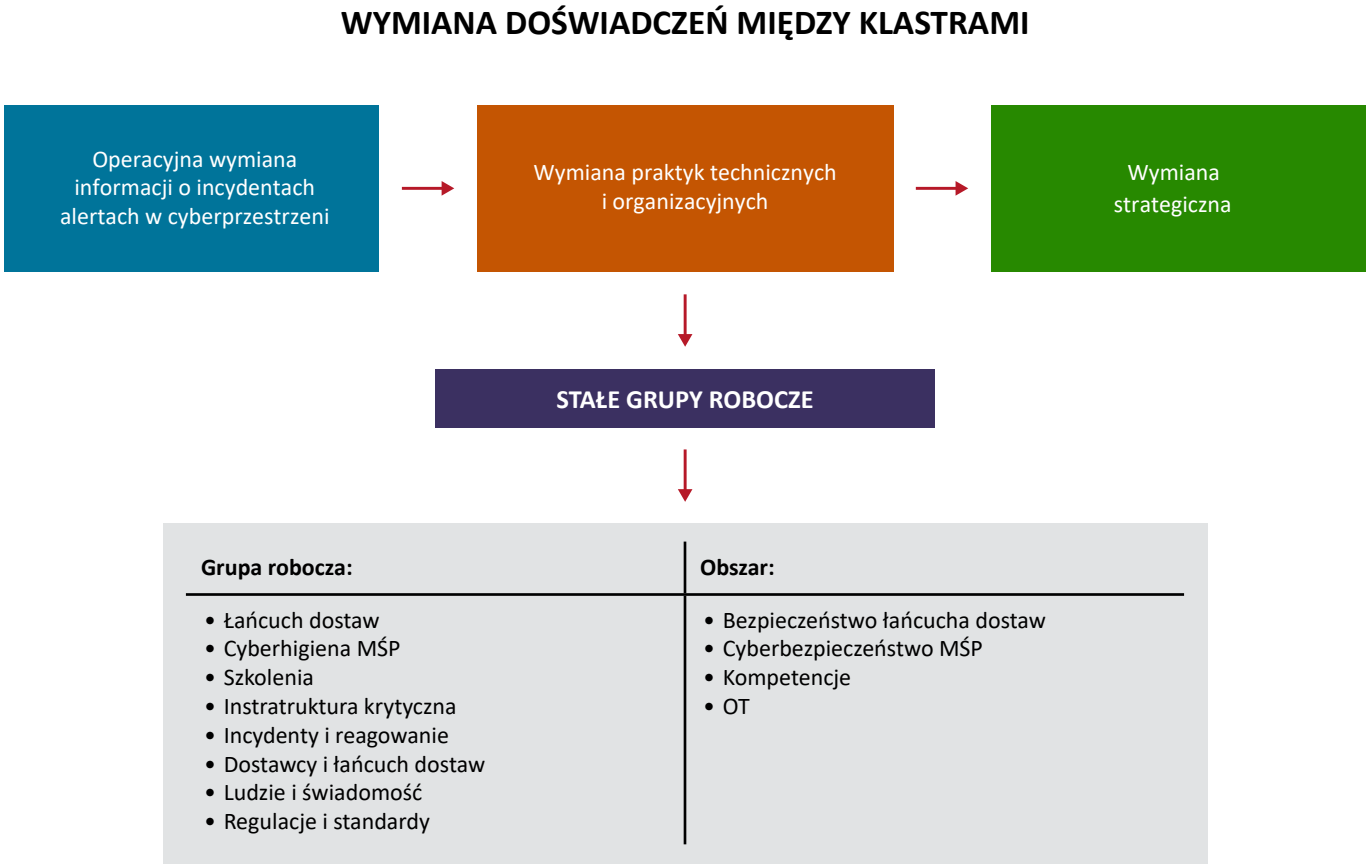
- Grupa „Regulacje i standardy” – interpretacje wymogów (NIS2, DORA, RODO), wzory polityk, listy sprawdzające zgodności.

Każda grupa ma lidera (z jednego klastra) i prosty roczny plan pracy: np. cztery spotkania online, jeden warsztat stacjonarny, dwa wspólne dokumenty do wypracowania. Praca takich grup powinna również być wspierana poprzez dedykowane narzędzia, np. wspólnie komunikatory, współdzielone dyski, mapy myśli, czy notatki.

Równolegle warto stosować model cyklicznego obiegu informacji, który jest charakterystyczny dla ISAC-ów i wielu europejskich sieci klastrów. Polega on na tym, że raz w miesiącu lub kwartale koordynatorzy wymieniają między sobą zestaw spójnych treści, które następnie mogą przekazywać członkom swoich klastrów. Zestaw taki może obejmować: streszczenia najważniejszych incydentów, alerty o podatnościach, interpretacje wytycznych regulatorów, rekomendacje narzędzi, przykłady dobrych praktyk i wnioski z incydentów zgłoszonych przez inne klastry. Warto stworzyć repozytorium wiedzy, które będzie dostępne np. na współdzielonym dysku – wtedy łatwo będzie można wrócić do każdego udostępnionego materiału.

Dodatkowym elementem jest współpraca oparta na benchmarkach branżowych. Klastry mogą porównywać swoje procedury, poziomy dojrzałości cyfrowej, czy modele szkoleniowe z innymi kla-

Rysunek 7.1 *Schemat wymiany doświadczeń między klastrami.*



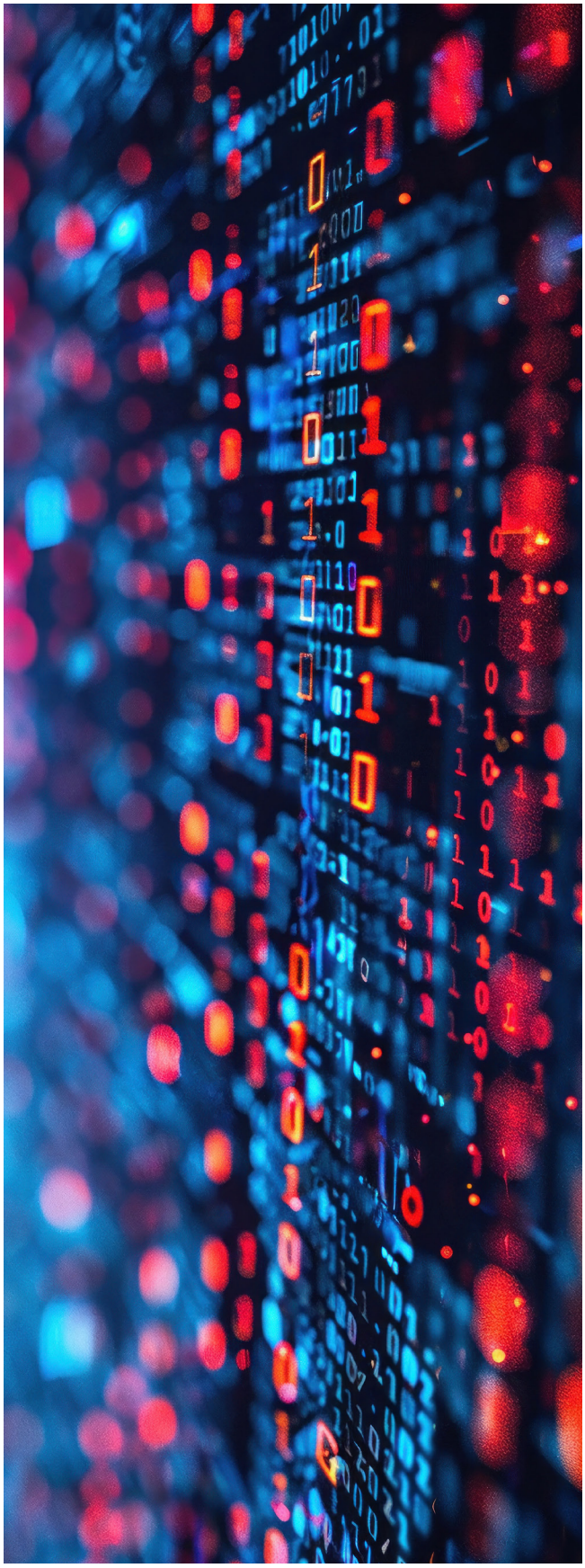
Źródło: Opracowanie własne.

strami w Polsce i Europie. Takie podejście pomaga identyfikować luki, określać priorytety i wybierać działania, które przynoszą najlepsze efekty.

Wreszcie, skuteczna wymiana wiedzy wymaga odpowiednich kanałów komunikacji. Klastry mogą stosować kombinację narzędzi: zamknięte grupy mailingowe, cykliczne newslettery, platformy wymiany dokumentów, webinary, spotkania hybrydowe oraz warsztaty tematyczne. Ważne, aby proces był nie tylko regularny, ale również zrozumiały, dlatego warto tworzyć krótkie podsumowania, infografiki, rekomendacje „do wdrożenia od zaraz" oraz gotowe szablony, które członkowie mogą zastosować bez specjalistycznej wiedzy.

Cały ten model wymiany wiedzy tworzy system, w którym klastry uczą się od siebie metod, narzędzi i sposobów reagowania na zagrożenia, zamiast działać w izolacji. Efekt jest podwójny: podmioty członkowskie zyskują dostęp do najlepszych praktyk, a koordynatorzy wzmacniają pozycję swojego klastra jako organizacji, która aktywnie wspiera rozwój kompetencji i bezpieczeństwo całego ekosystemu.

Dzięki regularnej wymianie doświadczeń klaster nie działa w izolacji – korzysta z wiedzy większej społeczności, która wspólnie mierzy się z podobnymi zagrożeniami. To znacząco wzmacnia odporność całego ekosystemu.



Załącznik nr 1 – Przykładowa karta pracy do ćwiczenia

Tytuł ćwiczenia: Test procedur reagowania na atak na łańcuch dostaw w klastrze.

Pole	Informacje wstępne
Data i czas trwania:	[DD/MM/RRRR], [HH:MM] – [HH:MM]
Lokalizacja:	[online/sala konferencyjna]
Koordynator ćwiczenia (moderator):	[imię i nazwisko, stanowisko]
Cel ćwiczenia:	[np. sprawdzenie, jak koordynator i członkowie reagują na atak ransomware na kluczowego dostawcę IT w klastrze (atak na łańcuch dostaw)]
Lista uczestników (firm/rola):	[wymień nazwy firm oraz role, np. firma X – prezes, firma Y – IT manager, klaster – koordynator]

A. Faza I: analiza incydentu i wstępna izolacja

Scenariusz wstępny: Otrzymujesz (jako koordynator/prezes) wiadomość od zarządu firmy członkowskiej X (kluczowego dostawcy usług dla innych członków), że ich systemy zostały zaszyfrowane, a hakerzy grożą publikacją Waszych wspólnych projektów. Firma X prosi o pilne wytyczne.

Pytanie Kluczowe	Decyzje i działania podjęte w trakcie ćwiczeń (notatki)	Odpowiedzialny/czas realizacji
1. Kto jest liderem kryzysowym?	[Kto powołuje zespół kryzysowy? Kto podejmuje decyzję o powiadomieniu pozostałych członków?]	[rola/imię]
2. Kanały komunikacji awaryjnej.	[Jak koordynator skontaktuje się z resztą klastra, jeśli e-maile i telefony są niemożliwe/niebezpieczne?]	[np. dedykowana grupa na komunikatorze Signal/WhatsApp]
3. Powiadomienie pozostałych członków.	[Kiedy i kogo zawiadamiamy? Czy informacja ma być ogólna, czy tylko dla firm powiązanych z dostawcą X? Treść wstępnego ostrzeżenia.]	[koordynator klastra]
4. Izolacja wektora ataku.	[Jakie są pierwsze instrukcje dla firm, które współpracowały z firmą X? (np. natychmiastowe odcięcie połączeń zdalnych, zmiana haseł, skanowanie systemów)]	[IT partner/koordynator]

B. Faza II: reagowanie, zgłaszanie i komunikacja zewnętrzna

Scenariusz: Zostajesz poinformowany, że atak rozprzestrzenia się. Kluczowy klient klastra pyta w mediach, czy jest bezpieczny. Musisz działać zgodnie z regulacjami.

Pytanie Kluczowe	Decyzje i działania podjęte w trakcie ćwiczeń (notatki)	Odpowiedzialny/czas realizacji
5. Obowiązki (CRA/NIS2).	[Czy i kiedy musimy zgłosić incydent do CSIRT/UODO? Kto za to odpowiada: firma X, czy klaster? Kto przygotowuje zgłoszenie?]	[Prawnik/właściciel danych]
6. Komunikacja zewnętrzna.	[Kto jest jedynym upoważnionym rzecznikiem do kontaktu z mediami/klientami w imieniu klastra? Jakie jest wstępne, zatwierdzone stanowisko?]	[rzecznik klastra]
7. Analiza kosztów i odpowiedzialności.	[Kto ponosi koszty analizy kryzysowej? Czy firma X miała ubezpieczenie? Czy klaster ma ubezpieczenie od ryzyka systemowego?]	[zarządy firm]
8. Uruchomienie planu ciągłości (BCP).	[Jak klaster zapewni zastępcze usługi dla firm, które straciły dostęp do usług firmy X? (np. uruchomienie serwisu awaryjnego przez inną firmę członkowską Y)]	[koordynator/partner technologiczny]

C. Faza III: wnioski i działania korygujące

Obszar	Wnioski/luki wykryte	Działania korygujące (Co musimy wdrożyć?)
Komunikacja.	[Np. lista alarmowa była nieaktualna. Brakowało alternatywnego kanału komunikacji poza e-mailem.]	[Wdrożenie dedykowanego, szyfrowanego komunikatora alarmowego do końca kwartału.]
Procedury/ dokumentacja.	[Np. nie było jasne, kto ma uprawnienia do podjęcia decyzji o odłączeniu systemów od internetu. Brakowało wzoru oświadczenia dla mediów.]	[Opracowanie i zatwierdzenie prostej procedury reagowania na incydenty w ciągu 2 miesięcy.]
Relacje z dostawcami.	[Np. okazało się, że firma X nie miała MFA na zdalnym dostępie.]	[Wprowadzenie jako obowiązkowego standardu w klastrze klauzuli o MFA dla wszystkich dostawców krytycznych.]
Szkolenia i świadomość.	[Np. uczestnicy byli sparaliżowani przez strach i pośpiech, nie skupiając się na faktach.]	[Zorganizowanie szkolenia antystresowego lub powtórzenie ćwiczeń za 6 miesięcy.]

Dalsze kroki

Termin	Działanie	Odpowiedzialny
[Data]	[Np. spotkanie z prawnikiem w celu weryfikacji klauzul o RODO/NIS2 w umowach z dostawcami.]	[Wdrożenie dedykowanego, szyfrowanego komunikatora alarmowego do końca kwartału.]
[Data]	[Np. opracowanie i zatwierdzenie klastrowego planu ciągłości działania.]	[grupa robocza ds. bezpieczeństwa]
[Data]	[Powtórzenie ćwiczenia TTX z nowym scenariuszem (np. atak phishingowy na finanse) i nowymi uczestnikami.]	[koordynator]

Rozdział 8

Studium przypadków

W Europie ciężko natrafić na studia przypadków, które opisują modelowy sposób wspierania członków klastra w zakresie cyberbezpieczeństwa przez koordynatora niebędącego typowym klastrem cyberbezpieczeństwa. Analiza projektów pozwoliła jednak wyróżnić kilka inicjatyw zbliżonych do rekomendowanych w niniejszym podręczniku modeli współpracy. Na ich podstawie zostały zaprezentowane poniżej trzy modele rozwoju usług wspierających proces budowania cyberodporności w klastrach.

8.1 Ogólna diagnoza potrzeb

Irlandzki klaster cyberbezpieczeństwa (Cyber Ireland) w 2023 r. przeprowadził projekt „Cyber Security for Advanced Manufacturing (Cyber4AM)". Założeniem projektu było połączenie irlandzkiego sektora cyberbezpieczeństwa z firmami MŚP działającymi w obszarze produkcyjnym, przygotowującym się do transformacji cyfrowej[126].

W ramach projektu klaster Cyber Ireland przeanalizował dojrzałość 20 MŚP ze szczególnym naciskiem na analizę potrzeb z obszaru cyberbezpieczeństwa. Kolejnym krokiem była identyfikacja dostępnych na irlandzkim rynku rozwiązań, które wpisywały się w potrzeby firm z sektora produkcyjnego. Projekt zakończył się raportem analizującym wpływ Przemysłu 4.0 na cyberbezpieczeństwo sektora produkcyjnego, ze szczególnym uwzględnieniem kwestii regulacyjnych, wyzwań czy rodzajów zagrożeń[127].

Wskazany projekt jest jednym z przykładów, w jaki sposób klastry polskie mogą wspierać swój sektor w obszarze cyberbezpieczeństwa, a konkretnie w obszarze analizy luk. Koordynator klastra na wzór irlandzkiego projektu może zacząć działania podnoszące poziom cyberodporności klastra i jego członków (a szerzej całego sektora) poprzez podobną analizę potrzeb i wyzwań w kontekście danego sektora, w którym operuje (np. automotive, bio-tech, czy produkcja). Działania takie najlepiej podejmować w porozumieniu z wyspecjalizowanymi klastrami ICT, które posiadają wiedzę z obszaru cyberbezpieczeństwa (np. Polski Klaster Cyberbezpieczeństwa #CyberMadeInPoland, Mazowiecki Klaster ICT itd.). Oprócz samej wiedzy z obszaru cyberbezpieczeństwa klastry te są w stanie zarekomendować konkretne rozwiązania lub usługi, które odpowiadają na zdefiniowane przez koordynatora potrzeby.

Powyższy projekt odpowiada też zdefiniowanym w podręczniku rekomendowanym sposobom wsparcia koordynatora. Wskazane w rozdziale 3 działania związane z ankietowaniem podmiotów członkowskich mogą być podstawą stworzenia takiego raportu, a cykliczna proaktywna diagnoza może być podstawą aktualizacji raportu, aby wiedza związana z lukami kompetencyjnymi i technologicznymi podmiotów członkowskich była aktualna. Dodatkowo raport taki może pokazać również stopień świadomości członków związany z obszarem cyberbezpieczeństwa w obszarze regulacji sektorowych, co również pozwoli koordynatorowi na lepsze dostosowanie swojej oferty względem członków klastra.

Wreszcie partnerstwo z klastrami ICT/cybersecurity da możliwość porównania narzędzi dostępnych na rynku, a także usług specjalistycznych, które inne klastry mogą świadczyć na rzecz danego koordynatora.

126 Cyber Irleand, „Cyber4Am – Cyber Security for Advanced Manufactoring & IN4.0" [artykuł online]. Dostęp: https://cyberireland.ie/cyber-security-for-advanced-manufacturing/. (24 listopada 2025)

127 Cyber Irleand, (2023) „Cyber4Am – Cyber Security for Advanced Manufactoring & IN4.0". Dostęp: https://cyberireland.ie/wp-content/uploads/2024/02/Cyber4AM-Summary-Report.pdf. (24 listopada 2025)

8.2 Budowa kompetencji wewnętrznych

1. **Punkt wyjścia:**

   W pierwszym kroku koordynator inwestuje w podniesienie kwalifikacji własnego zespołu poprzez szkolenia i certyfikacje w obszarze:

   - analizy potrzeb cyfrowych MŚP,
   - podstaw transformacji cyfrowej,
   - podstaw cyberbezpieczeństwa i oceny ryzyka,
   - zarządzania incydentami,
   - wymogów regulacyjnych (NIS2, RODO, CRA).

   Dzięki temu zespół klastra zyskuje umiejętność nawiązania z przedsiębiorcami dialogu o ich potrzebach technologicznych, bez potrzeby posiadania głębokiej wiedzy technicznej.

2. **Budowa ramowej metodyki oceny potrzeb:**

   Koordynator przygotowuje prostą metodykę oceny dojrzałości cyberbezpieczeństwa na podstawie:

   - narzędzi i list sprawdzających wskazanych w podręczniku,
   - elementów stosowanych w EDIH (ADMA, ang. Advanced Manufacturing Assessment),
   - uproszczonych narzędzi analizy ryzyka wskazanych w rozdziale 2,
   - wymagań normy ISO 27001.

   W efekcie klaster dysponuje własnym standardem diagnozy, który może stosować w każdym podmiocie członkowskim, niezależnie od branży.

3. **Świadczenie usług diagnozy i doradztwa podstawowego:**

   Zespół klastra zaczyna samodzielnie świadczyć usługę doradczą składającą się z:

   - diagnozy poziomu cyfryzacji i bezpieczeństwa,
   - wskazania luk i ryzyk,
   - rekomendacji działań,
   - przybliżonych ścieżek dojścia (technicznych i organizacyjnych).

   Jest to usługa na poziomie „light consulting” – koordynator klastra nie wdraża rozwiązań technicznych, lecz pomaga zrozumieć problemy i zaplanować kierunek zmian. Na tym etapie koordynator posiada już kompetencje do występowania w roli doradcy pierwszego kontaktu.

4. **Rozszerzenie kompetencji i specjalizacji, budowa stałej oferty:**

   W miarę zdobywania doświadczenia koordynator może poszerzać zakres usług poprzez:

   - dodatkowe szkolenia pracowników (np. audyty podstawowe, bezpieczeństwo chmury),
   - uczestnictwo w projektach europejskich lub regionalnych,
   - pracę z ekspertami zewnętrznymi.

   W wyniku wcześniejszych działań koordynator tworzy stałą ofertę usług, które mogą być dofinansowane ze środków publicznych, co ułatwia dostęp dla MŚP.

5. **Model współpracy z rynkiem**

   Klaster pozostaje organizacją nietechnologiczną, dlatego:

   - nie wdraża rozwiązań IT,
   - nie konkuruje z firmami technologicznymi,
   - pełni rolę nadzorczą, doradczą i koordynacyjną.

   W sytuacjach wymagających specjalizacji (wdrożenia, audyty pogłębione, OT, testy penetracyj-

ne) koordynator kieruje członka do partnerów rynkowych, ale robi to w sposób uporządkowany, zgodny z własną metodyką i diagnozą.

6. Finansowanie

Rozwój usług koordynatorów w takim modelu jest możliwy do sfinansowania przez program FENG, działania 2.17 „Rozwój oferty klastrów dla firm”[128]. W jego ramach koordynatorzy Krajowych Klastrów Kluczowych oraz Ponadregionalnych Klastrów Wzrostowych mają możliwość wytworzenia bądź ulepszenia istniejącej usługi proinnowacyjnej. Proponowane rozwiązanie wpisuje się w cele grantu, dając koordynatorom możliwość rozwinięcia unikalnej usługi wspierania swoich członków w bezpiecznej transformacji cyfrowej.

Zaletą takiego rozwiązania jest fakt, że koordynator na stałe nabywa kompetencję w obszarze diagnozy potrzeb i doradztwa w procesach związanych z cyberbezpieczeństwem. Nabycie kompetencji przez zespół koordynatora daje też swobodę w kształtowaniu zakresu usługi i jej ewentualnej modyfikacji, a w przyszłości również możliwość świadczenia jej rynkowo dla innych klastrów lub organizacji spoza swojego ekosystemu.

Wadą takiego podejścia w stosunku do oferty rynkowej jest wąski zakres usług z zakresu cyberbezpieczeństwa, które jest w stanie świadczyć koordynator oraz długość procesu nabywania umiejętności i praktyki z tego obszaru.

8.3 Konsolidowanie wiedzy z zewnątrz

W tej części publikacji zostaną opisane modele działania i współpracy w ramach tych inicjatyw. Sposób działania i finansowania EDIH można zastosować również w klastrach, które poprzez wyspecjalizowane projekty, mogą realnie wpływać na podnoszenie poziomu cyberbezpieczeństwa swoich członków.

Konsorcja EDIH stworzone są z firm prywatnych oraz instytucji publicznych wyspecjalizowanych w danej dziedzinie, działają więc w modelu przybliżonym do klastrów. Finansowanie działań EDIH ma dwa źródła publiczne: środki w ramach programów europejskich oraz krajowych. Co ważne MŚP mogą skorzystać z usług EDIH za darmo[129].

Podobny model można zaimplementować w polskich klastrach. Co warte podkreślenia, proponowane działania powinny stać w synergii z istniejącymi w Polsce EDIH-ami, aby uzupełniać istniejącą już na rynku ofertę bądź powinny skupiać się tylko na członkach bądź sektorze, w którym działa klaster.

128 Strona Informacyjna archiwalnego naboru do konkursu „Rozwój oferty klastrów dla firm - nabór dla koordynatorów Krajowych Klastrów Kluczowych” (2025). Dostęp: https://www.parp.gov.pl/component/grants/grants/rozwoj-oferty-klastrow-dla-firm-nabor-dla-koordynatorow-krajowych-klastrow-kluczowych. (24 listopada 2025)

129 Polska Agencja Rozwoju Przedsiębiorczości, „Europejskie Centra Innowacji Cyfrowych (EDIH)” [artykuł online]. Dostęp: https://www.parp.gov.pl/component/site/site/edih#mapa. (24 listopada 2025)

W rozdziale 5 zostały zaproponowane praktyczne narzędzia, jakich koordynator klastra może użyć, aby realnie wspierać swoich członków w podnoszeniu poziomu cyberodporności. Poniżej prezentujemy przykładowy model takiej współpracy oparty o założenia EDIH oraz specyfikę działalności klastrów:

1. Punkt wyjścia:

Koordynator zrzesza kilkadziesiąt podmiotów, głównie MŚP oraz podmiotów publicznych, czy organizacji trzeciego sektora. Nie posiada własnych ekspertów cybersecurity, nie prowadzi projektów technologicznych z obszaru bezpieczeństwa i nie dysponuje szeroką siecią ekspertów IT.

Widząc rosnące ryzyka oraz wyzwania regulacyjne, koordynator klastra postanawia stworzyć program wsparcia w oparciu o model EDIH:

- nie tworzy kompetencji wewnętrznie.
- pozyskuje partnerów z rynku, od których kupuje dane usługi,
- nawiązuje partnerstwa z innymi ekosystemami lub EDIH-ami specjalizującymi się w tym obszarze.

2. Budowa konsorcjum zewnętrznego

Partnerzy technologiczni:

- firmy usługowe z zakresu cyberbezpieczeństwa (audyty, testy penetracyjne, szkolenia),
- firmy produktowe z zakresu cyberbezpieczeństwa,
- dostawcy rozwiązań chmurowych,
- integratorzy IT z regionu.

Partnerzy z otoczenia biznesu:

- inny klaster wyspecjalizowany w cyberbezpieczeństwie,
- EDIH z regionu,
- uczelnie z kierunkami informatycznymi,
- organizacje branżowe.

Zasady współpracy:

- partnerzy świadczą usługi „na zaproszenie" klastra – w praktyce koordynator podpisuje umowy ramowe z wybranymi dostawcami,
- koordynator negocjuje ceny i zakres w oparciu o zapotrzebowania swoich członków i specyfikę sektora,
- klaster odpowiada za komunikację, rekrutację członków, administrację i rozliczenia,
- usługi i produkty są modularne.

Finansowanie:

- środki publiczne – np. ramach programu FENG 2.17,
- dotacje regionalne,
- wkład własny członków,
- sponsorzy i inwestorzy prywatni.

3. Proces wsparcia członków

Koordynator zajmuje się wewnętrzną rekrutacją członków zainteresowanych skorzystaniem z usług z obszaru cyberbezpieczeństwa. Rekrutacja powinna równolegle uwzględniać prostą diagnozę dojrzałości cyberbezpieczeństwa podmiotu. W diagnozie można użyć kwestii opisanych w liście sprawdzającej z obszaru cyberbezpieczeństwa załączonej do niniejszego poradnika. Ankieta powinna uwzględniać minimum następujące obszary:

- kontrola haseł i MFA,
- polityka nadawania, odbierania i przeglądania uprawnień,
- zasady bezpiecznej pracy zdalnej,

- wykorzystywane rozwiązania techniczne – antywirusy, firewall, kopie zapasowe, segmentowanie i monitorowanie sieci,
- częstotliwość szkoleń,
- przegląd procedur,
- analiza incydentów z ostatnich 2 lat,
- ubezpieczenia od cyberincydentów,
- znajomość regulacji i norm z obszaru cyberbezpieczeństwa.

Rolą koordynatora jest przygotowanie ankiety wstępnej diagnozy, a także dystrybucja jej wśród swoich członków.

Poniżej zaprezentowano przykładowy katalog usług, które może świadczyć koordynator w takim modelu.

Usługa 1: Audyt „light" w podmiotach członkowskich

Audyt taki powinien trwać 2-3 godziny i może być realizowany zdalnie.

Audytorzy sprawdzają stan faktyczny poziomu cyberbezpieczeństwa w podmiocie, bazując na wstępnej diagnozie oraz wywiadach z reprezentantami podmiotu.

Rolą koordynatora jest zakontraktowanie odpowiedniej liczby audytorów oraz dostarczenie wyników diagnozy oraz benchmarku sektora (jeśli posiada).

Usługa 2: Audyt NIS2/UKSC2

Zakontraktowani wcześniej specjaliści ds. zgodności z NIS2 świadczą usługi dla członków na zasadzie: pomocy w samoidentyfikacji, wstępnej ocenie zgodności podmiotu z regulacjami oraz przygotowują rekomendacje dotyczące procesu zapewnienia zgodności z regulacjami.

Usługa 3: Szybkie wdrożenia

Koordynator wraz z firmami z obszaru cyberbezpieczeństwa przygotowuje pakiety gotowych do wdrożeń rozwiązań np.

Pakiet 1 – Bezpieczna poczta:
- MFA,
- reguły antyphishingowe.

Pakiet 2 – Kopie zapasowe:
- konfiguracja backupu chmurowego,
- test odtwarzania.

Pakiet 3 – Bezpieczna praca zdalna:
- weryfikacja urządzeń,
- wdrożenie VPN,
- zasady przyznawania dostępu.

Pakiet 4 – Polityki bezpieczeństwa:
- polityka haseł,
- polityka bezpiecznej pracy zdalnej,
- procedura zgłaszania incydentów.

Pakiet 5 – Bezpieczna sieć:
- przegląd routerów, firewall, punktów Wi-Fi,
- segmentacja sieci,
- podstawowe monitorowanie logów.

Pakiet 6 – Bezpieczny przemysł:
- inwentaryzacja urządzeń OT,
- oddzielenie sieci OT od IT,
- wprowadzenie kontroli dostępu.

Usługa 4: Szkolenia

Zakontraktowani przez koordynatora trenerzy przeprowadzają szkolenia z zakresu cyberbezpieczeństwa. Rekomenduje się, aby formuła szkoleń nie uwzględniała tylko formy zdalnej, ale minimum 2 razy w roku, odbywała się w formule stacjonarnej. Szkolenia stacjonarne bardziej angażują uczestników i dają moż-

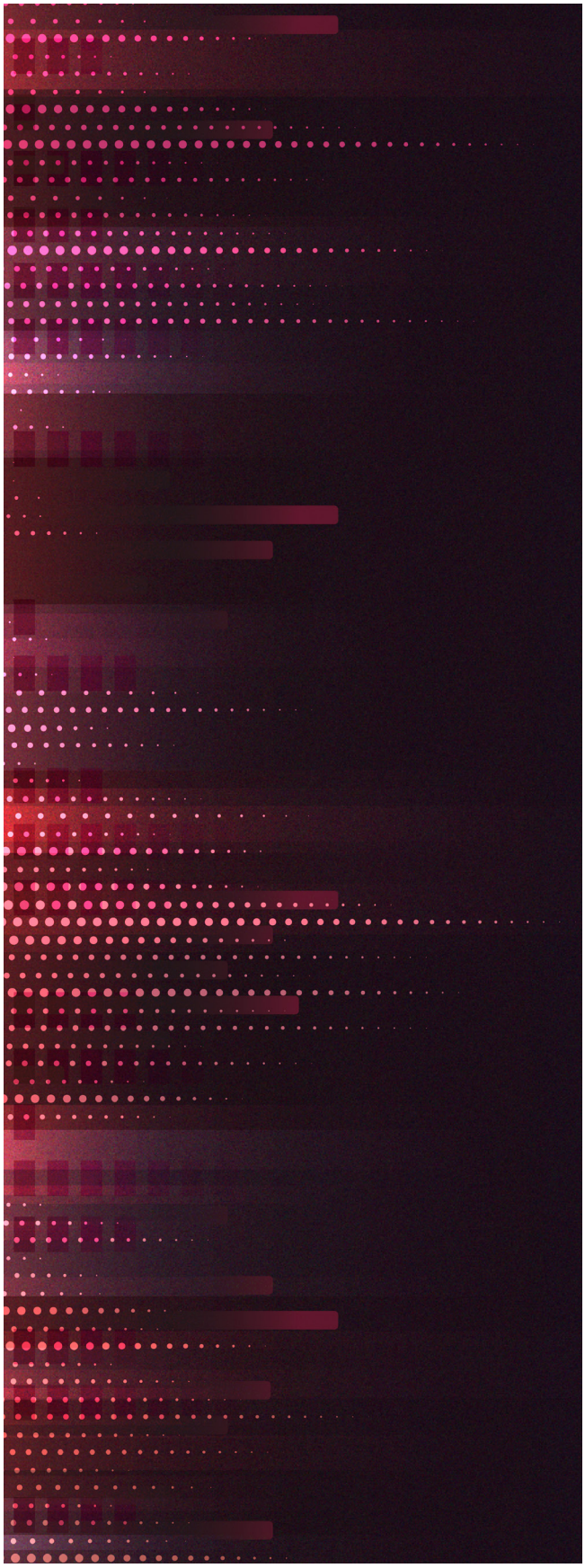
liwość wzbogacenia szkolenia o praktyczne ćwiczenia i warsztaty.
Tematy szkoleń powinny odpowiadać specyfice klastra, jego wielkości, ekspozycji na zagrożenia, a także uwzględniać kwestie regulacyjne. Poniżej zaprezentowane zostały przykładowe tematy szkoleń:

- „Zasady podstawowej cyberhigieny".
- „Czy hasła mnie obronią? – jak tworzyć silne hasła i wdrażać silne uwierzytelnianie".
- „Sprawdź, czy jesteś gotowy na NIS2".
- „Najbardziej popularne rodzaje zagrożeń na przykładzie faktycznych incydentów".
- „Jak budować kulturę organizacji w firmie".
- „Techniczne aspekty cyberbezpieczeństwa".

Minimalne zasoby koordynatora potrzebne do zbudowania takiego modelu:

- 1 osoba do organizacji projektu i komunikacji,
- 1 osoba do administracji umów i finansów,
- partnerzy technologiczni z rynku,
- mechanizm finansowania (np. wkład członków, sponsorzy, środki publiczne lub podejście hybrydowe).

Model opiera się głównie na agregowaniu usług, które są świadczone przez specjalistów, a usługi są finansowane lub współfinansowane przez koordynatora klastra. Koordynator zajmuje się zarządzaniem projektem, rekrutacją, koordynacją, kontraktowaniem specjalistycznych firm i rozliczaniem jego wyników. Jak widać, model uwzględnia pozyskiwanie kompetencji z zewnątrz poprzez kontraktowanie firm i ekspertów zajmujących się tematem cyberbezpieczeństwa, bądź nawiązywanie strategicznych partnerstw z innymi klastrami lub organizacjami branżowymi. Jest to dokładnie logika EDIH, ale zastosowana w klastrze, który sam nie ma kompetencji technicznych.



Rozdział 9

Praktyczne wskazówki dla koordynatora klastra

Niniejszy rozdział przedstawia zestaw praktycznych wskazówek dla koordynatorów klastrów, opartych na najlepszych praktykach, doświadczeniach z pracy z podmiotami członkowskimi oraz informacje o aktualnych trendach w obszarze cyberbezpieczeństwa. Wskazuje on najważniejsze elementy codziennego wsparcia podmiotów członkowskich od skutecznej komunikacji i prowadzenia działań edukacyjnych po monitorowanie efektów oraz wdrażanie narzędzi ułatwiających diagnozę i poprawę bezpieczeństwa.

Celem rozdziału jest wyposażenie koordynatora w praktyczny zestaw wskazówek, które ułatwią jego codzienną pracę, przyspieszą budowanie cyberodporności członków oraz pozwolą na konsekwentne rozwijanie kompetencji całego ekosystemu klastra.

9.1 Komunikacja i promocja – wskazówki jak tłumaczyć złożone tematy w sposób zrozumiały i motywujący

Prowadzenie skutecznej komunikacji w obszarze cyberbezpieczeństwa dla podmiotów członkowskich jest dużym wyzwaniem koordynatorów klastrów. Jeżeli koordynator zdecyduje się już na takie działania, komunikacja powinna przebiegać w sposób prosty i efektywny. Wskazówki zawarte w tym rozdziale mają charakter praktyczny i mogą być stosowane bezpośrednio w codziennej pracy klastra. Koordynatorzy powinni korzystać z nich jako przewodnika do planowania działań edukacyjnych, komunikacyjnych i operacyjnych w zakresie cyberbezpieczeństwa (ale i nie tylko). Wskazówki mogą służyć m.in. do przygotowania materiałów informacyjnych, organizowania szkoleń, tworzenia procedur reakcji na incydenty, czy monitorowania skuteczności działań w ekosystemie klastra.

1. **Używaj prostego języka** – tłumacz zagadnienia w sposób zrozumiały dla menedżerów i pracowników nieposiadających doświadczenia w IT. Tłumaczenie zagadnień technicznych (jak np. phishing, ransomware, uwierzytelnianie wieloskładnikowe) powinno przekładać się na język korzyści i ryzyka biznesowego. Zamiast operować żargonem sektora cyberbezpieczeństwa, koordynator powinien skupić się np. na tym, co podmiot traci w wyniku wystąpienia incydentów (dane, pieniądze, czas) i jak to wpływa na jego funkcjonowanie.

   » *Przykład:* zamiast mówić „atak DDoS powoduje niedostępność usług", można powiedzieć „atak przeciąża stronę tak, że przestaje działać".

2. **Segmentacja odbiorców** – dopasuj komunikaty do roli i odpowiedzialności odbiorcy (zarząd, dział IT, pracownicy). Zarząd mogą interesować aktualnie obowiązujące regulacje cyberbezpieczeństwa, straty finansowe i reputacyjne. Dział IT będzie skupiał się głównie na detalach technicznych, a pozostali pracownicy na zagrożeniach, z którym najczęściej mogą się spotkać w codziennej pracy (np. jak tworzyć hasła, które trudno złamać).

3. **Regularnie wysyłaj newslettery i alerty** – cykliczna komunikacja utrzymuje temat cyberbezpieczeństwa w świadomości pracowników. Newsletter może zawierać podsumowanie trendów, informacje o najnowszych, aktywnych kampaniach (np. mailach wyłudzających dane podszywających się pod lokalny bank) itp.

4. **Organizuj krótkie webinary i warsztaty** – webinary pozwalają na interaktywną edukację i odpowiadanie na pytania uczestników. Umożliwiają także zaproszenie ekspertów do przedstawienia danego zagadnienia. Takie działania pozwalają na tworzenie sieci kontaktów dla ekosystemu klastra oraz przekazywanie aktualnych informacji bez konieczności

posiadania wyspecjalizowanej wiedzy w zespole. Wykorzystywanie wiedzy ekspertów pozwala także na uproszczenie komunikacji. Ich doświadczenie w pracy z klientami pozwala w prosty sposób komunikować skomplikowane aspekty cyberbezpieczeństwa.

5. **Wykorzystuj przykłady z życia** – studia przypadków (case study) pokazujące skutki ataków lub efekty prewencji mają większą wartość merytoryczną ze względu na możliwość przełożenia sytuacji na organizację, którą się reprezentuje. Świetnym partnerem do tego typu działań będą lokalne firmy z branży cyberbezpieczeństwa, które mogą opowiedzieć o swoich doświadczeniach praktycznych z pracy z klientami.

6. **Stwórz zamknięte grupy dyskusyjne lub platformę online** – takie podejście umożliwia szybką wymianę informacji i dobrych praktyk. Działanie takich grup często opiera się na publikowaniu bieżących informacji z sieci lub ciekawostek z obszaru cyberbezpieczeństwa. Grupy pozwalają także na bezpośrednią interakcję pomiędzy członkami klastra, a przez to na lepszą wymianę informacji o nagłych incydentach, czy podatnościach koniecznych do załatania.

7. **Wykorzystuj listy sprawdzające i kwestionariusze samooceny zawarte w podręczniku** – takie działania pozwalają podmiotom członkowskim na samoocenę poziomu cyberodporności organizacji. Pozwalają one także na usystematyzowanie aktualnie posiadanych zasobów i działań. Odciążają jednocześnie każdy podmiot z osobna z konieczności stworzenia własnych materiałów sprawdzających (szczególnie istotne jest to dla MŚP, które nie posiadają własnego działu cyberbezpieczeństwa).

8. **Organizuj sesje Q&A z ekspertami** – bezpośredni kontakt z praktykami rozwiewa wątpliwości i buduje zaufanie. Pozwala także na budowanie szerokiej sieci kontaktów dla podmiotów członkowskich. Znajomość ekspertów jest kluczowa, w szczególności w momencie wystąpienia incydentu. Podmioty niechętnie dzielą się informacją o ataku na własną organizację, a jednocześnie muszą znaleźć wsparcie do jego obsługi.

9. **Udostępniaj narzędzia do samooceny i symulacji incydentów** – praktyczne ćwiczenia zwiększają przygotowanie na realne zagrożenia. Jako przykład można wykorzystać ćwiczenie „Table Top Exercise" zaproponowane w rozdziale 7. Działania takie można organizować jako warsztaty dla grupy podmiotów z klastra, co dodatkowo pomoże budować relacje jednocześnie rozwijając wspólny poziom cyberbezpieczeństwa. Relacje medialne z takich ćwiczeń pozwalają także na ukazanie klientom takiej organizacji jako przywiązującej wagę do cyberbezpieczeństwa.

10. **Monitoruj efekty komunikacji i dopasowuj treści** – regularne ankiety, informacja zwrotna i analiza aktywności pozwalają ulepszać przekaz i narzędzia edukacyjne.

9.2. Mierzenie rezultatów – system monitorowania postępów i raportowania rezultatów zwiększania cyberodporności w klastrze

Mierzenie rezultatów działań związanych z zwiększaniem cyberodporności w klastrze jest kluczowe dla koordynatora pod względem ulepszania swoich usług oraz dostarczania jak największej wartości dodanej dla podmiotów członkowskich. Proces ten można przedstawić w kilku krokach:

Krok 1: Ustalenie zakresu i celów monitorowania

Koordynator klastra określa, które aspekty będzie monitorował w ramach działalności podmiotów członkowskich. W ramach rozpoczęcia działań należy wskazać:

- Jakie obszary bezpieczeństwa będą monitorowane, np. realizacja szkoleń dla pracowników, posiadanie odpowiednich polityk bezpieczeństwa, certyfikatów, procesu realizacji kopii zapasowych, posiadania procedur wystąpienia incydentu.
- Jakie dane mają być raportowane – ustalenie wraz z podmiotami członkowskimi, które dane powinny być raportowane do koordynatora.
- Sposób raportowania danych – należy ustalić, czy dane będą raportowane na podstawie rozmów z przedstawicielami klastra, wypełniania ankiet (należy ustalić, czy ankiety powinny być anonimowe), czy mailowo.
- Przedstawiciela danego podmiotu członkowskiego, który będzie odpowiedzialny za zbieranie i przekazywanie informacji.

Cel: stworzenie klarownego procesu przekazywania informacji do koordynatora klastra, który w następstwie interpretuje dane oraz proponuje możliwe rozwiązania.

Krok 2: Przygotowanie narzędzi i szablonów

Koordynator klastra przygotowuje (np. na podstawie przykładowych rozwiązań zawartych w podręczniku):

- macierz wskaźników,
- listy sprawdzające do samooceny,
- szablony kwestionariuszy,
- instrukcję raportowania do koordynatora.

Wypełnienie przez podmioty członkowskie niezbędnych materiałów nie powinno zajmować więcej, niż 30 minut pracy osoby odpowiedzialnej za to działanie na kwartał.

Krok 3: Pierwsza samoocena

W celu rozpoczęcia działań oraz utworzenia raportu początkowego każdy podmiot członkowski powinien:

- wypełnić listę sprawdzającą / kwestionariusz utworzony w kroku 2,
- określić poziom realizowanych inicjatyw z zakresu cyberbezpieczeństwa w poszczególnych obszarach,
- zgłosić istniejące polityki, procedury, narzędzia (zgodnie ze schematem przyjętym przy realizacji mierzenia rezultatów).

Na podstawie zebranych danych koordynator opracowuje raport początkowy – punkt startowy, który będzie benchmarkiem dla dalszych działań oraz nowych podmiotów dołączających do klastra. Ze względu na wrażliwość danych raport nie powinien zawierać żadnych informacji wrażliwych lub takich, które ze względu na ich opublikowanie mogłyby zagrozić cyberbezpieczeństwu któregoś podmiotu.

Krok 4: Cykl raportowania (cyklicznie np. raz na pół roku / rok)

Członkowie powinny przesyłać wypełnione dokumenty utworzone w kroku 2. Następnie koordynator powinien zebrać dane w macierz oraz przeanalizować wyniki. W wyniku analizy koordynator powinien określić obszary, które wymagają największego wsparcia oraz szukać potencjalnych relacji pod kątem cyberzagrożeń, na podstawie przesłanych danych ze strony członków klastra.

Krok 5: Raport dla członków klastra (co 6 lub 12 miesięcy)

Na podstawie zebranych informacji koordynator udostępnia zaangażowanym podmiotom członkowskim raport ze zbiorczym poziomem wdrożenia praktyk z zakresu cyberbezpieczeństwa w klastrze. Ponadto koordynator tworzy opis zmian względem poprzedniego okresu, przygotowuje rekomendacje na kolejny okres oraz przygotowuje listę dobrych praktyk członków, które radzą sobie najlepiej.

Ważnym aspektem tego działania jest takie podejście do podmiotów członkowskich, aby wyniki tych działań nie zostały odebrane jako atak lub wytykanie im błędów. Celem raportowania oraz podejmowania działań naprawczych jest zwiększanie poziomu cyberbezpieczeństwa firm, a nie dyskredytowanie podmiotów członkowskich biorących w nich udział.

Krok 6: Ciągłe doskonalenie

Na podstawie zbieranych danych koordynator:

- aktualizuje materiały szkoleniowe oraz dostosowuje narrację pod dalsze działania,
- dostosowuje nowe narzędzia oraz listy sprawdzające,
- planuje działania grupowe (warsztaty, szkolenia, wspólne projekty),
- identyfikuje członków, które mogą potrzebować indywidualnego wsparcia.

Przykładowa macierz monitorowania i raportowania rezultatów działań z zakresu cyberbezpieczeństwa

Poniższa macierz została zaprojektowana tak, by podmioty członkowskie mogły raportować krótko, konkretnie i w sposób porównywalny, a koordynator – agregować dane. Jest to macierz przykładowa i każdorazowo w ramach kroku 2 powinna zostać ona dostosowana pod uwarunkowania danego klastra i podmiotów w nim zrzeszonych.

Legenda poziomów:

0 – brak działań,
1 – pierwsze elementy zostały wdrożone,
2 – częściowe wdrożenie / działają podstawowe procesy,
3 – pełne wdrożenie / procedury funkcjonują na stałe,
4 – wysoka dojrzałość / automatyzacja.

Tabela 9.1 *Przykładowa macierz monitorowania i raportowania rezultatów działań z zakresu cyberbezpieczeństwa.*

Obszar	Wskaźnik	Opis pomiaru	Poziom (0–4)	Dane liczbowe
Szkolenia i świadomość.	Liczba przeszkolonych pracowników.	% pracowników, którzy odbyli szkolenie w ostatnich 12 mies.	0–4	np. 70%
	Cykl edukacyjny.	Czy podmiot prowadzi regularne szkolenia?	0–4	Liczba szkoleń / rok
	Cykl informacyjny.	Czy podmiot prowadzi regularną komunikację zagrożeń?	0–4	Liczba newsletterów / rok
Zarządzanie ryzykiem.	Ocena ryzyka.	Czy podmiot prowadzi formalną ocenę ryzyka?	0–4	Rok ostatniej oceny

Obszar	Wskaźnik	Opis pomiaru	Poziom (0–4)	Dane liczbowe
Policy & governance.	Polityka cyberbezpieczeństwa.	Czy istnieje, jest aktualna i znana pracownikom?	0–4	Data aktualizacji
	Zgodność z regulacjami.	Czy organizacja sprawdziła wpływ nowych regulacji na działalność oraz wdrożyła odpowiednie środki?	0–4	Wskazać pod jaką legislację podpadają oraz co zostało zrealizowane
Procedury reagowania.	Plan reagowania na incydenty.	Czy podmiot ma plan reakcji na incydent i testował go?	0–4	Liczba symulacji / rok
Kopie zapasowe.	Backup krytycznych danych.	Regularność i testowanie backupów.	0–4	Czy w przeciągu roku wykonano chociaż raz backup danych?
Ochrona techniczna.	Aktualizacje systemów.	Audyt urządzeń z aktualnym oprogramowaniem.	0–4	Czy w przeciągu roku wykonano chociaż raz audyt aktualizacji?
	Produkty i licencje.	Produkty z zakresu cyberbezpieczeństwa wdrożone w organizacji.	0–4	Czy w przeciągu roku wykonano chociaż raz audyt licencji produktów?
Dojrzałość organizacyjna.	Budżet na cyberbezpieczeństwo.	Czy podmiot przewiduje budżet / jego zwiększenie?	0–4	Czy planuje się zmniejszyć/pozostawić bez zmian/zwiększyć budżet?

Źródło: Opracowanie własne.

9.3 Rekomendowane narzędzia i źródła – lista portali, centrów kompetencji, materiałów szkoleniowych i innych sprawdzonych źródeł wiedzy

W miarę jak koordynator klastra rozwija działania w obszarze cyberbezpieczeństwa, kluczowe jest nie tylko promowanie świadomości i procesów, ale także udostępnianie wiarygodnych, praktycznych zasobów i materiałów edukacyjnych. Podmioty członkowskie często mają różny poziom wiedzy i doświadczenia – od menedżerów po dział IT – dlatego dostarczanie szerokiego wachlarza źródeł wiedzy jest fundamentem efektywnej strategii wsparcia.

W tym podrozdziale przedstawiono zestaw rekomendowanych portali, instytucji, centrów kompetencji i materiałów szkoleniowych, które mogą służyć jako baza wiedzy dla klastrów i ich członków. Zasoby te pozwalają na:

- aktualizację wiedzy o najnowszych zagrożeniach i trendach (raporty i analizy),
- szkolenia techniczne i organizacyjne,
- budowanie kompetencji cyberbezpieczeństwa w firmach, nawet tych, które dopiero zaczynają.

Poniższa lista zawiera instytucje i materiały rekomendowane ze względu na ich wiarygodność, aktualność i praktyczne zastosowanie. Do większości z nich można odwołać się w codzien-

nej pracy klastra – zarówno w ramach edukacji, jak i w kontekście tworzenia wspólnej platformy wymiany wiedzy lub analiz zagrożeń. Większość wspomnianych instytucji prowadzi swoje kanały na mediach społecznościowych (X, Facebook, Linkedin). Zaleca się śledzenie promowanych inicjatyw z ich strony.

Źródła:

- CERT Polska – jednostka publiczna której zadaniem jest reagowanie na incydenty w cyberprzestrzeni, publikujący raporty, poradniki i analizy zagrożeń: https://cert.pl.
- NASK-PIB – instytucja badawcza i edukacyjna, wspierająca krajowy system cyberbezpieczeństwa publikująca wiele analiz, ekspertyz i poradników: https://www.nask.pl/.
- Certyfikacja NASK – baza wiedzy odnośnie do wszelkich certyfikacji obowiązujących w branży cyberbezpieczeństwa: https://certyfikacja.nask.pl/.
- Firma Bezpieczna Cyfrowo – nowatorski program mający na celu wsparcie polskich przedsiębiorców w budowaniu kompetencji cyfrowych oraz podniesieniu poziomu cyberbezpieczeństwa w sektorze MŚP. Na stronie programu znajduje się darmowa ankieta, którą przedsiębiorcy oraz pozostałe organizacje mogą wypełnić w celu sprawdzenia swojej cyberodporności: https://firmabezpiecznacyfrowo.pl/diagnoza/.
- Ministerstwo Cyfryzacji – cyberbezpieczeństwo - oficjalny portal z informacjami legislacyjnymi, poradnikami i programami wsparcia: https://www.gov.pl/web/cyfryzacja. Ponadto zaleca się śledzenie newslettera Ministerstwa prowadzonego na portalu Linkedin.
- CSIRT KNF – zespół reagowania na incydenty bezpieczeństwa komputerowego sektora finansowego, działający przy Komisji Nadzoru Finansowego. Monitoruje zagrożenia cyberbezpieczeństwa dotyczące banków, ubezpieczycieli, fintechów itp., analizuje incydenty, ostrzega instytucje finansowe i wspiera je w reagowaniu na cyberataki: https://www.knf.gov.pl/dla_rynku/CSIRT_KNF.
- CERT Orange Polska – zespół bezpieczeństwa Orange Polska zajmuje się analizą zagrożeń oraz reagowaniem na incydenty dotyczące klientów Orange i infrastruktury telekomunikacyjnej w Polsce. CERT Orange prowadzi także działania edukacyjne oraz udostępnia raporty o cyberzagrożeniach: https://cert.orange.pl/.
- Program Cyfrowy Biznes realizowany przez Ministerstwo Rozwoju i Technologii – kompleksowy punkt informacyjno-usługowy, skierowany do polskich przedsiębiorców. Jego celem jest promowanie i wspieranie cyfryzacji firm oraz ułatwienie im korzystania z nowoczesnych technologii: https://cyfrowy.biznes.gov.pl/pl/portal/036142.
- Krajowe Centrum Kompetencji Cyberbezpieczeństwa (NCC-PL) – centrum szkoleniowe i kompetencyjne, oferujące programy rozwojowe i inicjatywy edukacyjne: https://www.gov.pl/web/cyber-nccpl.
- ENISA (Europejska Agencja ds. Cyberbezpieczeństwa) – zasoby raportów, analiz i publikacji na temat zagrożeń cybernetycznych w Europie: https://www.enisa.europa.eu/. ENISA opublikowała również poradnik po cyberbezpieczeństwie dla MŚP dostępny na stronie: https://www.gov.pl/web/baza-wiedzy/cyber-bezpieczna-firma--mamy-poradnik.

- Centrum Projektów Polska Cyfrowa – informacje o programach finansujących cyberbezpieczeństwo (dotacje, projekty klastrowe): https://www.gov.pl/web/cppc/aktualnosci-2025.

- PARP4DIGITAL – pełni funkcję głównego centrum wsparcia dla MŚP w procesie transformacji cyfrowej i wdrażania założeń Przemysłu 4.0. Jego podstawowym celem jest ułatwienie firmom adaptacji nowych technologii, aby zwiększyć ich konkurencyjność i efektywność operacyjną. Platforma ta oferuje kompleksowy zestaw narzędzi: od bezpłatnych narzędzi diagnostycznych, które pozwalają firmom ocenić ich aktualny poziom cyfryzacji, przez szereg darmowych szkoleń i kursów online w ramach Akademii PARP, po dostęp do specjalistycznego doradztwa w Hubach Innowacji Cyfrowych (EDIH): https://www.parp.gov.pl/component/site/site/4digital.

- Cyfrowa Wyprawka – kompendium wiedzy o cyfryzacji dla organizacji oraz mechanizmów ich wsparcia (finansowych i doradczych) zmapowane i zebrane w jednym miejscu: https://pfr.pl/cyfrowa-wyprawka. W ramach Cyfrowej Wyprawki PFR przygotował Test Dojrzałości Cyfrowej: https://pfr.pl/test-dojrzalosci-cyfrowej, dzięki któremu można sprawdzić mocne i słabe strony dotyczące cyfryzacji danego podmiotu.

- Polski Klaster Cyberbezpieczeństwa #CyberMadeInPoland – klaster zrzeszający polskich dostawców usług i rozwiązań z zakresu cyberbezpieczeństwa. Prowadzi liczne darmowe szkolenia oraz realizuje raporty branżowe: https://cybermadeinpoland.pl/.

- Zaufana Trzecia Strona – to jeden z czołowych i najbardziej rozpoznawalnych portali w Polsce, który koncentruje się wyłącznie na tematyce bezpieczeństwa teleinformatycznego. Serwis słynie z bardzo dokładnych analiz, śledzenia bieżących zagrożeń i publikowania artykułów pisanych przystępnym językiem: https://zaufanatrzeciastrona.pl/.

- Sekurak – to serwis internetowy, którego głównym celem jest edukacja i podnoszenie świadomości w zakresie cyberbezpieczeństwa. Na swoim blogu Sekurak publikuje artykuły i analizy dotyczące technicznych aspektów bezpieczeństwa, często skupiając się na testach penetracyjnych, technikach hakerskich i obronie przed nimi: https://sekurak.pl/.

- Niebezpiecznik – publikuje codzienne wiadomości, szczegółowe ostrzeżenia przed nowymi atakami (np. phishingowymi, czy ransomware) oraz poradniki. Serwis często wyróżnia się bezpośrednim językiem i koncentracją na praktycznym wymiarze bezpieczeństwa, oferując użytkownikom konkretne instrukcje, jak chronić swoje dane i urządzenia: https://niebezpiecznik.pl/.

- Podręcznik cyberbezpieczeństwa i odporności zrealizowany przez BW Advisory – praktyczny poradnik dla MŚP i większych organizacji wskazujący jak krok po kroku budować cyfrową odporność organizacji: https://www.itgrc.pl/pl/knowledgehub.

- Poradnik cyberbezpieczeństwa realizowany przez Sektorową Radę ds. Kompetencji Telekomunikacja i Cyberbezpieczeństwo – poradnik szeroko opisujący dobre praktyki z zakresu zwiększania zwojej cyberodporności: https://srtcb.radasektorowa.pl/541-poradnik-cyberbezpieczenstwa.

- CyberDefence24 – to polski portal informacyjny, który skupia się na problematyce cyberbezpieczeństwa, cyfryzacji i technologii, ale często w kontekście państwowym, militarnym i infrastruktury krytycznej. W odróżnieniu od portali

typowo konsumenckich, CyberDefence24 analizuje zagrożenia z perspektywy strategicznej, zajmując się m.in. bezpieczeństwem informacyjnym państwa, dezinformacją, rozwiązaniami technologicznymi w służbach mundurowych i armii, oraz ochroną danych w dużych instytucjach: https://cyberdefence24.pl/.

9.4. Przewodnik po narzędziach zaproponowanych w podręczniku

W niniejszym rozdziale przedstawiono zestaw narzędzi, które zostały wybrane i opisane w całym podręczniku jako praktyczne wsparcie w codziennej pracy koordynatora klastra. Ich dobór nie jest przypadkowy, stanowią one odpowiedź na najczęściej pojawiające się potrzeby, wyzwania i zadania, z jakimi mierzą się podmioty członkowskie oraz koordynatorzy klastrów w dążeniu do zwiększania cyberodporności swojego ekosystemu. Celem rozdziału jest zebranie wszystkich narzędzi w jednym miejscu w celu ułatwienia ich wykorzystania.

Tabela 9.2 *Zbiór narzędzi prezentowanych w podręczniku.*

Nazwa narzędzia	Nazwa narzędzia	Zlokalizowanie w podręczniku
Lista sprawdzająca do samoidentyfikacji podlegania podmiotów członkowskich pod zapisy Ustawy o Krajowym Systemie Cyberbezpieczeństwa (NIS2).	Lista sprawdzająca umożliwia samodzielne przeprowadzenie procesu samoidentyfikacji bez zagłębiania się w zapisy UKSC2. Lista ta nie wskazuje jednoznacznie, czy podmiot podlega pod ustawę, niemniej jest w stanie bardzo mocno nakierować podmiot do zgłębienia tematu.	Rozdział 2.2.
Macierz ryzyka cyber dla MŚP.	Macierz umożliwia zestawienie ryzyk z zakresu cyberbezpieczeństwa mogących wpłynąć na działalność danego podmiotu. Wypełnienie macierzy na podstawie znajomości danej organizacji może wspomóc wizualnie w priorytetyzacji działań.	Rozdział 2.5
Polityka tworzenia haseł w organizacji.	Polityka tworzenia haseł jest narzędziem, które można rozesłać do pracowników swojej organizacji w celu edukacyjnym np. jak tworzyć bardziej bezpieczne hasła.	Rozdział 4.2
Polityka tworzenia kopii zapasowych.	Polityka określa zasady tworzenia, przechowywania i testowania kopii zapasowych danych organizacji. Celem jest zapewnienie ciągłości działania firmy, ograniczenie skutków awarii, błędów ludzkich i ataków cybernetycznych (w tym ransomware).	Rozdział 4.2
Diagnoza poziomu cyberbezpieczeństwa członków klastra.	Skrócona wersja kwestionariusza do zbadania poziomu cyberbezpieczeństwa członków klastra. Na podstawie tej wersji możliwe jest także utworzenie benchmarku dla danego klastra pod kątem ogólnego poziomu cyberbezpieczeństwa jego członków.	Rozdział 5.1

Nazwa narzędzia	Nazwa narzędzia	Zlokalizowanie w podręczniku
Macierz oceny ryzyka w łańcuchu dostaw.	Macierz służy do identyfikacji ryzyka występującego w łańcuchu dostaw danego podmiotu. Pozwala na wstępną identyfikację ryzyk wynikających ze współpracy z partnerami na rynku. Macierz powinna zostać wypełniona także przez koordynatora klastra z uwzględnieniem ryzyk wynikających ze współpracy z członkami klastra.	Rozdział 5.2
Analiza ryzyka na podstawie sektora działalności członków klastra.	Przykładowa analiza ryzyka nastawiona na daną branżę gospodarki – dla klastrów jest to bezpośrednie odniesienie do ich branży działalności. Dobrze zrobiony benchmark może być dodatkowo materiałem promocyjnym do angażowania nowych członków ze względu na posiadanie unikatowej wiedzy z cyberbezpieczeństwa w danym sektorze.	Rozdział 5.3
Lista sprawdzająca dotycząca weryfikacji dostawcy IT / usług cyberbezpieczeństwa.	Lista sprawdzająca służy do weryfikacji jakości oraz bezpieczeństwa współpracy z danym dostawcą IT / usług cyberbezpieczeństwa. Ze względu na częste dostępy tych dostawców do kluczowych części infrastruktury sieciowej danego podmiotu, zakres bezpiecznej współpracy jest kluczowy dla zachowania ciągłości działania i wyboru partnera / dostawcy. Koordynator klastra może prowadzić takie listy sprawdzające i udostępniać wyniki członkom klastra wskazując zaufanych i sprawdzonych dostawców.	Rozdział 5.4
Lista sprawdzająca dotycząca dofinansowań z zakresu cyberbezpieczeństwa.	Lista sprawdzająca służy jako narzędzie do systematycznego sprawdzania (zalecane raz na miesiąc), aktualnych programów dofinansowań projektów z zakresu cyberbezpieczeństwa.	Rozdział 6.1.4
Ćwiczenie Table Top Exercise.	Przykładowe karty do realizacji ćwiczenia Table Top Exercise odnośnie do reagowania na atak na łańcuch dostaw w klastrze. Ćwiczenie może być dobrym wyjściem dla odmiennego podejścia do aspektu szkoleniowego.	Rozdział 7.3
Macierz monitorowania i raportowania efektywności cyberbezpieczeństwa.	Macierz służy jako narzędzie do wspólnego raportowania postępów realizacji zwiększania poziomu cyberbezpieczeństwa w danym klastrze. Usystematyzowanie odpowiedzi pozwoli na dalszą sprawną interpretację danych jako ogółu dla danego klastra.	Rozdział 9.2
Lista sprawdzająca dotycząca cyberbezpieczeństwa podmiotów członkowskich.	Lista sprawdzająca pozwala na szybkie sprawdzenie poziomu cyberbezpieczeństwa w podmiotach członkowskich oraz procesów wykorzystania poszczególnych rozwiązań.	Załącznik do poradnika

Źródło: Opracowanie własne.

Rozdział 10

Zakończenie

Cyberbezpieczeństwo to proces, czasem niełatwy i wymagający podjęcia wielu działań, ale z całą pewnością nierozerwalnie związany z transformacją cyfrową. Świadomość zagrożeń i umiejętności budowania cyberobrony stają się więc jednymi z kluczowych umiejętności, a klastry mogą być ważnymi organizacjami wspierającymi procesy budowania cyberodporności w szczególności małych i średnich przedsiębiorstw oraz infrastruktury krytycznej.

Należy podkreślić, że żaden klaster – nawet technologiczny – nie jest w stanie całkowicie wyeliminować ryzyk cyberbezpieczeństwa, ale stosując się do porad, technik i narzędzi zamieszczonych w podręczniku, może realnie ograniczyć te ryzyka i razem ze swoimi członkami zbudować efektywny ekosystem cyberbezpieczeństwa. Koordynator, wyposażony w podstawowe kompetencje, proste narzędzia i sprawdzone modele współpracy, jest w stanie podnieść poziom bezpieczeństwa swoich członków, budując jednocześnie kulturę odpowiedzialności cyfrowej wśród swoich członków i partnerów.

Najważniejsze, aby traktować cyberbezpieczeństwo jako proces, a nie jednorazowe działania: regularnie diagnozować potrzeby, szkolić pracowników i podmioty członkowskie, budować odporność operacyjną i rozwijać usługi, które odpowiadają na rosnące wymagania technologiczne polskich firm. Co istotne ważne, aby traktować cyberbezpieczeństwo nie jako zbędny koszt obciążający budżety, a jako inwestycję w ciągłość operacyjną firm i całych sektorów polskiej gospodarki, w szczególności w dobie dynamicznej transformacji cyfrowej i ery niepewności geopolitycznej w której się znajdujemy.

Słownik[130]

0-Day – atak lub luka w oprogramowaniu, która jest wykorzystywana zanim zostanie naprawiona przez producenta.

ADMA – metodologia ADMA (ang. ADvanced MAnufacturing Assessment, tłum. zaawansowana produkcja) ukierunkowana jest na analizę poziomu zaawansowania/dojrzałości przedsiębiorstw produkcyjnych (w szczególności MŚP) oraz tworzenie efektywnych planów ich transformacji w kierunku Fabryk Przyszłości[131].

APT – Advanced Persistent Threat; zaawansowane i długotrwałe cyberzagrożenie ukierunkowane przeciwko konkretnej organizacji.

ARP – Agencja Rozwoju Przemysłu to polska państwowa instytucja, która wspiera rozwój przedsiębiorstw i przemysłu. Oferuje m.in. finansowanie (pożyczki, leasing), usługi doradcze oraz programy wspierające innowacje, restrukturyzację firm i tworzenie nowych miejsc pracy

BCP (ang. Business Continuity Plan, tłum. plan ciągłości działania) – to zestaw procedur i instrukcji pozwalających organizacji utrzymać lub szybko przywrócić kluczowe procesy biznesowe po incydencie, awarii lub katastrofie.

Botnet – sieć zainfekowanych komputerów kontrolowanych przez cyberprzestępców w celu przeprowadzania ataków lub rozsyłania spamu.

CER (Critical Entities Resilience Directive) – unijna dyrektywa dotycząca odporności podmiotów krytycznych, która ma na celu wzmocnienie ich fizycznej odporności i zdolności do przetrwania w obliczu różnorodnych zagrożeń, takich jak klęski żywiołowe, ataki terrorystyczne, sabotaż, czy zagrożenia zdrowia publicznego.

CERT – Computer Emergency Response Team; zespół monitorujący, analizujący i reagujący na incydenty cyberbezpieczeństwa.

CPPC – Centrum Projektów Polska Cyfrowa; instytucja wspierająca finansowanie i realizację projektów cyfryzacyjnych w Polsce.

CRA – Cyber Resilience Act; unijne Rozporządzenie nr 2024/2847 ws. horyzontalnych wymagań w zakresie cyberbezpieczeństwa w odniesieniu do produktów z elementami cyfrowymi.

130 Definicje w słowniku zostały przygotowane przez autorów podręcznika.

131 Polska Agencja Rozwoju Przedsiębiorczości, (2024) „Ankieta samooceny – Skan ADMA" [artykuł online]. Dostęp: https://www.parp.gov.pl/component/content/article/88254:ankieta-samooceny-skan-adma. (2 grudnia 2025)

CRM – Customer Relationship Management; systemy i procesy do zarządzania relacjami z klientami, często wrażliwe na ataki.

CSIRT – Computer Security Incident Response Team; zespół reagujący na incydenty bezpieczeństwa w organizacji.

CTI (ang. Cyber Threat Intelligence, tłum. Wywiad o Zagrożeniach Cybernetycznych) – proces zbierania, analizowania i udostępniania informacji o aktualnych i potencjalnych zagrożeniach w cyberprzestrzeni w celu zwiększenia bezpieczeństwa systemów i danych organizacji.

DDoS – Distributed Denial of Service; atak polegający na przeciążeniu usług sieciowych poprzez masowy ruch z wielu źródeł.

DORA – Digital Operational Resilience Act; europejska regulacja dotycząca odporności cyfrowej instytucji finansowych.

DRP (ang. Disaster Recovery Plan, tłum. plan odzyskiwania po katastrofie) – dokument określający procedury i działania niezbędne do przywrócenia działania systemów IT po poważnej awarii lub katastrofie.

Due Diligence – proces szczegółowej analizy i oceny podmiotu, projektu lub usługi (np. dostawcy technologii), mający na celu zidentyfikowanie ryzyk, weryfikację zgodności oraz potwierdzenie wiarygodności przed podjęciem decyzji biznesowej.

EDIH – European Digital Innovation Hub; centrum wsparcia cyfrowego dla MŚP i instytucji wspierające innowacje i transformację cyfrową.

EDR – Endpoint Detection and Response; system wykrywający i reagujący na zagrożenia w punktach końcowych sieci.

ENISA – European Union Agency for Cybersecurity; agencja UE zajmująca się cyberbezpieczeństwem i publikująca raporty, analizy i wytyczne.

ERP (Enterprise Resource Planning) – system informatyczny wspomagający zarządzanie zasobami przedsiębiorstwa, integrujący kluczowe obszary działalności firmy, takie jak finanse, kadry, produkcja, logistyka i sprzedaż, w jednym spójnym środowisku.

Heatmap (mapa ciepła) – graficzne narzędzie wizualizacji danych, w którym natężenie kolorów odzwierciedla skalę ryzyka, priorytetów lub innych wartości, ułatwiając szybkie identyfikowanie obszarów wymagających uwagi.

ICS – Industrial Control System; systemy sterowania procesami przemysłowymi, często krytyczne dla infrastruktury.

IoT – Internet of Things; urządzenia podłączone do internetu, które mogą stać się celem ataków.

IP (ang. Intellectual Property, tłum. własność intelektualna) – prawa przysługujące twórcom i właścicielom rezultatów działalności intelektualnej, takich jak patenty, znaki towarowe, prawa autorskie czy know-how, chroniące innowacje, pomysły i produkty przed nieuprawnionym wykorzystaniem.

ISAC – Information Sharing and Analysis Center; organizacja wymieniająca informacje o zagrożeniach w określonej branży lub sektorze.

ISO 27001 – międzynarodowy standard zarządzania bezpieczeństwem informacji w organizacjach.

ISO 22301 – międzynarodowy standard zarządzania ciągłością działania.

JST – Jednostka Samorządu Terytorialnego; administracyjny podmiot publiczny w Polsce.

MDM – Mobile Device Management; system do zarządzania urządzeniami mobilnymi w organizacji.

MFA – Multi-Factor Authentication; uwierzytelnianie wieloskładnikowe zwiększające bezpieczeństwo dostępu do systemów.

mObywatel – aplikacja mobilna udostępniająca cyfrowe dokumenty i usługi publiczne dla obywateli w Polsce.

NASK-PIB – Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy; instytucja wspierająca bezpieczeństwo cyfrowe i edukację w Polsce.

NDR – Network Detection and Response; system monitorujący sieć w celu wykrywania i reagowania na zagrożenia.

NIS2 – Dyrektywa UE w sprawie bezpieczeństwa sieci i systemów informacyjnych; regulacja zwiększająca wymogi cyberbezpieczeństwa w UE.
OT – Operational Technology; technologie i systemy sterujące procesami przemysłowymi i fizycznymi.

OWU – Ogólne Warunki Ubezpieczenia; dokument określający zakres i zasady ubezpieczenia organizacji.

PAM – Privileged Access Management; system zarządzania dostępem uprzywilejowanym w organizacji w celu ograniczenia ryzyka nadużyć.

PESTEL – Political, Economic, Social, Technological, Environmental, Legal; analiza czynników makroekonomicznych wpływających na organizację.

PPP – Public-Private Partnership; partnerstwo publiczno-prywatne w realizacji projektów lub usług.

PPT (People, Process, Technology) – model zarządzania bezpieczeństwem lub zmianą organizacyjną, który zakłada równoczesne doskonalenie trzech kluczowych obszarów: ludzi, procesów i technologii w celu osiągnięcia trwałych i skutecznych rezultatów.

RODO – Rozporządzenie o Ochronie Danych Osobowych; europejskie przepisy dotyczące ochrony danych osobowych.

RPO (ang. Recovery Point Objective, tłum. docelowy punkt odzyskiwania) – maksymalna akceptowalna ilość danych, które mogą zostać utracone w wyniku awarii, określająca punkt w czasie, do którego należy odtworzyć dane z kopii zapasowej.

RTO (ang. Recovery Time Objective, tłum. docelowy czas odzyskiwania) – maksymalny dopuszczalny czas, w którym systemy lub usługi muszą zostać przywrócone po awarii, aby zminimalizować straty dla organizacji.

SCADA – Supervisory Control and Data Acquisition; systemy nadzorujące i sterujące procesami przemysłowymi.

SIEM – Security Information and Event Management; system do zbierania, analizy i raportowania zdarzeń bezpieczeństwa w sieci.

SLA (ang. Service Level Agreement, tłum. umowa o poziomie usług) – umowa o gwarantowanym poziomie świadczenia usług między dostawcą a odbiorcą, określająca m.in. dostępność systemów, czas reakcji, jakość usług oraz zasady odpowiedzialności za ich niewykonanie.

SOC – Security Operations Center; centrum monitorowania i reagowania na incydenty bezpieczeństwa.

SQL – Structured Query Language; język zapytań do baz danych, podatny na ataki typu SQL Injection.

SWOT – Strengths, Weaknesses, Opportunities, Threats; analiza mocnych i słabych stron oraz szans i zagrożeń organizacji.

SZCD – System Zarządzania Ciągłością Działania; system zarządzania procesami i procedurami BCP w organizacji.

System CEPIK – Centralna Ewidencja Pojazdów i Kierowców; krajowy system gromadzący dane o pojazdach i kierowcach w Polsce.

UKSC2 – nowelizacja Ustawy o Krajowym Systemie Cyberbezpieczeństwa wdrażająca zapisy Dyrektywy NIS2.

VPN – Virtual Private Network; wirtualna sieć prywatna umożliwiająca bezpieczny zdalny dostęp do zasobów sieciowych.

Spis tabel

Tabela 2.1. Wykaz sektorów objętych Nowelizacją Ustawy o Krajowym Systemie Cyberbezpieczeństwa na podstawie projektu nowelizacji Ustawy o Krajowym Systemie Cyberbezpieczeństwa z dnia 7 października 2025 r. 27
Tabela 2.2 Przykładowa checklista wspomagająca proces samoidentyfikacji podmiotów. 27
Tabela 2.3 Zestawienie środków organizacyjnych i technicznych zgodnie z Art. 8 nowelizacji UKSC. 29
Tabela 2.4. Kwalifikacja sektorowa Krajowych Klastrów Kluczowych pod kątem NIS2/UKSC2. 31
Tabela 2.5 Przykładowa macierz ryzyka cyberbezpieczeństwa dla MŚP. 38
Tabela 2.6 Obszary wsparcia członków klastra w obszarze ubezpieczeń cybernetycznych 39
Tabela 3.1 Zalety i wady ankietowania podmiotów członkowskich w celu badania ich cyberodporności. 41
Tabela 3.2 Zalety i wady proaktywnego podejścia w badaniu cyberodporności podmiotów członkowskich. 43
Tabela 3.3 Podsumowanie porównawcze narzędzi diagnozy cyberodporności. 44
Tabela 3.4 Schematy nawiązywania relacji oraz realizacji współpracy z ekspertami, dostawcami produktów i usług oraz podmiotami administracji publicznej. 46
Tabela 3.5 *Zalety oraz wady ISAC klastra.* *49*
Tabela 4.1 Rodzaje ataków i ich konsekwencje dla klastra. 51
Tabela 9.1 Przykładowa macierz monitorowania i raportowania rezultatów działań z zakresu cyberbezpieczeństwa. 111
Tabela 9.2 Zbiór narzędzi prezentowanych w podręczniku. 115

Spis rysunków

Rysunek 1.1 Triada CIA. 10
Rysunek 1.2 Uproszczony atak z wykorzystaniem oprogramowania ransomware. 15
Rysunek 1.3 Mapa interesariuszy w kontekście cyberbezpieczeństwa klastra. 23
Rysunek 3.1 Schemat roli koordynatora klastra w ISAC klastrowym. 48
Rysunek 4.1 Główne zasady cyberhigieny. 55
Rysunek 5.1 63
Rysunek 7.1 Schemat wymiany doświadczeń między klastrami. 93

Bibliografia

1. Akamai, „What Is a Web Application Attack” [artykuł online]. Dostęp: https://www.akamai.com/glossary/what-is-a-web-application-attack. (24.11.2025)
2. Baker, Kurt, (2023) „The 12 Most Common Types of Malware” [artykuł online]. Dostęp: https://www.crowdstrike.com/en-us/cybersecurity-101/malware/types-of-malware/. (28 listopada 2025)
3. Baramundi, „Złośliwe oprogramowanie (malware)” [artykuł online]. Dostęp: https://www.baramundi.com/pl-pl/zasoby/slowniczek/pojecie/malware/. (24 listopada 2025)
4. Bochyńska, Nikola, (2022) „Walka ze spoofingiem w Polsce. Komendant CBZC: „Kampania przygotowana pod znane osoby i spersonalizowana” [artykuł online]. Dostęp: https://cyberdefence24.pl/armia-i-sluzby/walka-ze-spoofingiem-w-polsce-komendant-cbzc-kampania-przygotowana-pod-znane-osoby-i-spersonalizowana. (28 listopada 2025)
5. Centralne Biuro Zwalczania Cyberprzestępczości, „Ataki typu DDoS (Distributed Denial of Service)” [artykuł online]. Dostęp: https://cbzc.policja.gov.pl/bzc/zagrozenia-w-sieci/458,Atak-typu-DDoS--Distributed-Denial-of-Service.html. (24 listopada 2025)
6. Centrum Projektów Polska Cyfrowa, Ogłoszenie naboru do działania: „Cyberbezpieczny Samorząd“. Dostęp: https://www.gov.pl/web/cppc/cyberbezpieczny-samorzad. (20 listopada 2025)
7. Centrum Projektów Polska Cyfrowa, Ogłoszenie naboru do działania: „Inwestycja C3.1.1. Konkurs Grantowy–Cyberbezpieczny Rząd”. Dostęp: https://www.gov.pl/web/cppc/inwestycja-c-311-konkurs-grantowy-cyberbezpieczny-rzad. (20 listopada 2025)
8. CERT Polska, „Mroczny rycerz powraca: Analiza złośliwego oprogramowania Joker” [artykuł online]. Dostęp: https://cert.pl/posts/2024/10/analiza-joker/. (24 listopada 2025)
9. Checkpoint, „Wi-Fi Hacking: How It Works, and How to Stay Secure” [artykuł online]. Dostęp: https://www.checkpoint.com/cyber-hub/cyber-security/what-is-hacking/wi-fi-hacking-how-it-works--and-how-to-stay-secure/. (24.11.2025)
10. Chudziński, Paweł, „Czym jest malware i jak chronić się przed jego atakami” [artykuł online]. Dostęp: https://securivy.com/blog/malware/#Jak_chronic_sie_przed_szkodliwym_oprogramowaniem. (24 listopada 2025)
11. ComCert, „Socjotechnika, czyli włamanie do naszych emocji” [artykuł online]. Dostęp: https://www.comcert.pl/socjotechnika-czyli-wlamanie-do-naszych-emocji/. (24 listopada 2025)
12. Cyber Ireland, (2023) „Cyber4Am – Cyber Security for Advanced Manufactoring & IN4.0”. Dostęp: https://cyberireland.ie/wp-content/uploads/2024/02/Cyber4AM-Summary-Report.pdf. (24 listopada 2025)
13. Cyber Ireland, „Cyber4Am – Cyber Security for Advanced Manufactoring & IN4.0” [artykuł online]. Dostęp: https://cyberireland.ie/cyber-security-for-advanced-manufacturing/. (24 listopada 2025)
14. Cyber Resilience Act. Dostęp: https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act. (24 listopada 2024)
15. DAGMA Bezpieczeństwo IT, Raport „Cyberportret polskiego biznesu 2025”. Dostęp: https://in.eset.pl/cyberportret-polskiego-biznesu. (24 listopada 2025)
16. DAGMA Bezpieczeństwo IT, Raport „Cyberportret polskiego biznesu 2025”, Dostęp: https://in.eset.pl/cyberportret-polskiego-biznesu. (24 listopada 2025)

17. Directorate-General for Communications Networks, Content and Technology, (2025) „ECCC to finance EUR 390 million in cybersecurity projects under Digital Europe Programme for 2025-2027". Dostęp: https://cybersecurity-centre.europa.eu/news/eccc-finance-eur-390-million-cybersecurity-projects-under-digital-europe-programme-2025-2027-2025-03-28_en. (26 listopada 2025)
18. Dowództwo Komponentu Wojsk Obrony Cyberprzestrzeni, „Przebieg ataku oraz zabezpieczanie przed ransomware" [artykuł online]. Dostęp: https://www.wojsko-polskie.pl/woc/articles/publikacje-r/przebieg-ataku-oraz-zabezpieczanie-przed-ransomware/. (24 listopada 2025)
19. Dyrektywa (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 (NIS2). Dz.U. L 333 z 27.12.2022. Dostęp: https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32022L2555. (24 listopada 2025)
20. European Union Agency for Cybersecurity, (2024) „Enisa Threat Landscape 2024" [artykuł online]. Dostęp: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024. (17 listopada 2025)
21. EY, „Phishing – co to jest i jak reagować na oszustwa internetowe?" [artykuł online]. Dostęp: https://www.ey.com/pl_pl/insights/consulting/phishing-co-to-jest#definicja. (24 listopada 2025)
22. F-secure, „Mobile Malware" [artykuł online]. Dostęp: https://www.f-secure.com/en/articles/mobile-malware. (24.11.2025)
23. Findia, „Ubezpieczenia cyber". Dostęp: https://findia.pl/ubezpieczenie-cyber?gad_source=1&gad_campaignid=9889458441&gbraid=0AAAACb46qf7rIDzHtHg_OnW_6gv6mtIH&gclid=Cj0KCQiArOvIBhDLARIsAPwJXObfQGSSnMP7YRZNqPM8K7eM58s_OD7G1y_HtDlfoZJpL6MLWZex8jkaAo_GEALw_wcB. (24 listopada 2025)
24. ISO, „ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems – Requirements". Dostęp: https://www.iso.org/standard/27001. (24 listopada 2025)
25. ISO, „Security and resilience — Business continuity management systems — Requirements ISO/IEC 22301:2019". Dostęp: https://www.iso.org/standard/75106.html. (24 listopada 2025)
26. Keepersecurity, „Czym jest atak na łańcuch dostaw?" [artykuł online]. Dostęp: https://www.keepersecurity.com/pl_PL/threats/supply-chain-attack/. (24 listopada 2025)
27. Kklimczuk, Oskar, (2025) „Atak na Urząd Miasta w Wadowicach. Wysokie ryzyko kradzieży danych" [artykuł online]. Dostęp: https://cyberdefence24.pl/cyberbezpieczenstwo/atak-na-urzad-miasta-w-wadowicach-wysokie-ryzyko-kradziezy-danych. (28 listopada 2025)
28. Krajowe Centrum Kompetencji Cyberbezpieczeństwa, „Europejskie huby innowacji cyfrowych (European Digital Innovation Hub, EDIH)" [artykuł online]. Dostęp: https://www.gov.pl/web/cyber-nccpl/europejskie-huby-innowacji-cyfrowych-european-digital-innovation-hub-edih. (20 listopada 2025)
29. Lista Krajowych Klastrów Kluczowych [artykuł online]. Dostęp: https://www.gov.pl/web/rozwoj-technologia/lista-kkk. (24 listopada 2025)
30. Makowiec, Paweł, (2024), „Wyłudzał dane logowania od pasażerów samolotów. Wszystko dzięki Wi-Fi" [artykuł online]. Dostęp: https://cyberdefence24.pl/cyberbezpieczenstwo/wyludzal-dane-logowania-od-pasazerow-samolotow-wszystko-dzieki-wi-fi. (28 listopada 2025)
31. Makowiec, Paweł, (2025) „Cyberatak na gminy. Sprawcy podszywają się pod ministerstwo" [artykuł online]. Dostęp: https://cyberdefence24.pl/cyberbezpieczenstwo/cyberatak-na-gminy-sprawcy-podszywaja-sie-pod-ministerstwo. (28 listopada 2025)

32. Makowiec, Paweł, (2025) „Kolejny atak DDoS na system BLIK" [artykuł online]. Dostęp: https://cyberdefence24.pl/cyberbezpieczenstwo/kolejny-atak-ddos-na-system-blik. (28 listopada 2025)
33. Marszycki, Mikołaj, „Zmasowany atak DDos na polskie e-usługi: mObywatel i CEPIK" [artykuł online]. Dostęp: https://itwiz.pl/zmasowany-atak-ddos-na-polskie-e-uslugi-mobywatel-i-cepik/. (24 listopada 2025)
34. Microsoft, „Co to jest atak DDos?" [artykuł online]. Dostęp: https://www.microsoft.com/pl-pl/security/business/security-101/what-is-a-ddos-attack. (24.11.2025)
35. Microsoft, „Wprowadzenie do bezpieczeństwa w chmurze" [artykuł online]. Dostęp: https://www.microsoft.com/pl-pl/security/business/security-101/what-is-cloud-security. (24.11.2025)
36. Ministerstwo Cyfryzacji, (2023) „Oszustwa typu BEC" [artykuł online]. Dostęp: https://www.gov.pl/web/cyfryzacja/oszustwa-typu-bec. (2 grudnia 2025)
37. Ministerstwo Cyfryzacji, (2024) „Udział Ministerstwa Cyfryzacji w ćwiczeniach Cyber Europe 2024" [artykuł online]. Dostęp: https://www.gov.pl/web/cyfryzacja/udzial-ministerstwa-cyfryzacji-w-cwiczeniach-cyber-europe-2024. (26 listopada 2025)
38. Ministerstwo Cyfryzacji, „Czym jest spoofing? Jak go rozpoznać i nie dać się nabrać?" [artykuł online]. Dostęp: https://www.gov.pl/web/cyfryzacja/czym-jest-spoofing--jak-go-rozpoznac-i-nie-dac-sie-nabrac. (24.11.2025)
39. Ministerstwo Cyfryzacji, „Jak zapobiegać atakom typu ransomware? – Poradnik PRCyber-03" [artykuł online]. Dostęp: https://www.gov.pl/web/baza-wiedzy/jak-zapobiegac-atakom-typu-ransomware---poradnik-prcyber-03. (24 listopada 2025)
40. Ministerstwo Cyfryzacji, „Łagodzenie skutków ataków szkodliwego oprogramowania" [artykuł online]. Dostęp: https://www.gov.pl/web/baza-wiedzy/lagodzenie-skutkow-atakow-szkodliwego-oprogramowania. (24.11.2025)
41. Ministerstwo Cyfryzacji, „Ransomware – jedno z najpoważniejszych zagrożeń w cyberprzestrzeni" [artykuł online]. Dostęp: https://www.gov.pl/web/baza-wiedzy/ransomware--jedno-z-najpowazniejszych-zagrozen-w-cyberprzestrzeni. (24 listopada 2025)
42. Ministerstwo Cyfryzacji, „Rosyjskie cyberataki" [artykuł online]. Dostęp: https://www.gov.pl/web/sluzby-specjalne/rosyjskie-cyberataki. (24 listopada 2025)
43. NASK, „BiuletynNASK". Dostęp: https://www.linkedin.com/newsletters/biuletyn-nask-7048947139384623104/. (24 listopada 2025)
44. NASK, „Inteligentne sprzęty domowe potrafią nas przechytrzyć. Zbierają dane, mogą ułatwić dostęp do konta" [artykuł online]. Dostęp: https://www.nask.pl/magazyn/inteligentne-sprzety-domowe-potrafia-nas-przechytrzyc-moga-ulatwic-cyberprzestepcom-dostep-do-konta. (24 listopada 2025)
45. NASK, Poradnik „Firma Bezpieczna Cyfrowo" [artykuł online]. Dostęp: https://firmabezpiecznacyfrowo.pl/poradnik/#1. (24 listopada 2025)
46. nFlo, „Bezpieczeństwo sieci OT: analiza, różnice z IT, zagrożenia i najlepsze praktyki" [artykuł online]. Dostęp: https://nflo.pl/baza-wiedzy/bezpieczenstwo-sieci-ot-analiza-roznice-z-it-zagrozenia-i-najlepsze-praktyki/#jakie-zagrozenia-cybernetyczne-zagrazaja-sieciom-przemyslowym. (24 listopada 2025)
47. nFlo, „Co to jest 0-Day exploit" [artykuł online]. Dostęp: https://nflo.pl/slownik/0-day-exploit/#strong-co-to-jest-0-day-exploit-definicja-strong. (24 listopada 2025)
48. Niebezpiecznik, „Atak na klientów 9000 różnych polskich sklepów internetowych" [artykuł online]. Dostęp: https://niebezpiecznik.pl/post/atak-na-klientow-9000-roznych-polskich-sklepow-internetowych/. (24 listopada 2025)

49. ODO24.pl, „Przykłady phishingu – analiza najczęstszych błędów użytkowników” [artykuł online]. Dostęp: https://odo24.pl/blog-post.przyklady-phishingu. (24 listopada 2025)
50. Olszewska, Monika, (2025) „Natalia Sikora oszukana ‘na Anthony’ego Hopkinsa’! 39-letnia wokalistka straciła mnóstwo pieniędzy” [artykuł online]. Dostęp: https://tvn.pl/gwiazdy/natalia-sikora-ofiara-oszustwa-na-anthony-ego-hopkinsa-wokalistka-myslala-ze-dostala-zyciowa-szanse-st8752674. (28 listopada 2025)
51. Pachucki, M., (2025) „CIA, ale nie ta z Langley: triada, na której oparte jest bezpieczeństwo informacji” [artykuł online]. Dostęp: https://cybershieldon.pl/cia-%E2%80%93-ale-nie-ta-z-langley-triada-na-ktorej-oparte-jest-bezpieczenstwo-informacji. (17 listopada 2025)
52. Palczewski, Szymon, (2025) „Oszustwo na PKO BP. Wschodni akcent w słuchawce” [artykuł online]. Dostęp: https://cyberdefence24.pl/cyberbezpieczenstwo/oszustwo-na-pko-bp-wschodni-akcent-w-sluchawce. (28 listopada 2025)
53. Pentest Tools Blog, (2024) „Breaking down the 5 most common SQL injection attacks” [artykuł online]. Dostęp: https://pentest-tools.com/blog/sql-injection-attacks. (28 listopada 2025)
54. Polska Agencja Rozwoju Przedsiębiorczości, (2024) „Ankieta samooceny – Skan ADMA” [artykuł online]. Dostęp: https://www.parp.gov.pl/component/content/article/88254:ankieta-samooceny-skan-adma. (2 grudnia 2025)
55. Polska Agencja Rozwoju Przedsiębiorczości, „Europejskie Centra Innowacji Cyfrowych (EDIH)” [artykuł online]. Dostęp: https://www.parp.gov.pl/component/site/site/edih#mapa. (24 listopada 2025)
56. Polska Agencja Rozwoju Przedsiębiorczości, „Europejskie Centra Innowacji Cyfrowych (EDIH)” [artykuł online]. Dostęp: https://www.parp.gov.pl/component/site/site/edih#mapa. (28 listopada 2025)
57. Polska Agencja Rozwoju Przedsiębiorczości, Kursy online. Dostęp: https://www.parp.gov.pl/component/site/site/kursy-online. (28 listopada 2025)
58. Portal informacyjny archiwalnego naboru do konkursu „Dig.IT”. Dostęp: https://digit.arp.pl/. (20 listopada 2025)
59. Portal informacyjny o Krajowym Planie Odbudowy, Aktualności, [artykuł online]. Dostęp: https://www.kpo.gov.pl/strony/aktualnosci/projekt-ustawy-o-funduszu-bezpieczenstwa-i-obronnosci-fbio-w-sejmie/. (20 listopada 2025)
60. Portal informacyjny dotyczący Kredytu Technologicznego. Dostęp: https://www.bgk.pl/produkty/kredyt-technologiczny/. (20 listopada 2025)
61. Portal informacyjny Programu „Cyfrowa Europa”. Dostęp: https://digital-strategy.ec.europa.eu/pl/activities/digital-programme. (20 listopada 2025)
62. Portal Informacyjny dotyczący Funduszy Europejskich dla Nowoczesnej Gospodarki. Dostęp: https://www.nowoczesnagospodarka.gov.pl/. (20 listopada 2025)
63. Portal Informacyjny Inicjatywy STEP. Dostęp: https://www.parp.gov.pl/component/site/site/step#konkursy. (26 listopada 2025)
64. Portal Informacyjny Programu „Cyfrowa Europa”. Dostęp: https://digital-strategy.ec.europa.eu/en/activities/work-programmes-digital. (26 listopada 2025)
65. Przykłady fałszywych SMS można znaleźć na stronie CERT Polska. Dostęp: https://cert.pl/baza-wiedzy/falszywe-smsy/. (24 listopada 2025)
66. Projekt Ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (projekt z dnia 7 października 2025 r.). Dostęp: https://legislacja.gov.pl/projekt/12384504/katalog/13055207. (24 listopada 2025)

67. Resilia, „Normy ISO w firmie: czym są? Wszystko o normach ISO, wdrażaniu i certyfikatach” [artykuł online]. Dostęp: https://resilia.pl/blog/normy-iso-definicja-rodzaje-czy-warto-wdrazac/. (24 listopada 2025)
68. Rogalewicz, Mikołaj, (2025) „Nowy malware na Androida. Jest w stanie naśladować człowieka” [artykuł online]. Dostęp: https://cyberdefence24.pl/cyberbezpieczenstwo/nowy-malware-na-androida-jest-w-stanie-nasladowac-czlowieka. (28 listopada 2025)
69. Rozporządzenie (UE) 2019/881 w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych. Dz.U. L 151 z 07.06.2019. Dostęp: https://eur-lex.europa.eu/legal-content/PL/ALL/?uri=CELEX:32019R0881. (24 listopada 2025)
70. Rozporządzenie (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego oraz zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014 i (UE) 2019/2033. Dz.U. L 333 z 27.12.2022. Dostęp: https://eur-lex.europa.eu/legal-content/PL/ALL/?uri=CELEX:32022R2554. (24 listopada 2025)
71. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/2847 z dnia 23 października 2024 r. w sprawie horyzontalnych wymagań w zakresie cyberbezpieczeństwa w odniesieniu do produktów z elementami cyfrowymi oraz w sprawie zmiany rozporządzeń (UE) nr 168/2013 i (UE) 2019/1020 i dyrektywy (UE) 2020/1828 (akt o cyberodporności). Dostęp: https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng. (24 listopada 2025)
72. Rządowy projekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw. Dostęp: https://www.sejm.gov.pl/sejm10.nsf/agent.xsp?symbol=RPL&Id=RM-0610-195-25. (17 listopada 2025)
73. Samodzielna ocena poziomu jakości i bezpieczeństwa usług cyfrowych dostępna na stronie internetowej NASK. Dostęp: https://firmabezpiecznacyfrowo.pl/diagnoza/. (24 listopada 2025)
74. Sekurak, „Jedna z największych korporacji z branży ochrony zdrowia w USA zapłaciła $ 22 000 000 okupu ransomware. Dostali do nich z wykorzystaniem wykradzionych danych logowanie. Change Healthcare” [artykuł online]. Dostęp: https://sekurak.pl/jedna-z-najwiekszych-korporacji-z-branzy-ochrony-zdrowia-w-usa-zaplacila-22000000-okupu-ransomware-dostali-sie-do-nich-z-wykorzystaniem-wykradzionych-danych-logowania-change-healthcare/. (24 listopada 2025)
75. Serwis Rzeczypospolitej Polskiej, (2024) „KSC-EXE 2024: ćwiczenia krajowego systemu cyberbezpieczeństwa 2024” [artykuł online]. Dostęp: https://www.gov.pl/web/baza-wiedzy/ksc-exe-2024-cwiczenia-krajowego-systemu-cyberbezpieczenstwa. (26 listopada 2025)
76. Serwis Rzeczypospolitej Polskiej, „Cyberbezpieczny Wodociąg założenia nowego konkursu grantowego ze środków KPO” [artykuł online]. Dostęp: https://www.gov.pl/web/baza-wiedzy/cyberbezpieczny-wodociag-zalozenia-nowego-konkursu-grantowego-ze-srodkow-kpo. (20 listopada 2025)
77. Serwis Rzeczypospolitej Polskiej, „Informacja o szkoleniach dla podmiotów krajowego systemu cyberbezpieczeństwa” [artykuł online]. Dostęp: https://www.gov.pl/web/baza-wiedzy/harmonogramszkolen. (28 listopada 2025)
78. Strona informacyjna archiwalnego naboru do konkursu „Rozwój oferty klastrów dla firm - nabór dla koordynatorów Krajowych Klastrów Kluczowych” (2025). Dostęp: https://www.parp.gov.pl/component/grants/grants/rozwoj-oferty-klastrow-dla-firm-nabor-dla-koordynatorow-krajowych-klastrow-kluczowych. (24 listopada 2025)

79. Strona Informacyjna archiwalnego naboru do konkursu „Rozwój oferty klastrów dla firm - nabór dla koordynatorów Krajowych Klastrów Kluczowych” (2025). Dostęp: https://www.parp.gov.pl/component/grants/grants/rozwoj-oferty-klastrow-dla-firm-nabor-dla-koordynatorow-krajowych-klastrow-kluczowych. (28 listopada 2025)
80. Strona informacyjna dotycząca EDIH-u Cybersec. Dostęp: https://cyber-sec.net.pl. (21 listopada 2025)
81. Strona informacyjna dotycząca EDIH-u Hub4Industry. Dostęp: https://hub4industry.pl/. (21 listopada 2025)
82. Strona informacyjna dotycząca EDIH-u Koalicja dla Innowacji. Dostęp: https://koalicjadlainnowacji.pl/wama-edih/wyszukiwarka-uslug/. (21 listopada 2025)
83. Strona informacyjna dotycząca EDIH-u rethink digital hub. Dostęp: https://re-d.pl/#uslugi. (21 listopada 2025)
84. Strona informacyjna dotycząca EDIH-u Silesian Smart Systems. Dostęp: https://www.silesiasmart-systems.pl/start-3836?lang_id=10. (21.11.2025)
85. Strona informacyjna dotycząca EDIH-u Wro4digITal. Dostęp: https://www.technologpark.pl/edih/. (21 listopada 2025)
86. Strona internetowa CERT Polska. Dostęp: https://cert.pl/falszywe-zalaczniki/. (24 listopada 2025)
87. Strona internetowa CERT Polska. Dostęp: https://cert.pl/posts/2023/04/phishing-webmail/. (24 listopada 2025)
88. Strona internetowa CSO Council. Dostęp: https://csoc.pl/. (26 listopada 2025)
89. Strona internetowa Cyber Threat Alliance. Dostęp: https://www.cyberthreatalliance.org/. (26 listopada 2025)
90. Strona internetowa Cybersecurity Advisors Network. Dostęp: https://cybersecurityadvisors.network/. (26 listopada 2025)
91. Strona internetowa Cyfrowa Polska. Dostęp: https://cyfrowapolska.org/. (26 listopada 2025)
92. Strona internetowa Digitalsme. Dostęp: https://www.digitalsme.eu/. (26 listopada 2025)
93. Strona internetowa ECSO. Dostęp: https://ecs-org.eu/. (26 listopada 2025)
94. Strona internetowa Euroklastra SGG. Dostęp: https://www.sgg.si/eng-aec-eurocluster/. (26 listopada 2025)
95. Strona internetowa Euroklastra Silicon Europe. Dostęp: https://www.silicon-europe.eu/home/. (26 listopada 2025)
96. Strona internetowa Euroklastra Sustain. Dostęp: https://www.sustaineurocluster.com/. (26 listopada 2025)
97. Strona internetowa European Cluster Collaboration Platform. Dostęp: https://www.clustercollaboration.eu/euroclusters. (26 listopada 2025)
98. Strona internetowa ISSA Polska. Dostęp: https://issa.org.pl/. (26 listopada 2025)
99. Strona internetowa Klastra #CyberMadeInPoland. Dostęp: https://cybermadeinpoland.pl/. (26 listopada 2025)
100. Strona internetowa Klastra Cyber Ireland. Dostęp: https://cyberireland.ie/. (26 listopada 2025)
101. Strona internetowa Klastra CyberLur. Dostęp: https://cyberlur.es/aei-home. (26 listopada 2025)
102. Strona internetowa Klastra Cyscoe. Dostęp: https://cyscoe.ro/. (26 listopada 2025)
103. Strona internetowa Klastra LSEC. Dostęp: https://www.digitalsecuritycatalyst.com/. (26 listopada 2025)
104. Strona internetowa Klastra The Dutch Security Cluster. Dostęp: https://securitydelta.nl/. (26 listopada 2025)

105. Strona internetowa Łódzkiego Klastra ICT. Dostęp: https://ictcluster.pl/. (26 listopada 2025)
106. Strona internetowa narzędzie Manager haseł Google. Dostęp: https://passwords.google.com/intro. (28 listopada 2025)
107. Strona internetowa narzędzia KeePass. Dostęp: https://keepass.info/. (28 listopada 2025)
108. Strona internetowa narzędzia Percpass. Dostęp: https://percpass.com/. (28 listopada 2025)
109. Strona internetowa PARP. Dostęp: https://www.parp.gov.pl/component/site/site/4digital. (24 listopada 2025)
110. Strona internetowa PIIT. Dostęp: https://piit.org.pl/. (26 listopada 2025)
111. Strona internetowa Pomorskiego Klastra ICT. Dostęp: https://interizon.pl/pl/. (26 listopada 2025)
112. Strona internetowa PPBW. Dostęp: https://ppbw.pl/. (26 listopada 2025)
113. Test AIMIND (określa poziom dojrzałości przedsiębiorstwa w obszarze wdrażania i wykorzystania sztucznej inteligencji) dla AI4SME. Dostępny na stronie internetowej PARP. Dostęp: https://ai4msp.pl/test-aimind/. (24 listopada 2025)
114. Test Dojrzałości Cyfrowej dostępny na stronie internetowej PFR. Dostęp: https://pfr.pl/test-dojrzalosci-cyfrowej. (24 listopada 2025)
115. Trendmicro, „Czym jest social engineering?" [artykuł online]. Dostęp: https://www.trendmicro.com/pl_pl/what-is/social-engineering.html. (24.11.2025)
116. US National Institute of Standards and Technology, „Phishing". Dostęp: https://www.nist.gov/itl/smallbusinesscyber/guidance-topic/phishing. (24 listopada 2025)
117. Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. Dz.U. 2018, poz. 1560. Dostęp: https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20180001560. (24 listopada 2025)
118. Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych. Dz.U. 2018, poz. 1000. Dostęp: https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20180001000. (24 listopada 2025)
119. Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych. Dostęp: https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20180001000. (24 listopada 2025)
120. Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. 2018 poz. 150 ze zm.).
121. Więcej na temat umów SLA można znaleźć na stronie internetowej nFlo. Dostęp: https://nflo.pl/slownik/service-level-agreement/. (25 listopada 2025)
122. Xopero Software, „Plan Backupu. Jak go stworzyć aby był skuteczny i niezawodny". Dostęp: https://xopero.com/pl/dokumenty/backup-plan/. (28 listopada 2025)
123. Zespół autorski RCI Kraków, (2024) „Triada CIA jako fundament bezpieczeństwa" [artykuł online]. Dostęp: https://rcikrakow.wp.mil.pl/aktualnosci/triada-cia-jako-fundament-bezpieczenstwa/. (17 listopada 2025)
124. Zespół Bezpieczeństwa Informacji Wrocławskiego Centrum Sieciowo-Superkomputerowego. Dostęp: https://di.pwr.edu.pl/aktualnosci/ostrzezenie-o-atakach-na-konta-ms365-115.html. (28 listopada 2025)