Rekomendacje zespołu CERT Polska dla ustanawiania zespołów CSIRT

CERT.PL
NASK

Rekomendacje zespołu CERT Polska dla ustanawiania zespołów CSIRT

TLP: CLEAR

NASK-PIB

Wersja 1.0

Warszawa, lipiec 2025

Wytworzone w CSIRT NASK w ramach dotacji KSC
udzielonej przez Ministerstwo Cyfryzacji.

PROJEKT FINANSOWANY ZE ŚRODKÓW
MINISTERSTWA CYFRYZACJI

Publikacja wyraża jedynie poglądy autora/ów i nie może być utożsamiana
z oficjalnym stanowiskiem Ministerstwa Cyfryzacji.

Spis treści

Wprowadzenie

Cele rekomendacji

Oddajemy w Państwa ręce dokument, którego podstawowym celem jest wsparcie w procesie ustanawiania CSIRT-ów oraz rozwijania ich zdolności operacyjnych. Pierwsze, niepubliczne wydanie niniejszych rekomendacji, zostało przygotowane z myślą o powstawaniu CSIRT-ów sektorowych zgodnie z projektem nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa. Chcemy, żeby proces tworzenia zespołów cyberbezpieczeństwa przebiegał w sposób uporządkowany, a same zespoły działały spójnie i porównywalnie. W związku z tym zależy nam, by powstające CSIRT-y osiągały co najmniej poziom podstawowej dojrzałości (Basic) zgodnie z „ENISA CSIRT Maturity Framework”[1].

Dzięki temu CSIRT-y będą mogły skutecznie wykonywać powierzone zadania oraz produktywnie współpracować z CSIRT-ami poziomu krajowego (CSIRT MON, CSIRT NASK, CISIRT GOV) lub CSIRT-ami sektorowymi. To z kolei umożliwi organizacjom lepsze zarządzanie ryzykiem zakłóceń w funkcjonowaniu usług. Zachęcamy do uwzględnienia naszych rekomendacji podczas tworzenia zespołów cyberbezpieczeństwa oraz do dzielenia się swoimi doświadczeniami z innymi instytucjami, które stają przed podobnym wyzwaniem.

Zakres stosowania rekomendacji

W dokumencie zostały przedstawione praktyczne porady dotyczące organizacji i funkcjonowania zespołów CSIRT. Rekomendacje kierowane są przede wszystkim do osób odpowiedzialnych za tworzenie zespołów cyberbezpieczeństwa w podmiotach krajowego systemu cyberbezpieczeństwa (dalej również: KSC), ale również do pracowników innych podmiotów, w tym komercyjnych, które podejmą decyzję o powołaniu podobnego zespołu. Dokument ma charakter wspomagający – nie jest wiążący, lecz jego stosowanie umożliwi ujednolicenie zasad oraz zwiększy szanse na sprawne i zgodne z regulacjami funkcjonowanie zespołu, a także wpłynie na harmonijną współpracę z zespołami CSIRT poziomu krajowego i CSIRT-ami sektorowymi.

[1] „ENISA CSIRT Maturity Framework” określa trzy poziomy dojrzałości zespołów CSIRT: podstawowy (ang. *Basic*), średnio zaawansowany (ang. *Intermediate*) i zaawansowany (ang. *Advanced*) https://www.enisa.europa.eu/sites/default/files/publications/WP%202021%20O.4.1%20ENISA%20CSIRT%20maturity%20methodology%20improvement.pdf

Niniejsze rekomendacje dotyczą zespołów CSIRT – zespołów reagowania na incydenty bezpieczeństwa komputerowego, jednak można je odnieść odpowiednio również do innych zespołów bezpieczeństwa komputerowego, takich jak CERT, SOC czy ISAC.

Metodyka i przyjęte założenia

CSIRT-y będą powstawały w różnych obszarach działania państwa i organizacjach różnego rodzaju. W tym kontekście ważne jest, aby zasady powoływania tych zespołów były jasno określone oraz jednolite. Rekomendacje zebrane w tej publikacji są oparte na dwóch uzupełniających się modelach: SIM3 („Security Incident Management Maturity Model")[2], który stanowi podstawę oceny dojrzałości zespołów CSIRT, oraz modelu opracowanego na jego bazie „ENISA CSIRT Maturity Framework" (dalej również: „ENISA CMF"). Powyższe modele posłużyły do zidentyfikowania rekomendacji funkcjonalnych, organizacyjnych i technicznych, których spełnienie ułatwi organom ustanawiającym CSIRT-y osiągnięcie poziomu podstawowej dojrzałości (Basic), zgodnie z wytycznymi przyjętymi przez ENISA.

Obecnie (w czasie powstawania tych rekomendacji) CSIRT-y funkcjonują w ograniczonym zakresie. W konsekwencji organizacje dysponują niewielkimi praktycznymi doświadczeniami w budowie i prowadzeniu CSIRT-u. Podczas opracowywania niniejszych rekomendacji zespół CERT Polska przyjął również założenie, że zespoły, które zostaną ustanowione, w początkowym okresie funkcjonowania będą miały niski poziom dojrzałości organizacyjnej i operacyjnej, wynikający z wczesnego etapu rozwoju, braku wcześniejszych doświadczeń w zarządzaniu incydentami oraz z potencjalnie ograniczonych zasobów.

Poziom Basic oznacza minimalny poziom dojrzałości zespołu CSIRT, pozwalający na skuteczne świadczenie podstawowych usług w zakresie reagowania na incydenty i wspierania constituency. Zespoły funkcjonujące poniżej tego poziomu nie będą zdolne do efektywnej reakcji na incydenty, wsparcia podmiotów oraz współpracy z CSIRT-ami poziomu krajowego lub sektorowymi.

Ocena poziomu dojrzałości Basic opiera się na analizie 45 parametrów, podzielonych na cztery obszary: organizacja (O), zasoby ludzkie (H – ang. *human*), narzędzia (T – ang. *tools*) i procesy (P). Każdy parametr jest oceniany w czterostopniowej skali (0–4), gdzie poziomy wyższe oznaczają większą dojrzałość.

[2] https://opencsirt.org/wp-content/uploads/2023/11/SIM3_v2_interim_standard.pdf

Tabela 1. Opis poziomów parametrów określających stopień dojrzałości CSIRT-ów

Poziom	Opis
0	Brak dostępnych ustaleń, brak świadomości lub definicji w danym obszarze
1	Pewne działania lub zasady są znane i stosowane, ale nie zostały nigdzie zapisane (wiedza oparta na przekazie ustnym oraz doświadczeniu zespołu)
2	Działania lub zasady zostały spisane wewnętrznie i są stosowane (np. w wiki zespołu lub innym repozytorium wiedzy), ale nie zostały jeszcze formalnie zatwierdzone przez kierownictwo
3	Dokumenty, procedury lub zasady są formalnie zatwierdzone przez kierownictwo CSIRT i wprowadzone do operacyjnego wykorzystania
4	Dokumenty i zasady są nie tylko zatwierdzone, lecz także regularnie poddawane przeglądowi i kontroli przez wyższy poziom zarządzania (np. w ramach audytów lub przeglądów rocznych)

Wymagane poziomy dojrzałości dla poziomu Basic zostały określone dla każdego parametru indywidualnie i są zestawione w poniższej tabeli.

Tabela 2. Wymagane poziomy dojrzałości dla każdego parametru

Parametr	Nazwa parametru	Minimalne wartości dla poziomu		
		Basic	Intermediate	Advanced
O-1	Mandat	3	4	4
O-2	*Constituency*	3	4	4
O-3	Uprawnienia	3	4	4
O-4	Odpowiedzialność	3	4	4
O-5	Opis świadczonych usług	3	4	4
O-6	Polityka komunikacji z mediami	2	3	4
O-7	Opis poziomu świadczenia usług	3	4	4
O-8	Klasyfikacja incydentów	2	3	4
O-9	Udział w systemach współpracy CSIRT	3	4	4
O-10	Ramy organizacyjne zespołu	3	3	3
O-11	Polityka bezpieczeństwa	2	3	4
H-1	Kodeks postępowania	2	3	3
H-2	Odporność kadrowa	2	3	4
H-3	Opis umiejętności	2	2	3

H-4	Rozwój kompetencji członków zespołu	2	3	4
H-5	Szkolenia techniczne	1	2	3
H-6	Szkolenia z umiejętności miękkich	1	2	3
H-7	Budowanie sieci kontaktów	2	3	3
T-1	Zasoby i konfiguracje	1	2	3
T-2	Źródła informacji	2	3	4
T-3	Zintegrowany system komunikacji	2	3	3
T-4	System śledzenia incydentów	2	3	3
T-5	Odporne połączenia głosowe	2	3	3
T-6	Odporna komunikacja tekstowa	2	3	3
T-7	Stały dostępu do internetu	2	3	3
T-8	Narzędzia do zapobiegania incydentom	2	2	3
T-9	Narzędzia do wykrywania incydentów	2	3	3
T-10	Narzędzia do rozwiązywania incydentów	2	3	3
P-1	Eskalacja na poziom zarządzania	3	4	4
P-2	Eskalacja do zespołu prasowego	2	3	3
P-3	Eskalacja do działu prawnego	2	3	3
P-4	Zapobieganie incydentom	2	3	4
P-5	Wykrywanie incydentów	2	3	4
P-6	Rozwiązywanie incydentów	2	3	4
P-7	Rozwiązywanie szczególnych incydentów	2	3	4
P-8	Audyt i zbieranie informacji zwrotnej	3	4	4
P-9	Alarmowy kontakt z zespołem	2	3	3
P-10	Obecność w internecie	2	3	3
P-11	Bezpieczne przetwarzanie informacji	2	3	3
P-12	Zarządzanie źródłami informacji	2	3	4
P-13	Komunikacja z podmiotami *constituency*	2	3	4
P-14	Raportowanie do organu nadzorującego	3	4	4
P-15	Raportowanie do *constituency*	2	3	3
P-16	Spotkania wewnętrzne	2	2	3
P-17	Współpraca z zespołami partnerskimi	2	3	4

W dalszej części publikacji znajdują się szczegółowe rekomendacje odnoszące się do poszczególnych parametrów. Każda rekomendacja została opracowana tak, aby osiągnięcie poziomu dojrzałości Basic przez CSIRT-y było możliwe do realizacji zgodnie z wymaganiami ustawy o krajowym systemie cyberbezpieczeństwa oraz z najlepszymi praktykami zespołu CERT Polska.

Podstawy prawne i powiązane regulacje

Podstawą prawną opracowania niniejszych rekomendacji jest ustawa o krajowym systemie cyberbezpieczeństwa. CSIRT-y poziomu krajowego mają ustawowy obowiązek opracowywania standardów, rekomendacji i dobrych praktyk (art. 26 ust. 3 pkt 14 lit. d) oraz wspierania podmiotów krajowego systemu cyberbezpieczeństwa w budowaniu ich potencjału i zdolności w obszarze cyberbezpieczeństwa (art. 26 ust. 3 pkt 14 lit. e).

Należy podkreślić, że w chwili opracowywania niniejszych rekomendacji trwają prace legislacyjne nad nowelizacją ustawy o krajowym systemie cyberbezpieczeństwa. Planowane przepisy obejmują m.in. obowiązki związane z przyjmowaniem i przekazywaniem zgłoszeń oraz sprawozdań, reagowaniem na incydenty, analizą podatności i zagrożeń, współpracą z CSIRT-ami poziomu krajowego i sektorowymi, a także wspieraniem monitorowania, edukacji i podnoszenia poziomu bezpieczeństwa systemów informacyjnych. Nowelizacja przewiduje również możliwość wykonywania dodatkowych działań technicznych, koordynacyjnych i doradczych. W związku z powyższym, planując ustanowienie i rozwój CSIRT-u, należy uwzględnić przyszły zakres obowiązków wynikający z projektowanych przepisów.

W świetle najnowszych regulacji, na podmioty kluczowe i ważne, a także na szeroką grupę organizacji z sektorów uznanych za krytyczne, nałożono istotnie rozszerzone obowiązki w zakresie raportowania incydentów bezpieczeństwa. Podstawowym wymogiem jest niezwłoczne zgłaszanie poważnych incydentów do właściwych zespołów CSIRT, przy czym wstępne powiadomienie musi nastąpić w ciągu 24 godzin od wykrycia zdarzenia, a pełny raport zawierający szczegółowe informacje o incydencie, jego skutkach oraz podjętych działaniach naprawczych powinien zostać przekazany w terminie do 72 godzin. Nowe przepisy precyzują również zakres informacji wymaganych w zgłoszeniach oraz nakładają obowiązek prowadzenia rejestru incydentów, który podlega kontroli organów nadzorczych.

Realizacja rekomendacji zespołu CERT Polska – prowadząca do osiągnięcia poziomu podstawowej dojrzałości (Basic) zgodnie z „ENISA CSIRT Maturity Framework" – zapewni fundament organizacyjny i operacyjny, który będzie wystarczający do skutecznego wdrożenia zadań zespołów cyberbezpieczeństwa.

Sposób korzystania z rekomendacji

Jak już wspomniano wcześniej, dokument ma charakter wspomagający – nie jest wiążący, lecz jego stosowanie umożliwi ujednolicenie zasad oraz zwiększy szanse na sprawne i zgodne z regulacjami funkcjonowanie CSIRT-ów, a także wpłynie na harmonijną współpracę z zespołami CSIRT poziomu krajowego i innymi CSIRT-ami. Wskazano w nim minimalne wymagania funkcjonalne, operacyjne i organizacyjne, jednak pozostaje możliwość odstąpienia od wymagań, które w danych warunkach są niemożliwe do wdrożenia (technicznie lub organizacyjnie) albo które zgodnie z przeprowadzoną analizą nie mają zastosowania lub wskazany w rekomendacjach cel zostanie osiągnięty za pomocą wdrożenia innych środków. Poszczególne rekomendacje zostały przedstawione i omówione zgodnie z kolejnością wprowadzoną w „ENISA CSIRT Maturity Framework".

Najważniejsze definicje i skróty

Constituency – grupa podmiotów, dla których zespół CSIRT świadczy usługi z zakresu cyberbezpieczeństwa.
CSIRT (Computer Security Incident Response Team) – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego.
DCS (Distributed Control System) – rozproszony system sterowania używany do automatyzacji i zarządzania procesami przemysłowymi, np. w rafineriach, elektrowniach czy zakładach chemicznych. W odróżnieniu od SCADA, DCS działa głównie lokalnie i skupia się na precyzyjnym sterowaniu procesami w czasie rzeczywistym.
ENISA (European Union Agency for Cybersecurity) – Agencja Unii Europejskiej ds. Cyberbezpieczeństwa.
ERP (Enterprise Resource Planning) – zintegrowany system informatyczny wspierający zarządzanie zasobami przedsiębiorstwa. Obejmuje różne obszary działalności, takie jak finanse, logistyka, produkcja, kadry czy sprzedaż.
HIS (Hospital Information System) – szpitalny system informatyczny wspomagający zarządzanie placówką medyczną. Umożliwia m.in. rejestrację pacjentów, dokumentację medyczną, planowanie zabiegów oraz zarządzanie personelem i sprzętem.

MoU (Memorandum of Understanding) – rodzaj porozumienia zawieranego pomiędzy dwiema lub więcej stronami, które formalnie deklarują wolę współdziałania w określonym przedsięwzięciu, bez tworzenia wiążących zobowiązań prawnych. MoU służy najczęściej do określenia zasad współpracy, wymiany informacji lub wspólnego działania w określonych sytuacjach, np. między zespołami CSIRT.

NIS (Network and Information Security) – dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii.

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

OUK – operator usługi kluczowej.

RFC („Request for Comments") – seria dokumentów technicznych publikowanych przez IETF (Internet Engineering Task Force), w których opisuje się protokoły i standardy dotyczące sieci komputerowych.

SCADA (Supervisory Control and Data Acquisition) – system nadzorujący i zbierający dane, wykorzystywany do zdalnego monitorowania i sterowania procesami przemysłowymi lub infrastrukturą krytyczną, taką jak sieci energetyczne, wodociągi czy systemy transportowe.

SIM3 („Security Incident Management Maturity Model") – model oceny dojrzałości zespołów cyberbezpieczeństwa.

UoKSC – ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2024 poz. 1077 t.j.).

Organizacja (O)

Parametry obszaru O (Organizacja) odnoszą się do podstawowych elementów organizacyjnych, które definiują ramy funkcjonowania zespołu CSIRT. Obejmują one zarówno podstawy prawne i formalne działania zespołu (mandat, umocowanie, odpowiedzialność), jak i określenie obszaru działania zespołu (z ang. *constituency*), świadczonych usług, uprawnień, poziomu usług oraz udziału w szerszym ekosystemie bezpieczeństwa. Parametry te pozwalają ocenić, czy CSIRT został utworzony na solidnych podstawach formalno-strukturalnych, a jego działalność jest zgodna z przyjętymi celami strategicznymi oraz dobrze zintegrowana z otoczeniem organizacyjnym.

Mandat (O-1)

Wartość parametru dla dojrzałości zespołu na poziomie Basic: 3.

Mandat to formalne umocowanie zespołu CSIRT do działania. Określa podstawę prawną jego istnienia, relacje z otoczeniem instytucjonalnym (osadzenie w strukturze organizacyjnej), nadaje kompetencje i zakres odpowiedzialności. Stanowi on podstawę do podejmowania czynności w imieniu organizacji macierzystej lub na rzecz constituency oraz do współpracy z innymi interesariuszami systemu cyberbezpieczeństwa. Mandat może być ustanowiony na różnych poziomach:

- w akcie prawa powszechnie obowiązującego (np. ustawa, rozporządzenie) – rekomendowane w przypadku tworzenia CSIRT sektorowego,
- w regulacjach wewnętrznych (np. statut, regulamin organizacyjny),
- poprzez zarządzenie lub decyzję o utworzeniu jednostki.

Dodatkowo mandat zespołu może zawierać określenie zadań i kompetencji zespołu lub zawierać odwołania do innych dokumentów wewnętrznych organizacji (np. w regulaminu organizacyjnego, statutu, instrukcji lub innych wewnętrznych aktów prawnych).

W praktyce oznacza to, że mandat zespołu powinien być:

- udokumentowany i jednoznacznie sformułowany,
- zatwierdzony przez kierownictwo organizacji macierzystej lub inny organ nadrzędny,
- zakomunikowany i znany członkom zespołu oraz interesariuszom,
- zintegrowany z operacyjnym funkcjonowaniem CSIRT-u, np. poprzez jego publikację w systemach wewnętrznych (wiki, intranet, dokumentacja robocza),

- (opcjonalnie) objęty systemem przeglądów i aktualizacji[3].

Constituency (O-2)

Wartość parametru dla dojrzałości zespołu na poziomie Basic: 3.

Constituency[4] to pojęcie określające obszar działania[5] zespołu CSIRT, czyli grupę podmiotów, systemów lub zasobów, dla których zespół świadczy usługi z zakresu cyberbezpieczeństwa. Działalność ta może mieć charakter wewnętrzny (np. w ramach jednej organizacji), zewnętrzny (obejmujący wiele niezależnych podmiotów w sektorze, regionie lub branży) lub mieszany.

Aby opis *constituency* na potrzeby działań operacyjnych zespołu CSIRT był użyteczny, powinien zawierać możliwie najszerszy zestaw danych identyfikujących zarówno strukturę organizacyjną, jak i środowisko techniczne podmiotów sektora[6].

Zespół CERT Polska w szczególności rekomenduje uwzględnienie w opisie następujących informacji (do budowy opisu *constituency* rekomendujemy narzędzia opisane w parametrze T-1):

- komponenty organizacyjne, takie jak:
  - pełna lista podmiotów wchodzących w skład obszaru działania,
  - dane kontaktowe (w tym numery alarmowe i e-mail do kontaktów operacyjnych),
  - dane jednostek/komórek organizacyjnych odpowiedzialnych za cyberbezpieczeństwo w poszczególnych podmiotach,
- komponenty techniczne:

[3] Do osiągnięcia poziomu 3. wystarczająca jest forma pisemna i akceptacja co najmniej kierownika zespołu CSIRT. Działania wskazane jako opcja zapewnią osiągnięcie poziomu 4.
[4] W środowisku CSIRT anglojęzyczny termin *constituency* jest powszechnie stosowany jako określenie obszaru działania zespołu. Z tego powodu w tytule parametru świadomie pozostawiono brzmienie oryginalne.
[5] W przypadku administracji odpowiednikiem tego terminu może być „właściwość organu".
[6] Poniższy katalog stanowi maksymalnie rozszerzony zbiór. Jesteśmy świadomi, że nie jest możliwe stworzenie podobnego katalogu w początkowym etapie funkcjonowania zespołu CSIRT, tym niemniej powinno się dążyć do pozyskania jak największej ilości informacji dotyczących *constituency* oraz sukcesywnie rozbudowywać tę bazę wiedzy.

  - zakresy adresacji IP (IPv4/IPv6)[7], nazwy domenowe, przypisane numery systemów autonomicznych (AS),
  - typy wykorzystywanych systemów operacyjnych i aplikacji (z uwzględnieniem wersji i dostawców, jeśli to możliwe),
  - informacje o krytycznych systemach biznesowych, technologicznych i rozwiązaniach typowych dla sektora (np. systemy klasy HIS, SCADA, ERP), ich producentach, wersjach, modelach,
  - elementy infrastruktury wewnętrznej (np. firewall, przełączniki, load balancery, narzędzia ITSec),
  - informacje o systemach zintegrowanych lub zależnościach między systemami (np. architektura aplikacji wielowarstwowych, zależności API),
- informacje pomocnicze (ułatwiające szybkie szacowanie ryzyka):
  - wykaz usług i systemów wspierających procesy kluczowe, zależności między systemami (co pozwala szybko określić wpływ np. technicznej podatności na bezpieczeństwo sektora),
  - sposób realizacji usług zewnętrznych (np. outsourcing IT, operatorzy chmurowi).

Opis ten powinien być przechowywany w uzgodniony sposób, dostępny dla zainteresowanych oraz **regularnie aktualizowany** (jego opracowanie nie może mieć charakteru jednorazowego działania), tak by mógł być wykorzystywany zarówno w codziennej pracy zespołu, jak i podczas obsługi incydentów. Zaleca się prowadzenie bazy danych lub rejestru *constituency* w sposób umożliwiający szybkie wyszukiwanie, przeszukiwanie według kategorii technicznych i organizacyjnych oraz analizę wpływu zagrożeń na wybrane obszary. W większości przypadków dobrze zorganizowany arkusz kalkulacyjny (np. w formacie Excel) jest w zupełności wystarczający do spełnienia tych wymagań, o ile zapewnia możliwość filtrowania, sortowania oraz aktualizacji danych przez uprawnione osoby.

[7] Zalecamy, aby obejmowały one wyłącznie statyczne adresy publiczne, wykorzystywane do udostępniania usług, komunikacji z siecią publiczną lub zarządzania zasobami. Adresy dynamiczne, przydzielane tymczasowo przez dostawców usług internetowych, nie są w praktyce przydatne i nie są przedmiotem tej rekomendacji.

Co istotne, obszar działania danego CSIRT-u powinien być jawny, dostępny i łatwy do weryfikacji[8]. Publicznie dostępne informacje na temat *constituency* mogą być jednak mniej szczegółowe niż te przetwarzane w wewnętrznych repozytoriach, np. można je ograniczyć do listy obsługiwanych podmiotów, zakresu adresacji IP lub numerów AS. Pozwoli to zewnętrznym podmiotom (np. innym CSIRT-om, podmiotom zgłaszającym, badaczom bezpieczeństwa) właściwie kierować ostrzeżenia, zgłoszenia i zapytania, a także wzmocni transparentność funkcjonowania zespołu.

Poprawnie zarządzany opis *constituency* ma znaczenie nie tylko operacyjne, lecz także strategiczne. Opracowany na podstawie zadań CSIRT-u opis *constituency*:

- umożliwia szybkie przypisanie incydentu do podmiotu lub grupy podmiotów i skraca czas reakcji,
- pozwala określić skalę zagrożenia dla branży na podstawie profilu tego zagrożenia (np. podatność, dedykowany malware),
- wspiera szacowanie ryzyka, mapowanie zależności i budowanie scenariuszy potencjalnych incydentów,
- stanowi podstawę do komunikacji z podmiotami objętymi wsparciem CSIRT-u,
- wspiera budowę świadomości sytuacyjnej w constituency,
- pozwala lepiej dopasować komunikaty ostrzegawcze, prognozy zagrożeń i zalecenia operacyjne do realnych potrzeb constituency,
- umożliwia budowę automatycznych reguł monitorowania, pozwalających natychmiast powiązać nowe zagrożenia z właściwymi podmiotami.

Uprawnienia (O-3)

Wartość parametru dla dojrzałości zespołu na poziomie Basic: 3.

Uprawnienia oznaczają formalnie nadany zakres uprawnień zespołu CSIRT względem jego *constituency*, umożliwiający realizację jego zadań. W kontekście CSIRT-ów ten parametr odnosi się do tego, co zespół ma prawo zrobić, aby efektywnie wykonywać swój mandat.

Zakres uprawnień może obejmować działania o charakterze:

[8] Jednym ze sposobów realizacji tej rekomendacji (jak i części innych parametrów z obszaru O) jest publikacja deklaracji (manifestu) RFC 2350 – https://www.ietf.org/rfc/rfc2350.txt. RFC 2350 jest powszechnie publikowany przez zespoły CSIRT poziomu krajowego, sektorowe, jak i te zorganizowane w podmiotach komercyjnych.

- rekomendacyjnym (udzielanie porad, wydawanie ostrzeżeń, zaleceń),
- koordynacyjnym (zwoływanie spotkań, kierowanie działaniami w sytuacji incydentu, inicjowanie współpracy, eskalacja do danego podmiotu lub zespołu CSIRT poziomu krajowego lub sektorowego)
- operacyjnym lub interwencyjnym (np. wykonywanie analiz technicznych, inicjowanie działań naprawczych czy przekazywanie zaleceń organowi nadzorczemu).

Zespół powinien dysponować pisemnym, zatwierdzonym przez kierownictwo opisem swoich uprawnień, który stanowi formalne oparcie dla jego działań, zwłaszcza w sytuacjach spornych, nagłych lub wymagających eskalacji. Przykładowo dla CSIRT-ów sektorowych, tworzonych przez organy właściwe ds. cyberbezpieczeństwa, podstawowym źródłem określenia uprawnień są przepisy art. 44 UoKSC oraz projektowane zmiany w tej ustawie. Należy mieć na uwadze, że przepisy ustawowe, choć stanowią formalne źródło uprawnień, mają charakter ogólny, dlatego ich doprecyzowanie i operacyjne rozwinięcie powinno nastąpić w dokumentach wewnętrznych, takich jak np.:

- zarządzenia lub decyzje ustanawiające zespół,
- wewnętrzne akty organizacyjne (np. regulaminy, statuty),
- procedury operacyjne (np. dotyczące konkretnego typu incydentów).

Zakres uprawnień zespołów cyberbezpieczeństwa powinien zostać określony w praktyce – z uwzględnieniem zarówno potrzeb constituency, jak i realnych zdolności operacyjnych zespołu. Podczas opracowywania takiego zestawu warto zwrócić uwagę na następujące elementy:

- jakie formy może przyjmować wsparcie udzielane podmiotom – czy ogranicza się ono do doradztwa i konsultacji (np. opiniowanie reakcji operatora w przypadku incydentów), czy obejmuje również działania o charakterze technicznym lub operacyjnym (np. udział w reagowaniu na incydent, analiza malware, wsparcie w komunikacji z dostawcą),
- czy zespół ma prawo wydawać zalecenia lub rekomendacje oraz jaka jest ich formalna moc – np. na ile są to zalecenia wiążące, czy mogą być podstawą do dalszych działań nadzorczych,
- czy zespół może występować z inicjatywą wobec innych interesariuszy, w tym CSIRT-ów poziomu krajowego i sektorowych oraz dostawców usług dla constituency,

- w jakim zakresie odbywa się komunikacja z podmiotami międzynarodowymi,
- w jakich sytuacjach zespół ma prawo do eskalacji, np. do przekazania zgłoszenia do CSIRT-u poziomu krajowego lub sektorowego, wnioskowania o działanie nadzorcze lub przekazania ostrzeżenia do całego sektora.

Precyzyjne zdefiniowanie uprawnień zespołu cyberbezpieczeństwa zapewnia mu podstawę do działania w sytuacjach, gdy konieczne jest podejmowanie szybkich decyzji, prowadzenie koordynacji między wieloma podmiotami lub egzekwowanie ustalonych procedur.

Odpowiedzialność (O-4)

Wartość parametru dla dojrzałości zespołu na poziomie Basic: 3.

Odpowiedzialność (ang. *Responsibility*) określa, za co zespół CSIRT jest odpowiedzialny względem swojego obszaru działania (*constituency*), czyli jakie zadania powinien realizować, aby wypełnić przypisany mu mandat. W przeciwieństwie do parametru Uprawnienia, który opisuje, co zespół *ma prawo robić*, odpowiedzialność definiuje to, co *musi lub powinien robić* – niezależnie od tego, czy ma cały zestaw środków lub uprawnień do egzekwowania działań.

Zakres odpowiedzialności CSIRT-u powinien być określony na podstawie odpowiedniego dokumentu. Przykładowo, art. 44 UoKSC wskazuje pięć podstawowych zadań[9] przypisanych sektorowym zespołom CSIRT:

- przyjmowanie zgłoszeń o incydentach poważnych i wsparcie w ich obsłudze,
- wspieranie operatorów usług kluczowych w realizacji ich obowiązków ustawowych,
- analizowanie incydentów i wyciąganie wniosków,
- współpracę z CSIRT-ami poziomu krajowego,
- współpracę z innymi państwami, w tym państwami członkowskimi Unii Europejskiej, w zakresie przetwarzania informacji o incydentach poważnych.

Na tej podstawie można zdefiniować, za jakie konkretne działania zespół ponosi odpowiedzialność względem swojego *constituency* i w jaki sposób będzie je realizował.

[9] Należy mieć na uwadze, że przewidywana nowelizacja UoKSC wprowadza nowe zadania dla CSIRT-ów sektorowych. Co istotniejsze, proponowane zmiany wprowadzają limity czasowe dla realizacji określonych działań, np. na przekazanie do właściwego CSIRT MON, CSIRT NASK albo CSIRT GOV wczesnego ostrzeżenia, zgłoszenia lub sprawozdań (do 8 godzin od jego otrzymania) lub przekazanie podmiotowi zgłaszającemu (jeśli o to zawnioskuje) wytycznych dotyczących wdrożenia środków lub udzielenia dodatkowego wsparcia technicznego (do 24 godzin).

Zakres odpowiedzialności powinien być formalnie zdefiniowany i zatwierdzony co najmniej przez kierownictwo zespołu CSIRT.
W dokumencie określającym odpowiedzialność należy możliwie precyzyjnie opisać:

- jakie działania zespół ma obowiązek podejmować (np. przyjęcie każdego zgłoszenia incydentu poważnego, opracowanie rekomendacji dla operatora),
- jakie obowiązki informacyjne wobec CSIRT-ów poziomu krajowego i innych podmiotów spoczywają na zespole,
- jakie formy współpracy, analizy i raportowania stanowią minimum oczekiwane wobec zespołu.

Szczególną uwagę należy zwrócić na to, by zakres odpowiedzialności nie był znacznie szerszy niż rzeczywiste uprawnienia. Sytuacje, w których zespół odpowiada za bezpieczeństwo organizacji, ale nie ma prawa żądać informacji lub koordynować działań, prowadzą do nieefektywności i zwiększenia ryzyka zakłócenia funkcjonowania. Należy dążyć do tego, by luka między O-3 i O-4 była niewielka i kontrolowana.

Zakres odpowiedzialności powinien podlegać okresowemu przeglądowi, co pozwoli dostosować go do zmian w otoczeniu prawnym, do oczekiwań organizacji oraz do możliwości i uprawnień samego zespołu.

Opis świadczonych usług (O-5)

Wartość parametru dla dojrzałości zespołu na poziomie Basic: 3.

Opis świadczonych usług (ang. *Service Description*) to formalny dokument lub zestaw informacji określający, jakie konkretne usługi z zakresu cyberbezpieczeństwa zespół CSIRT świadczy swojemu obszarowi działania (*constituency*). Opis powinien precyzować, co i w jaki sposób CSIRT zamierza wykonać dla swojego *constituency*.

Jednym z najlepiej ugruntowanych i szeroko przyjętych punktów odniesienia w zakresie definiowania i klasyfikacji usług zespołów CSIRT jest dokument „CSIRT Services Framework”[10], opracowany przez organizację Forum of Incident Response and Security Teams (FIRST) – międzynarodowe stowarzyszenie skupiające zespoły reagowania na incydenty z całego świata[11]. Dokument ten to uporządkowany katalog usług, które mogą być świadczone przez zespoły CSIRT, niezależnie od ich modelu organizacyjnego, poziomu technicznego czy rodzaju obsługiwanej organizacji. Zawiera opisy poszczególnych obszarów usługowych oraz szczegółowe definicje funkcji,

[10] https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2-1
[11] https://www.first.org/

które składają się na daną usługę. Rekomendujemy ten dokument jako podstawę do opracowania własnego katalogu usług zespołu CSIRT.

W kontekście działalności zespołów CSIRT usługę należy rozumieć jako zorganizowany zestaw rozpoznawalnych, spójnych funkcji (procesów) ukierunkowanych na osiągnięcie konkretnego rezultatu. Rezultat ten to wartość dostarczana odbiorcy usługi, odpowiadająca na pytania: *co otrzymam na końcu?*, *czemu ta usługa służy?*, *jaką potrzebę zaspokaja?*. Może to być zarówno bezpośredni efekt techniczny (np. raport z analizy), jak i rezultat organizacyjny, informacyjny (np. budowanie świadomości, rekomendacja) lub decyzyjny (np. ostrzeżenie, ułatwienie działań naprawczych, koordynacja obsługi incydentu). Usługa nie jest więc pojedynczym działaniem czy incydentalną reakcją, lecz uporządkowanym i powtarzalnym zestawem procesów realizowanym według określonego celu, zakresu, metody i spodziewanego efektu. Tak rozumiane usługi są podstawowym sposobem realizacji mandatu i odpowiedzialności zespołu CSIRT oraz punktem odniesienia do oceny jego gotowości operacyjnej.

Dla CSIRT-ów kluczowe znaczenie ma to, by usługi były:

- zgodne z zakresem wynikającym z przepisów prawa (np. art. 44 UoKSC) oraz powiązane z mandatem i odpowiedzialnością zespołu,
- dostosowane do realnych potrzeb organizacji i poziomu dojrzałości zespołu,
- możliwe do świadczenia przy dostępnych zasobach i kompetencjach.

Opis usług powinien zawierać co najmniej (przykładowy opis usługi znajduje się w **załączniku nr 1**):

- nazwę i opis usługi, jej cel i rezultat,
- możliwie precyzyjny zakres świadczonych działań (np. „analiza artefaktów – tylko statyczna”, „wsparcie techniczne – wyłącznie doradcze”), w tym wyraźne wskazanie ograniczeń (czego zespół nie robi w ramach danej usługi),
- dostępność czasową (godziny pracy, dostępność w sytuacjach nadzwyczajnych).

CSIRT może mieć charakter zespołu koordynacyjnego, jak i również operacyjnego. Koordynacja[12] w kontekście usług z zakresu cyberbezpieczeństwa oznacza usystematyzowany proces komunikacji i wymiany informacji pomiędzy wszystkimi podmiotami zaangażowanymi w obsługę incydentu. Jej celem jest skuteczna i efektywna ob-

[12] Opracowanie własne na podstawie opisu usługi Information security incident coordination i przypisanych jej funkcji z FIRST „CSIRT Services Framework”.

sługa incydentu w sposób prowadzący do zmniejszenia ryzyka zakłócenia funkcjonowania usług kluczowych lub ważnych. Istotą koordynacji jest utrzymywanie ciągłego, uporządkowanego obiegu informacji tak, aby właściwe (tj. faktycznie zaangażowane w obsługę incydentu) strony miały dostęp do aktualnych, dokładnych i terminowych (na czas) danych.

Koordynacja obejmuje m.in.:

- przekazywanie informacji o statusie działań prowadzonych w odpowiedzi na incydent,
- monitorowanie działań i komunikacji między podmiotami biorącymi udział w reagowaniu,
- dystrybucję istotnych danych i wniosków, w tym wskaźników kompromitacji, wyników analiz czy zaleceń operacyjnych,
- prowadzenie ukierunkowanej komunikacji z interesariuszami – z uwzględnieniem wymagań poufności, dostępności i integralności informacji, konieczności stosowania polityk retencji, klasyfikacji (np. TLP), czy obsługi NDA oraz informacji niejawnych,
- przekazywanie powiadomień do podmiotów potencjalnie dotkniętych incydentem lub mogących mieć wpływ na jego obsługę – z jasnym określeniem oczekiwanej roli, zakresu wsparcia i punktów kontaktowych.

W praktyce oznacza to, że CSIRT pełniący funkcję koordynacyjną:

- identyfikuje strony, które powinny zostać poinformowane lub zaangażowane, i komunikuje im aktualne informacje oraz oczekiwania,
- monitoruje przebieg działań i dba o ich zgodność z przyjętym planem reagowania,
- zarządza eskalacją w przypadku opóźnień lub konieczności podjęcia decyzji przez wyższy poziom zarządzania,
- ułatwia wymianę informacji z innymi zespołami CSIRT oraz organizacjami zewnętrznymi, w tym z partnerami krajowymi i międzynarodowymi.

W związku z tym rekomendujemy następujący zestaw podstawowych usług zespołu CSIRT (nazwy i numery usług w nawiasach pochodzą z katalogu FIRST „CSIRT Services Framework”).

Tabela 3. Rekomendowany zestaw usług zespołu cyberbezpieczeństwa

Nazwa usługi	Uwagi
Z obszaru zarządzania incydentami cyberbezpieczeństwa	
Przyjmowanie zgłoszeń o incydentach bezpieczeństwa informacji (6.1 Service: Information security incident report acceptance)	Zgodnie z trybem pracy określonym w modelu operacyjnym zespołu
Analiza incydentów bezpieczeństwa informacji (6.2 Service: Information security incident analysis)	W zakresie, jaki jest zgodny z oczekiwaniem organizacji oraz jaki jest niezbędny do oceny, czy i jaki incydent ma wpływ na bezpieczeństwo organizacji
Analiza artefaktów i materiału dowodowego (6.3 Service: Artifact and forensic evidence analysis)	W zależności od zdolności zespołu, charakterystyki i potrzeb constituency
Koordynacja obsługi incydentów bezpieczeństwa informacji (6.5 Service: Information security incident coordination)	W zakresie zapewnienia skoordynowanej reakcji zmierzającej do minimalizacji ryzyka zakłócenia świadczenia usług
Wsparcie zarządzania kryzysowego (6.6 Service: Crisis management support)	W zakresie, w jakim potencjalny incydent poważny może wywołać sytuację kryzysową w organizacji, sektorze lub w regionie
Z obszaru zarządzania podatnościami	
Przyjmowanie zgłoszeń o podatnościach (7.2 Service: Vulnerability report intake)	Zgodnie z trybem pracy określonym w modelu operacyjnym zespołu
Analiza podatności (7.3 Service: Vulnerability analysis)	W zakresie oceny wpływu podatności na bezpieczeństwo podmiotów w constituency
Koordynacja działań związanych z podatnościami (7.4 Service: Vulnerability coordination)	W zakresie współpracy podmiotów w constituency z CSIRT-ami poziomu krajowego
Ujawnianie informacji o podatności (7.5 Service: Vulnerability disclosure)	W zakresie dostarczenia (przekazania) podmiotom *constituency* informacji o podatności
Reakcja na podatności (7.6 Service: Vulnerability response)	W zakresie aktywnego poszukiwania (skanowania) znanych podatności w ramach *constituency* w celach prewencyjnych, a w przypadku wykrycia – naprawczych. W zależności od zdolności zespołu, charakterystyki i potrzeb sektora
Z obszaru świadomości sytuacyjnej[13]	
Pozyskiwanie danych (8.1 Service: Data acquisition)	W zakresie niezbędnym do budowania świadomości zagrożeń dla sektora

[13] Pojęcie świadomości sytuacyjnej (ang. *situational awareness*) odnosi się do zdolności CSIRT-u do identyfikowania, interpretowania i przekazywania kluczowych informacji o zagrożeniach, które mogą wpłynąć na bezpieczeństwo jego *constituency*. Obejmuje ono zarówno pozyskiwanie informacji, ocenę aktualnego stanu bezpieczeństwa constituency, jak i przewidywanie możliwych zmian w celu umożliwienia lepszego podejmowania decyzji przez podmioty wspierane przez zespół.

Analiza i synteza informacji (8.2 Service: Analysis and synthesis)	W zakresie określania ryzyka dla sektora i generowania operacyjnych informacji dla *constituency*
Komunikacja (8.3 Service: Communication)	W zakresie kanałów i sposobów przekazywania operacyjnej informacji dla *constituency*
Z obszaru transferu wiedzy	
Budowanie świadomości (9.1 Service: Awareness building)	W zakresie minimalizacji ryzyka wynikającego z niskiej świadomości użytkowników technologii ICT oraz niewystarczającej dojrzałości organizacyjnej i kompetencyjnej podmiotów constituency oraz ich pracowników w zakresie cyberbezpieczeństwa
Szkolenia i edukacja (9.2 Service: Training and education)	
Doradztwo w zakresie polityk i rozwiązań technicznych (9.4 Service: Technical and policy advisory)	W zakresie udzielenia wsparcia technicznego w razie potrzeby oraz rekomendowania rozwiązań wspierających rozwój polityk bezpieczeństwa

Do świadczenia wyżej wymienionych usług niezbędne są następujące zasoby: personel (wymagania dla personelu określone są w rozdziałach oznaczonych literą H), infrastruktura własna zespołu i zestaw narzędzi (wymagania dla tego obszaru określone są w rozdziałach oznaczonych literą T) oraz procedury (wymagania odnoszące się do nich określone są w rozdziałach oznaczonych literą P).

Opis katalogu usług powinien być okresowo przeglądany i aktualizowany, np. w takich przypadkach, jak zmiana mandatu, pojawienie się nowych zagrożeń, wdrożenie nowych narzędzi, a także wraz z rozwijaniem nowych usług i osiąganiem kolejnych poziomów dojrzałości zespołu.

Polityka komunikacji z mediami (O-6)

Wartość parametru dla dojrzałości zespołu na poziomie Basic: 2.

Polityka komunikacji z mediami (ang. *Public Media Policy*) określa zasady kontaktów zespołu CSIRT z mediami i opinią publiczną. W rzeczywistości, w której informacje o incydentach rozprzestrzeniają się bardzo szybko – niejednokrotnie zanim zostaną formalnie potwierdzone – istotne jest posiadanie spójnej i jednoznacznej polityki informacyjnej. Pozwala ona zespołowi CSIRT właściwie reagować na zapytania mediów, a także samodzielnie i proaktywnie inicjować komunikaty ostrzegawcze lub edukacyjne w przestrzeni publicznej.

W przypadku CSIRT-ów funkcjonujących w ramach administracji publicznej, rekomendujemy ścisłą współpracę z działem odpowiedzialnym za komunikację zewnętrzną (PR) organu właściwego ds. cyberbezpieczeństwa, a także wyznaczenie wewnętrznych reguł dotyczących (zob. również opis parametru P-2):

- zasad przygotowywania i zatwierdzania komunikatów publicznych,
- podziału ról i odpowiedzialności za kontakt z mediami,
- sytuacji, w których zespół może samodzielnie występować w imieniu CSIRT-u,
- obsługi profili informacyjnych w mediach społecznościowych (np. X, LinkedIn, a w niektórych przypadkach także Facebook), służących m.in. do szybkiego rozpowszechniania ostrzeżeń lub rekomendacji.

Zgodnie z wymaganiami poziomu podstawowego dojrzałości zespół powinien posiadać co najmniej wewnętrznie uzgodniony dokument lub procedurę opisującą te zasady, dostępną dla członków zespołu i spójną z codzienną praktyką działania. Nie jest wymagane formalne zatwierdzenie przez kierownictwo organizacji, ale zaleca się jego zaangażowanie na etapie uzgadniania treści.

Opis poziomu świadczenia usług (O-7)

Wartość parametru dla dojrzałości zespołu na poziomie Basic: 3.

Opis poziomu świadczenia usług (ang. *Service Level Description – SLA*) określa, jakie standardy reakcji i czasu realizacji obowiązują w ramach poszczególnych usług świadczonych przez CSIRT.

Dla CSIRT-ów, które pełnią funkcję koordynacyjną, dobrze zdefiniowane (realistyczne, ale jednocześnie jednoznaczne) SLA zapewnia przewidywalność, zwiększa efektywność oraz umożliwia ocenę skuteczności zespołu i jego zdolności do realizacji mandatu oraz buduje zaufanie wewnątrz constituency i partnerów zewnętrznych.

W praktyce opis poziomów usług może przyjąć formę syntetycznej tabeli powiązanej z katalogiem świadczonych usług (zob. parametr O-5), dzięki czemu będzie spójny, przejrzysty i możliwy do aktualizacji w miarę rozwoju zespołu. Przydatne jest również powiązanie SLA z klasyfikacją incydentów (zob. parametr O-8) – tak, aby dla każdego rodzaju zdarzenia i jego wagi można było przypisać odpowiedni czas reakcji i zakres działań.

W dokumencie warto odróżnić:

- zobowiązania o charakterze stałym (wynikające z przepisów prawa, formalnych porozumień lub zobowiązań, np. czas przesłania pierwszej odpowiedzi przez członka zespołu CSIRT) od
- realizowanych na zasadzie best effort (np. wartości orientacyjne lub deklarowany czas reakcji, które można modyfikować w zależności od dostępnych zasobów lub poziomu zagrożenia).

Opis poziomu świadczenia usług powinien podlegać okresowemu przeglądowi, a jego aktualna wersja powinna być łatwo dostępna zarówno wewnętrznie (dla członków zespołu), jak i – w zakresie ogólnym – publicznie, np. w formie dokumentu RFC 2350 lub jego odpowiednika.

Klasyfikacja incydentów (O-8)

Wartość parametru dla dojrzałości zespołu na poziomie Basic: 2.

Klasyfikacja incydentów (taksonomia) to uporządkowany schemat, według którego CSIRT identyfikuje, oznacza i kategoryzuje incydenty bezpieczeństwa informacji. Celem klasyfikacji jest zapewnienie spójnego opisu zgłoszeń i umożliwienie efektywnego zarządzania nimi – w tym przypisania priorytetów, eskalacji, analiz porównawczych oraz raportowania do interesariuszy i organów nadzorczych.

Rekomendujemy stosowanie istniejących, uznanych taksonomii, np. taksonomii ENISA, wykorzystywanej również w zespole CSIRT NASK – „Reference Incident Classification Taxonomy”[14]. Dokument ten oferuje uniwersalne i czytelne kategorie techniczne, które mogą być z łatwością rozwinięte o dodatkowe parametry (np. wpływ, priorytet, SLA) zgodne z profilem usług zespołu.

[14] https://www.enisa.europa.eu/sites/default/files/publications/WP2017%20O-3-1-1%20Good%20practice%20guide%20on%20how%20to%20improve%20CSIRT%20capabilities.pdf

INCIDENT CLASSIFICATION	INCIDENT EXAMPLES	DESCRIPTION
Abusive Content	Spam	or "Unsolicited Bulk Email", this means that the recipient has not granted verifiable permission for the message to be sent and that the message is sent as part of a larger collection of messages, all having a functionally comparable content
	Harmful Speech	Discreditation or discrimination of somebody (e.g. cyber stalking, racism and threats against one or more individuals)
	Child/Sexual/Violence/ ...	Child pornography, glorification of violence, ...
Malicious Code	Virus	Software that is intentionally included or inserted in a system for a harmful purpose. A user interaction is normally necessary to activate the code.
	Worm	
	Trojan	
	Spyware	
	Dialler	
	Rootkit	
Information Gathering	Scanning	Attacks that send requests to a system to discover weak points. This includes also some kind of testing processes to gather information about hosts, services and accounts. Examples: fingerd, DNS querying, ICMP, SMTP (EXPN, RCPT, ...), port scanning.
	Sniffing	Observing and recording of network traffic (wiretapping).
	Social engineering	Gathering information from a human being in a non-technical way (e.g. lies, tricks, bribes, or threats).
Intrusion Attempts	Exploiting known vulnerabilities	An attempt to compromise a system or to disrupt any service by exploiting vulnerabilities with a standardised identifier such as CVE name (e.g. buffer overflow, backdoor, cross site scripting, etc.).
	Login attempts	Multiple login attempts (Guessing / cracking of passwords, brute force).
	New attack signature	An attempt using an unknown exploit.

Rysunek 1. Fragment tabeli z dokumentu ENISA „Reference Incident Classification Taxonomy"

Stosowanie jednolitej taksonomii incydentów przynosi korzyści w codziennej pracy zespołu CSIRT:

- umożliwia spójne rozumienie i interpretację incydentów przez wszystkich interesariuszy – zespół, operatorów usług kluczowych, CSIRT-y poziomu krajowego i sektorowe oraz inne podmioty zaangażowane w reakcję,
- pozwala na szybszą, wstępną ocenę ryzyka oraz jego potencjalnego wpływu na constituency,
- ułatwia przypisanie odpowiednich zasobów i określenie priorytetów działań – na podstawie klasy incydentu,
- wspiera efektywną koordynację działań i komunikację pomiędzy różnymi zespołami – dzięki „wspólnemu językowi" opisu incydentu,
- poprawia jakość analiz porównawczych, budowanie świadomości sytuacyjnej oraz tworzenie raportów i statystyk, które mogą być porównywalne w skali krajowej i międzynarodowej,

- sprzyja automatyzacji procesów (np. w systemach IR, SOAR) dzięki możliwości tagowania incydentów według jednolitego schematu.

Stosowana taksonomia powinna być formalnie zatwierdzona przez kierownictwo CSIRT i dostępna w systemach wewnętrznych zespołu. Rekomendujemy także jej okresowy przegląd i aktualizację na podstawie doświadczeń operacyjnych, zmieniających się zagrożeń oraz potrzeb constituency.

Udział w systemach współpracy CSIRT (O-9)

Wartość parametru dla dojrzałości zespołu na poziomie Basic: 3.

Udział w systemach współpracy CSIRT odnosi się do zaangażowania zespołu w formalne lub nieformalne inicjatywy współpracy pomiędzy zespołami CSIRT zarówno na poziomie krajowym, sektorowym, jak i międzynarodowym. Współpraca ta może mieć charakter bezpośredni (np. członkostwo) lub pośredni (poprzez CSIRT poziomu krajowego, który występuje w imieniu innych CSIRT-ów).

Uczestnictwo w systemach współpracy CSIRT przynosi szereg istotnych korzyści, np.:

- umożliwia szybką i bezpieczną wymianę informacji o zagrożeniach i incydentach z zespołami z innych, dotkniętych podobnym incydentem, krajów lub sektorów,
- ułatwia uzyskiwanie wsparcia technicznego, analitycznego i organizacyjnego od bardziej doświadczonych zespołów,
- pozwala na uczestnictwo w ćwiczeniach, projektach rozwojowych i szkoleniach organizowanych przez społeczność CSIRT,
- umożliwia bieżące śledzenie trendów w obszarze cyberbezpieczeństwa oraz przyjęcie dobrych praktyk, a w niektórych przypadkach także korzystanie ze źródeł informacji o zagrożeniach, udostępnianych przez inne zespoły.

Rekomendujemy w szczególności:

- uzyskanie akredytacji TF-CSIRT,
- członkostwo w organizacji FIRST (Forum of Incident Response and Security Teams),
- aktywny udział w grupach roboczych, forach wymiany informacji lub inicjatywach kierowanych do constituency.

Uczestnictwo w inicjatywach typu TF-CSIRT lub FIRST wymaga przejścia formalnego procesu uzyskiwania akredytacji/członkostwa. Wiąże się również z koniecznością

wniesienia opłat członkowskich[15], a w przypadku FIRST dodatkowo ze zgodą na przeprowadzenie wizytacji przez zespół popierający członkostwo[16]. Te czynniki należy uwzględnić w planowaniu budżetu oraz terminu uzyskania akredytacji/członkostwa.

Ramy organizacyjne zespołu (O-10)

Wartość parametru dla dojrzałości zespołu na poziomie Basic: 3.

Ramy organizacyjne zespołu CSIRT (ang. *Organisational Framework*), często nazywane również z ang. *team charter*, to podstawowy dokument wewnętrzny, który w sposób całościowy opisuje fundamenty funkcjonowania zespołu. Powinien on integrować co najmniej zakres parametrów od O-1 do O-9. Dokument ten stanowi formalny punkt odniesienia w procesie oceny dojrzałości, audytów, przeglądów funkcjonalnych oraz w kontaktach z interesariuszami.

Ramy organizacyjne mogą przyjąć postać jednego spójnego dokumentu lub zestawu dokumentów powiązanych ze sobą (np. zarządzenie o utworzeniu zespołu, opis usług, regulamin działania zespołu, RFC 2350). Kluczowe jest, aby zawarte w nich informacje były aktualne, jednoznaczne, zatwierdzone przez kierownictwo zespołu (lub wyższy szczebel zarządczy) oraz publicznie dostępne w zakresie niezbędnym do współpracy z interesariuszami i CSIRT-ami poziomu krajowego.

Dodatkowo w ramach dokumentu warto zawrzeć informacje o:

- modelu operacyjnym zespołu (np. tryb pracy: 8/5, dyżury, 24/7) – na początkowym etapie funkcjonowania CSIRT-u rekomendujemy przyjęcie trybu pracy 8/5 (tj. w dni robocze, w godzinach pracy), z jednoczesnym zapewnieniem możliwości przyjmowania zgłoszeń o incydentach poza tymi godzinami, np. poprzez system dyżurów on-call lub mechanizmy automatycznego powiadamiania. W miarę rozwoju zespołu, katalogu świadczonych usług oraz wzrostu dojrzałości możliwe jest przejście do trybu całodobowego (24/7). Warto rozważyć również tryb mieszany, w którym dostępność całodobowa dotyczy jedynie wybranych usług lub zadań,
- kluczowych rolach w zespole i w zarządzaniu incydentami (zob. opis parametru H-2),
- wewnętrznej strukturze organizacyjnej zespołu – podziale na mniejsze zespoły czy linie obsługi incydentów,

[15] https://www.trusted-introducer.org/invitation-package.pdf
[16] https://www.first.org/membership/

- podstawowych procesach zarządczych i operacyjnych – opisy lub odwołania do procesów funkcjonujących w zespole, zgodnych z katalogiem usług (parametr O-5) z obszarów zarządzania incydentami, zarządzanie podatnościami, świadomością sytuacyjną i transferem wiedzy,
- regułach i formach współpracy z innymi komórkami organizacji (np. działem prawnym, PR) oraz podmiotami sektora – dokument powinien wskazywać, w jakich sytuacjach oraz w jakim zakresie inne jednostki organizacji angażowane są w realizację zadań zespołu, np.:
  - dział prawny – w przypadku incydentów z możliwym naruszeniem prawa, konieczności analizy obowiązków wynikających z przepisów lub interpretacji przepisów,
  - dział PR – przy opracowywaniu komunikatów zewnętrznych i obsłudze sytuacji kryzysowych,
  - inne komórki merytoryczne – przy identyfikacji skutków incydentu dla procesów nadzorowanych przez organizację lub interpretacji danych przekazywanych przez podmioty constituency.

Ramy organizacyjne zespołu to praktyczne narzędzie, które pomaga jasno opisać, jak działa CSIRT. Rekomendujemy ich przegląd i aktualizację przynajmniej raz do roku lub po istotnych zmianach w strukturze, mandacie, świadczonych usługach lub otoczeniu prawnym.

Polityka bezpieczeństwa (O-11)

Wartość parametru dla dojrzałości zespołu na poziomie Basic: 2.

Polityka bezpieczeństwa (ang. *Security Policy*) określa ramy organizacyjne, techniczne i proceduralne dotyczące bezpieczeństwa informacji i ciągłości działania. Dokument ten powinien opisywać sposób ochrony danych, systemów i procesów niezbędnych do realizacji usług CSIRT-u, a także regulować zasady dostępów, przetwarzania informacji, testowania zabezpieczeń, komunikacji zewnętrznej oraz ciągłości działania zespołu.

Zespół CSIRT może działać w ramach polityki bezpieczeństwa organizacji (jeśli taka polityka obejmuje również CSIRT), może także przyjąć własną, niezależną politykę – szczególnie w przypadku specyficznych potrzeb technicznych lub wymagań operacyjnych (np. odbierania nieprzefiltrowanych wiadomości e-mail, stosowania specjalistycznych narzędzi analitycznych, testów podatności, obsługi danych wrażliwych lub prowadzenia szyfrowanej komunikacji).

W przypadku CSIRT-ów tworzonych w ramach administracji publicznej minimalnym punktem odniesienia dla ustanowienia polityki bezpieczeństwa powinno być rozporządzenie w sprawie Krajowych Ram Interoperacyjności[17], które określa wymagania w zakresie bezpieczeństwa przetwarzania informacji w systemach teleinformatycznych administracji publicznej.

Przydatne może być także wykorzystanie wytycznych zawartych w normach:

- PN-EN ISO/IEC 27001 – w zakresie systemu zarządzania bezpieczeństwem informacji,
- PN-EN ISO 22301 – w zakresie systemu zarządzania ciągłością działania.

Wykorzystanie lub wdrożenie powyższych standardów nie musi oznaczać uzyskania formalnej certyfikacji – kluczowymi kwestiami są: dopasowanie polityki do potrzeb zespołu, jej spójność z innymi dokumentami wewnętrznymi oraz regularny przegląd i aktualizacja.

Niezależnie od wyżej wymienionych przepisów i norm, z uwagi na specyfikę pracy CSIRT-u, zakres polityki bezpieczeństwa powinien obejmować m.in.:

- ochronę danych operacyjnych, w tym informacji o incydentach i podatnościach oraz źródłach informacji,
- zabezpieczenie infrastruktury i narzędzi wykorzystywanych przez CSIRT,
- zasady dostępu do wewnętrznych repozytoriów,
- sposób postępowania z danymi objętymi klauzulami poufności lub NDA,
- procedury reagowania na incydenty wewnętrzne w zespole,
- zapewnienie ciągłości działania zespołu w sytuacjach awaryjnych (takich jak np. niedostępność personelu),
- specyficzne wymagania związane z zadaniami zespołu (np. uruchamianie środowisk testowych, honeypotów, analiza złośliwego oprogramowania),
- dostosowanie procedur i narzędzi do wymagań ochrony danych osobowych (jeśli mają zastosowanie).

[17] Rozporządzenie Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. z 2024 poz. 773).

Zasoby ludzkie (H)

W zespole CSIRT pracują razem osoby zapewniające usługi opisane w części „Organizacja". Komponent H w modelu SIM3 składa się z siedmiu parametrów, które dotyczą spraw związanych z personelem, jego kwalifikacjami, szkoleniami i współpracą zewnętrzną.

Kodeks postępowania (H-1)

Wartość parametru dla dojrzałości zespołu na poziomie Basic: 2.

Zespół CSIRT często pracuje z danymi wrażliwymi, komunikuje się z partnerami zewnętrznymi, ma dostęp do informacji na temat taktyk, technik i procedur (TTP) stosowanych przez przestępców oraz o szczegółach incydentów. Członkowie zespołu dysponują zaawansowanymi kompetencjami technicznymi, mają więc potencjalnie możliwość wykorzystania tej wiedzy w sposób nieetyczny lub sprzeczny z prawem. Dlatego tak istotne jest, aby osoby pracujące w zespole CSIRT wyróżniały się nie tylko profesjonalizmem, lecz także nieskazitelnym charakterem i wysokimi standardami etycznymi. Odpowiedzialne i profesjonalne zachowanie pracowników zespołu nie może ograniczać się tylko do środowiska pracy, ale powinno także mieć zastosowanie w życiu prywatnym. Do osiągnięcia poziomu 2. niezbędne jest, aby zespół CSIRT miał wewnętrznie spisane zasady etycznego postępowania. Dodatkowo rekomendujemy, by zasady te zostały zaakceptowane i przyjęte przez kierownictwo organizacji.

Kodeks postępowania powinien zawierać:

- zobowiązanie do przestrzegania prawa krajowego i międzynarodowego,
- zobowiązanie do ochrony informacji przed ujawnieniem nieupoważnionym podmiotom,
- zobowiązanie do współpracy z innymi podmiotami zgodnie z przyjętymi procedurami,
- zobowiązanie do minimalizowania ryzyka dla użytkowników przy obsłudze podatności,
- zobowiązanie do wykonywania zadań w sposób obiektywny i do przeciwdziałania wystąpieniu konfliktu interesów,
- zobowiązanie do kierowania się profesjonalizmem zawodowym i zachowania najwyższych standardów etycznych w czasie pracy oraz w życiu prywatnym,
- zobowiązanie do pracy zespołowej w duchu uprzejmości i koleżeństwa oraz do ciągłego rozwoju, aby stanowić wsparcie dla zespołu.

Odporność kadrowa (H-2)

Wartość parametru dla dojrzałości zespołu na poziomie Basic: 2.

Odporność kadrowa (ang. *Staff Resilience*) oznacza zdolność zespołu CSIRT do zachowania ciągłości świadczenia usług w sytuacjach losowych, takich jak choroba czy krótkoterminowe kryzysy operacyjne, oraz planowanych, takich jak urlopy, delegacje czy rezygnacja z pracy. Zespół CSIRT musi ustalić minimalną liczbę pracowników, aby utrzymać zdolności operacyjne i zapewnić ciągłość świadczenia usług (zob. O-5) na określonym poziomie (zob. O-7).

Utrzymanie odpowiedniego poziomu odporności kadrowej wymaga jednak uwzględnienia nie tylko liczby osób, lecz także zakresu kompetencji członków zespołu oraz możliwości ich zastępowania się w przypadku niedostępności któregoś z nich. Istotne jest przypisanie zadań do ról w taki sposób, aby kluczowe usługi zespołu mogły być realizowane w sposób nieprzerwany.

W przypadku CSIRT-ów rekomendujemy zabezpieczenie przynajmniej następujących ról:

- kierownik zespołu (ang. *CSIRT manager*) – odpowiedzialny za zarządzanie zespołem, relacje z organizacją i reprezentowanie zespołu na zewnątrz,
- specjalista ds. obsługi incydentów (ang. *incident handler*) – odpowiadający za koordynację przebiegu obsługi incydentów i komunikację z podmiotami constituency,
- analityk ds. bezpieczeństwa (ang. *security analyst*) – odpowiedzialny za analizę techniczną zdarzeń, danych i artefaktów,
- specjalista ds. komunikacji (ang. *communication expert*) – odpowiadający za bezpieczny i efektywny przepływ informacji, w tym między CSIRT-ami poziomu krajowego i sektorowymi, oraz prowadzenie komunikacji w mediach społecznościowych.

Jeśli kompetencje dla podanych wyżej ról w zespole są współdzielone oraz jeśli zespół pracuje w trybie 8/5, to aby osiągnąć minimalną odporność kadrową, powinien on liczyć co najmniej trzy osoby w pełnym wymiarze czasu pracy. Przy czym faktyczna liczba etatów (FTE[18]) przypisanych do każdej roli powinna być dostosowana przede wszystkim do skali działalności zespołu (liczby obsługiwanych podmiotów) oraz

[18] Z ang. *Full-Time Equivalent* – miara obciążenia pracą pracownika, będąca ekwiwalentem pracownika zatrudnionego w pełnym wymiarze godzin (pełnego etatu).

przyjętego trybu pracy. Przykładowo zapewnienie jednoosobowej obsady na stanowisku w trybie 24/7 wymaga 5,25 FTE (z uwzględnieniem urlopów i średniego czasu nieobecności w pracy z innych powodów), co w praktyce oznacza konieczność zatrudnienia sześciu pracowników.

Zgodnie z poziomem 2. modelu ENISA CMF zespół powinien przygotować wewnętrzny, udokumentowany opis zapewniania odporności kadrowej. Dobrą praktyką w tym zakresie jest opracowywanie grafików pracy i wprowadzenie podstawowych procedur przekazywania obowiązków na czas nieobecności, uwzględniających m.in. wymagane dostępy i uprawnienia, wgląd w komunikację dotyczącą obsługiwanych incydentów czy statusy prowadzonych spraw. W ramach szerszej polityki zarządzania ciągłością działania można uwzględnić możliwości tymczasowego uzupełniania zespołu (np. poprzez wsparcie z innych komórek organizacyjnych).

Praktycznym narzędziem wspierającym zarówno planowanie zasobów, jak i bieżące zarządzanie dostępnością kompetencji w zespole jest macierz kompetencji. Tego typu tabela pozwala w sposób przejrzysty zestawić:

- wymagania kompetencyjne wynikające z pełnionej roli (zob. parametr H-3),
- aktualny poziom kompetencji poszczególnych członków zespołu (samoocena lub ocena przełożonego),
- znajomość i poziom biegłości w obsłudze narzędzi istotnych dla zespołu CSIRT (np. zdefiniowanych w obszarze parametrów T).

Dobrze przygotowana macierz kompetencji:

- identyfikuje obszary ryzyka wynikające z nadmiernej koncentracji wiedzy lub braku zastępowalności,
- ułatwia planowanie szkoleń i rozwój kompetencji,
- wspiera decyzje kadrowe i organizacyjne (np. planowanie dyżurów, dobór do projektów),
- pozwala ocenić wpływ nieobecności danego pracownika na realizację kluczowych zadań.

Poniżej przedstawiamy przykładowy układ macierzy kompetencji. Takie macierze (jeśli CSIRT liczy wiele osób) można przygotowywać dla pojedynczych zespołów lub w podziale na usługi.

Tabela 4. Przykładowy układ macierzy kompetencji zespołu

Imię i nazwisko	Rola/ Stanowisko	Wymagane narzędzia	Obsługiwane narzędzia	Kogo może zastępować
Jan Kowalski	specjalista ds. obsługi incydentów	system ticketowy, komunikator, Malware Database (MWDB)	system ticketowy, komunikator, MWDB, Artemis	Anna Nowak, Piotr Zieliński
Anna Nowak	analityk ds. bezpieczeństwa	system ticketowy, komunikator, MWDB, analizator ruchu sieciowego, MWDB, skaner podatności	system ticketowy, komunikator, analizator ruchu sieciowego, MWDB, skaner podatności, platforma wymiany informacji o zagrożeniach cyberbezpieczeństwa, disassembler	Jan Kowalski
Piotr Zieliński	kierownik zespołu	pakiet biurowy, system ticketowy, komunikator	pakiet biurowy, system ticketowy, komunikator, MWDB, wyszukiwarka urządzeń i usług dostępnych w internecie, social media	Maria Lewandowska
Maria Lewandowska	specjalista ds. komunikacji	pakiet biurowy, system ticketowy, komunikator, social media	pakiet biurowy, system ticketow, komunikator, social media	—

Opis umiejętności (H-3)

Wartość parametru dla dojrzałości zespołu na poziomie Basic: 2.

Role w zespole CSIRT powinny być zdefiniowane i opisane, tak aby pracownicy wypełniali postawione przed nimi zadania na oczekiwanym poziomie. Dzięki sprecyzowaniu oraz udokumentowaniu wymaganych umiejętności i kompetencji dla poszczególnych ról w zespole CSIRT możliwe są właściwy dobór personelu oraz planowanie rozwoju zawodowego. Pozwala to również na identyfikację luk kompetencyjnych, które mogą mieć wpływ na efektywność realizacji zadań zespołu.

Opisy stanowisk w zespole muszą uwzględniać potrzebne umiejętności techniczne, wiedzę, doświadczenie oraz umiejętności miękkie. Przykładowo poniżej przedstawiamy tabelę z opisem umiejętności dla specjalisty ds. obsługi incydentów.

Tabela 5. Przykładowy opis umiejętności dla specjalisty ds. obsługi incydentów

Obszar kompetencji	Wymagania
Wykształcenie	Wyższe techniczne lub student ostatnich lat studiów o kierunku technicznym.
Wymagane kwalifikacje	• Znajomość języka angielskiego w stopniu umożliwiającym posługiwanie się dokumentacją techniczną, prowadzenie korespondencji oraz obsługa zgłoszeń telefonicznych. • Poświadczanie bezpieczeństwa do klauzuli POUFNE. • Znajomość zagrożeń z zakresu cyberbezpieczeństwa. • Znajomość procesów obsługi incydentów bezpieczeństwa.
Kwalifikacje uzupełniające	• Certyfikat/szkolenie z obszaru tzw. *blue team*. • Znajomość języka rosyjskiego. • Podstawowa umiejętność programowania.
Wymagane doświadczenie zawodowe	• Administrowanie systemami operacyjnymi Linux/*NIX i/lub Windows. • Obsługa zgłoszeń dotyczących cyberbezpieczeństwa. • Reagowanie na zagrożenia IT. • Weryfikacja i wyszukiwanie nowych zagrożeń. • Analiza zagrożeń. • Umiejętność korelacji danych dotyczących domeny. • Doświadczenie minimum 1 rok w ramach obsługi incydentów.
Wiedza	• Znajomość podstaw technicznych zasad działania internetu. • Znajomość podstawowych narzędzi kryptograficznych. • Znajomość podstaw bezpieczeństwa informacji. • Znajomość narzędzi do rejestracji oraz obsługi zgłoszeń i incydentów. • Znajomość procesów obsługi incydentów bezpieczeństwa. • Wiedza z zakresu cyberbezpieczeństwa. • Znajomość ustawy o krajowym systemie cyberbezpieczeństwa. • Znajomość ustawy o zwalczaniu nadużyć w komunikacji elektronicznej. • Znajomość narzędzi do tworzenia masowych wysyłek wiadomości e-mail. • Znajomość funkcjonowania Listy Ostrzeżeń przed niebezpiecznymi stronami. • Znajomość obsługi narzędzia klasy MWDB. • Znajomość metod weryfikacji podatnych instancji. • Wiedza na temat grup APT oraz grup haktywistycznych.

Umiejętności	• Umiejętność telefonicznej obsługi klienta. • Prawo jazdy kat. B i uprawnienia do prowadzenia samochodu służbowego.
Kompetencje oraz cechy dodatkowe	• Umiejętność skutecznej realizacji postawionych zadań. • Umiejętność analitycznego myślenia. • Umiejętność pracy samodzielnej oraz w zespole. • Umiejętność pracy pod presją czasu i w warunkach napływania znacznej ilości informacji. • Rzetelne podejście do pracy i wysoki poziom etyki zawodowej.

Wymagany zestaw kompetencji w zespole CSIRT powinien być ściśle powiązany z katalogiem świadczonych usług (zob. parametr O-5) i zapewniać zdolność ich skutecznej realizacji. Rozwijanie zdolności wykraczających poza ten katalog – takich jak zaawansowane analizy z zakresu informatyki śledczej (forensic) czy złośliwego oprogramowania – powinno być koordynowane z zespołami CSIRT poziomu krajowego, tak by kompetencje się wzajemnie uzupełniały i by się nie dublowały. Przydatnym narzędziem do identyfikacji i opisu wymagań kompetencyjnych na poszczególnych stanowiskach jest „NICE Framework”[19]. Rekomendujemy formalne zatwierdzenie wymagań kompetencyjnych przez kierownictwo organizacji.

Rozwój kompetencji członków zespołu (H-4)

Wartość parametru dla dojrzałości zespołu na poziomie Basic: 2.

Rozwój kompetencji członków zespołu CSIRT (ang. *Staff Development*) powinien mieć charakter planowy i systematyczny. Obejmuje on zarówno szkolenie nowych pracowników, jak i doskonalenie umiejętności osób już zatrudnionych. Kluczowym celem jest zapewnienie, że każdy członek zespołu posiada i rozwija kompetencje niezbędne do realizacji przypisanych mu zadań, zgodnych z katalogiem usług CSIRT-u. Ponadto dobrze zaplanowana polityka rozwoju przyczynia się do zwiększenia motywacji, ograniczenia rotacji kadr oraz do podniesienia dojrzałości operacyjnej zespołu.

Zakres rozwoju kompetencji może obejmować m.in.:

- program wdrożeniowy dla nowych pracowników (onboarding) uwzględniający m.in. strukturę organizacji, obowiązujące procedury i podstawy prawne, używane systemy i narzędzia czy powierzony zakres zadań,

[19] https://niccs.cisa.gov/workforce-development/nice-framework

- plan szkoleń i certyfikacji zewnętrznych,
- wewnętrzne warsztaty i ćwiczenia techniczne (np. hands-on labs, CTF-y),
- rozwój kompetencji miękkich (np. komunikacja, praca zespołowa, prezentacja ustaleń technicznych w sposób zrozumiały dla interesariuszy nietechnicznych),
- mentoring i dzielenie się wiedzą wewnątrz zespołu,
- udział w konferencjach branżowych, seminariach i grupach roboczych,
- regularne rozmowy rozwojowe i oceny postępów pracowników,
- wsparcie dla inicjatyw edukacyjnych wzmacniających współpracę i integrację zespołu.

Formalne zatwierdzenie polityki rozwoju przez kierownictwo zespołu nie jest wymagane na poziomie 2., jednak zespół powinien co najmniej opracowywać, utrzymywać i aktualizować roczny plan szkoleń (uwzględniający parametry H-5 i H-6 oraz pozyskanie wymaganych/oczekiwanych certyfikatów), a także mieć zabezpieczony budżet do ich realizacji.

Szkolenia techniczne (H-5)

Wartość parametru dla dojrzałości zespołu na poziomie Basic: 1.

Zespół CSIRT powinien zapewnić swoim członkom dostęp do podstawowych szkoleń technicznych, wspierających realizację ich ról i obowiązków oraz umożliwiających podniesienie kwalifikacji, w szczególności w obszarach odpowiadających zakresowi świadczonych usług (zob. O-5). Regularny dostęp do zewnętrznych szkoleń technicznych jest niezbędny do utrzymania kompetencji zespołu na właściwym poziomie. To kluczowy warunek umożliwiający skuteczne reagowanie na zmieniające się zagrożenia w cyberprzestrzeni. Warto zadbać, by członkowie zespołu znali dostępne możliwości rozwoju i byli zachęcani do udziału w szkoleniach zgodnych z ich specjalizacją i zakresem obowiązków.

Zespół CSIRT, uwzględniając wymagania wynikające z pełnionych ról (zob. parametr H-3), powinien zidentyfikować potrzeby technicznego rozwoju pracowników oraz opracować na tej podstawie (lub jako część planu opisanego w parametrze H-4) plan szkoleń technicznych. Na poziomie Basic zalecamy wybór szkoleń:

- dostępnych online lub w modelu hybrydowym,
- zgodnych z rolą CSIRT-u (np. o profilu koordynacyjnym),
- o potwierdzonej jakości (np. prowadzone przez organizacje, takie jak ENISA, FIRST, lub uznanych dostawców komercyjnych),
- dopasowanych do dostępnego budżetu.

Jako narzędzie pomocnicze polecamy „Security Certification Roadmap" autorstwa Paula Jerimy'ego (https://pauljerimy.com/security-certification-roadmap/), który grupuje dostępne certyfikaty i szkolenia według obszarów specjalizacji (np. Communication and Network Security, Security and Risk Management, Software Security, Security Operations) oraz poziomu zaawansowania. Dla zespołów o profilu „blue team" (obrona i reagowanie) rekomendujemy w szczególności certyfikaty i kursy oznaczone kolorem niebieskim. Warto również uwzględnić możliwość udziału w praktykach i wydarzeniach branżowych (warsztaty, ćwiczenia, konferencje) jako element poszerzający wiedzę i wspierający networking.

Szkolenia z umiejętności miękkich (H-6)

Wartość parametru dla dojrzałości zespołu na poziomie Basic: 1.

Choć kompetencje techniczne stanowią podstawę funkcjonowania zespołów CSIRT, w praktyce to właśnie umiejętności miękkie często decydują o skuteczności działania – zwłaszcza w zespołach o profilu koordynacyjnym, gdzie większość działań opiera się na współpracy, komunikacji i relacjach z innymi interesariuszami.

Rekomendujemy, by umożliwić członkom zespołu rozwój umiejętności takich jak:

- komunikacja interpersonalna i pisemna (tworzenie raportów, alertów, rekomendacji),
- zarządzanie stresem i działanie pod presją czasu,
- prowadzenie rozmów z trudnymi interesariuszami,
- prowadzenie prezentacji, spotkań i warsztatów,
- współpraca w zespole oraz z partnerami zewnętrznymi,
- komunikacja kryzysowa, także z mediami – w razie potrzeby.

Zespół CSIRT, uwzględniając wymagania wynikające z pełnionych ról (zob. parametr H-3), powinien zidentyfikować potrzeby w zakresie obszarów wymienionych wyżej oraz opracować na tej podstawie (lub jako część planu opisanego w parametrze H-4) plan szkoleń. Warto zwrócić uwagę, że kompetencje miękkie mają zastosowanie nie tylko w działaniach roboczych zespołu, lecz także w komunikacji nieformalnej, społecznej (np. na konferencjach, w mediach społecznościowych) oraz w reprezentowaniu zespołu na zewnątrz.

Dobrą praktyką jest także udział w warsztatach i wydarzeniach branżowych, które sprzyjają budowaniu kompetencji miękkich w sposób naturalny, poprzez kontakt z innymi profesjonalistami i wymianę doświadczeń. Największą wartość mają warsztaty

praktyczne oraz ćwiczenia symulacyjne, w tym te uwzględniające sytuacje kryzysowe i konieczność działania zespołowego.

Budowanie sieci kontaktów (H-7)

Wartość parametru dla dojrzałości zespołu na poziomie Basic: 2.

Nawiązywanie i utrzymywanie relacji z innymi zespołami CSIRT oraz inicjatywy współpracy branżowej umożliwiają wymianę informacji o zagrożeniach i dobrych praktykach. Współpraca znacząco zwiększa efektywność działań zespołu poprzez dostęp do szerszego zakresu wiedzy oraz wsparcia merytorycznego.

Sieć relacji powinna być budowana na podstawie kontaktów pozyskanych w ramach uczestnictwa w systemach współpracy CSIRT (zob. parametr O-9). Warto, żeby przedstawiciele zespołu brali udział w spotkaniach i wydarzeniach. Osobista znajomość członków *constituency* oraz przedstawicieli innych zespołów CSIRT i związana z tym możliwość dostępu do pozasłużbowych danych kontaktowych mogą być szczególnie przydatne w sytuacjach niecierpiących zwłoki.

Do osiągnięcia poziomu 2. niezbędne jest, aby zespół CSIRT miał wewnętrznie spisane zasady członkostwa w zewnętrznych organizacjach.

Narzędzia (T)

Jednym z głównych wyzwań na etapie budowy CSIRT-u jest zaprojektowanie i wdrożenie odpowiedniego zaplecza technicznego, które umożliwi skuteczną realizację zadań. Kluczowy jest właściwy dobór narzędzi zarówno pod względem ich funkcjonalności, jak i zgodności z potrzebami wynikającymi z katalogu świadczonych usług (zob. parametr O-5). To właśnie zakres usług determinuje, jakie narzędzia powinny znaleźć się ostatecznie w zasobie zespołu. Inne będą potrzebne w przypadku CSIRT-u o profilu koordynacyjnym, inne dla zespołów rozbudowujących dodatkowo zdolności analizy technicznej (np. forensic czy malware analysis). Nasze rekomendacje w zakresie zaplecza technicznego będą oparte na pierwotnym założeniu, że zespół cyberbezpieczeństwa powinien mieć charakter koordynacyjny.

Warto podkreślić, że współczesne narzędzia coraz częściej łączą wiele funkcji, co oznacza, że systemy służące pierwotnie do wykrywania incydentów mogą wspierać również działania analityczne czy komunikację z podmiotami objętymi usługą. Dlatego narzędzia omawiane w dalszej części publikacji mogą być przypisane do więcej niż jednego parametru T. Należy to traktować jako naturalną konsekwencję rosnącej uniwersalności stosowanych rozwiązań, a nie ograniczenie naszych rekomendacji. W opisach parametrów koncentrujemy się na wskazaniu obszarów funkcjonalnych oraz dojrzałości wymaganej dla poszczególnych kategorii narzędzi. Ważne jest, aby każdy członek zespołu CSIRT był świadomy dostępnych narzędzi oraz ich zastosowania. Dlatego zaleca się dokumentowanie i przechowywanie listy tych narzędzi w wewnętrznym repozytorium wiedzy (zob. parametr T-1), co zapewnia spójność działań i efektywność operacyjną.

Zaplecze techniczne CSIRT-u obejmuje również infrastrukturę własną (wewnętrzną) zespołu. Powinna ona umożliwiać wdrożenie niezbędnych narzędzi, wspierać realizację zadań oraz zapewnić bezpieczeństwo operacyjne.

Do najważniejszych zagadnień z obszaru infrastruktury własnej, które należy uwzględnić w trakcie tworzenia zespołu CSIRT, należą:

- segmentacja sieci – zaprojektowanie architektury logicznej z wyodrębnieniem VLAN-ów oraz wdrożeniem mechanizmów kontroli i inspekcji ruchu sieciowego pomiędzy segmentami,
- system pocztowy – uruchomienie niezależnego serwera pocztowego z uwzględnieniem wymagań bezpieczeństwa (TLS, MFA, antyspam) i integracji z innymi narzędziami CSIRT-u,

- tzw. „brudny” internet – wydzielenie izolowanego środowiska do analizy zagrożeń, z zastosowaniem anonimizacji, inspekcji ruchu i monitorowania sesji,
- system monitorowania infrastruktury wewnętrznej – wdrożenie rozwiązań klasy EDR/XDR, SIEM, IDS/IPS, NDR oraz PAM, umożliwiających detekcję i reakcję na potencjalne incydenty wewnętrzne,
- system przechowywania danych – zaprojektowanie i implementacja warstwowego systemu storage dostosowanego do rodzaju danych (obrazy dysków, logi, próbki malware, backupy, dokumentacja operacyjna),
- repozytorium wiedzy – uruchomienie systemu wiki lub bazy wiedzy zawierającej procedury operacyjne, scenariusze reagowania oraz informacje o constituency,
- stacje klienckie – standaryzacja środowisk pracy na podstawie ról operacyjnych, z określeniem wymagań dotyczących systemów operacyjnych, narzędzi i zabezpieczeń,
- środowisko wirtualizacyjne – wdrożenie platformy wirtualizacji (np. Proxmox, ESXi, KVM) wraz z systemem zarządzania, automatyzacją wdrażania maszyn oraz integracją z pozostałymi komponentami infrastruktury CSIRT.

Minimalny zestaw rekomendowanych zasobów został przedstawiony w **załączniku nr 2** „Przykładowa architektura i wymagania dla środowiska wewnętrznego CSIRT”.

Uwaga: przed skorzystaniem z różnych opisywanych poniżej narzędzi i usług należy dokładnie zapoznać się z warunkami licencyjnymi. Na przykład pliki przesłane do serwisu VirusTotal są dostępne do pobrania dla innych użytkowników (zwłaszcza tych mających konta premium), co wiąże się z ryzykiem ujawnienia wrażliwych informacji.

Zasoby i konfiguracje IT (T-1)

Wartość parametru dla dojrzałości zespołu na poziomie Basic: 1.

Efektywne zarządzanie incydentami oraz świadczenie usług przez CSIRT wymagają możliwie największej wiedzy na temat środowiska technicznego podmiotów wchodzących w skład jego *constituency* (zob. również opis parametru O-2). Zespół powinien zatem posiadać dostęp do aktualnej i wystarczająco szczegółowej listy zasobów IT wykorzystywanych przez podmioty constituency, w tym do informacji o sprzęcie, oprogramowaniu, systemach OT oraz o ich konfiguracjach (np. wersje systemów, aplikacji, wykorzystywane komponenty).

Dostęp do takich informacji umożliwia:

- świadczenie usług w sposób dostosowany do realiów technologicznych constituency,
- efektywniejsze szacowanie podatności i ryzyka,
- szybsze reagowanie na nowe zagrożenia (np. możliwość oceny, które podmioty są zagrożone konkretną podatnością),
- prowadzenie działań analitycznych, ostrzegawczych i prewencyjnych.

CSIRT nie musi samodzielnie prowadzić kompletnego wykazu zasobów. W praktyce rekomendujemy stworzenie i utrzymywanie bazy na podstawie danych przekazywanych przez punkty kontaktowe w podmiotach constituency, zbierane w trakcie obsługi incydentów lub na wniosek CSIRT-u poziomu krajowego lub sektorowego.

Zakres listy powinien obejmować co najmniej zasoby krytyczne dla ciągłości działania podmiotów constituency lub mające istotny wpływ na bezpieczeństwo teleinformatyczne. Przykłady takich zasobów to systemy SCADA i DCS w infrastrukturze przemysłowej, systemy klasy ERP lub HIS w sektorze ochrony zdrowia, platformy zarządzania danymi w administracji publicznej, serwery DNS, systemy uwierzytelniania, poczty elektronicznej czy repozytoria kodu wykorzystywane w procesach DevOps. Warto również uwzględnić typowe komponenty infrastruktury sieciowej (firewalle, przełączniki, urządzenia brzegowe), jak i używane platformy chmurowe, jeżeli mają wpływ na przetwarzanie danych lub realizację usług kluczowych w danym sektorze.

Dla zespołów, które utrzymują własne repozytorium wiedzy, dobrym rozwiązaniem może być integracja tej listy z systemem zarządzania treścią. Takie repozytorium może funkcjonować na bazie oprogramowania typu wiki lub innych narzędzi umożliwiających tworzenie i aktualizowanie dokumentacji przez zespół. W zależności od potrzeb i skali działania, możliwe jest również wykorzystanie narzędzi klasy ITAM lub prostych systemów bazodanowych.

W praktyce, szczególnie na początkowym etapie funkcjonowania zespołu, do prowadzenia takiego rejestru wystarczy dobrze zaprojektowany arkusz kalkulacyjny (np. Excel), zawierający informacje o:

- typach urządzeń i oprogramowania (serwery, systemy operacyjne, bazy danych, aplikacje biznesowe, systemy SCADA itp.),
- wersjach systemów i aplikacji,
- konfiguracjach istotnych z punktu widzenia bezpieczeństwa (np. otwarte porty, domyślne konta, aktualizacje),
- lokalizacji lub przynależności do konkretnego podmiotu.

Dla zespołów działających w zróżnicowanych technologicznie sektorach rekomenduje się skupienie na elementach infrastruktury krytycznej i systemach kluczowych dla realizacji usług podstawowych.

Źródła informacji (T-2)

Wartość parametru dla dojrzałości zespołu na poziomie Basic: 2.

W ramach realizacji wymagań CSIRT powinien zapewnić sobie stały dostęp do wiarygodnych i aktualnych źródeł informacji o zagrożeniach oraz podatnościach, w szczególności tych istotnych z punktu widzenia obsługiwanego constituency.

Zalecamy, aby CSIRT sektorowy regularnie pozyskiwał dane dotyczące m.in.:

- znanych podatności w oprogramowaniu oraz komponentów wykorzystywanych w podmiotach constituency,
- podatności konfiguracyjnych np. publicznie dostępne panele logowania, domyślne konfiguracje, błędne ustawienia usług,
- technik, taktyk i procedur (TTP) stosowanych przez grupy przestępcze i innych zagrożeń APT,
- wskaźników kompromitacji (IoC),
- zagrożeń związanych z łańcuchem dostaw, phishingiem czy kampaniami ukierunkowanymi.

Jednym ze sposobów realizacji wymagania posiadania sprawdzonych źródeł wiedzy może być skorzystanie z bezpłatnych narzędzi i usług udostępnianych przez CERT Polska. Narzędzia te wspierają automatyczne pozyskiwanie oraz analizę informacji o zagrożeniach, w tym danych kontekstowych istotnych dla podmiotów constituency.

Poniżej przedstawiamy rekomendowane narzędzia CERT Polska, z których powinien korzystać każdy CSIRT:

- MWDB (Malware Database), https://mwdb.cert.pl/ – baza danych złośliwego oprogramowania z informacjami o IoC, TTP, powiązaniach między kampaniami.
- moje.cert.pl – system łączący wiele systemów rozwijanych przez CERT Polska. Można za jego pomocą m.in. uzyskać informacje na temat wycieków haseł użytkowników w swojej domenie, zamówić bezpłatne skanowanie bezpieczeństwa wszystkich swoich domen czy otrzymywać informacje o infekcjach szkodliwym oprogramowaniem i innych zagrożeniach w swoich sieciach.

- n6 (Network Security Incident eXchange), https://cert.pl/n6/ – usługa, dzięki której przedsiębiorstwa i instytucje otrzymują informacje o problemach bezpieczeństwa w ich infrastrukturze. Udostępniane dane dotyczą m.in. infekcji szkodliwym oprogramowaniem, hostowania szkodliwej treści (np. phishing) czy podatności w aplikacjach dostępnych z internetu.

Aby mieć pełny obraz zagrożeń, CSIRT-y powinny korzystać również z innych dostępnych źródeł, zarówno komercyjnych, jak i udostępnianych na licencji open source.

Wśród źródeł danych można wymienić m.in.:

- Serwisy umożliwiające weryfikację podejrzanych plików pod kątem szkodliwości i przedstawienie wyników oraz pozwalające przeszukiwać pliki weryfikowane przez wszystkich innych użytkowników.
- Serwisy będące wyszukiwarkami urządzeń i usług dostępnych w internecie, które umożliwiają identyfikację otwartych portów, banerów usług oraz potencjalnych podatności w publicznie dostępnej infrastrukturze sieciowej.
- Shadowserver, https://www.shadowserver.org/ – bezpłatnie udostępniane dane z globalnych skanów sieci, które pomagają wykrywać zagrożenia, podatności i nieprawidłowo skonfigurowane usługi.

Warto korzystać również z różnych otwartych źródeł danych udostępnianych np. przez:

- instytucje branżowe i międzynarodowe (np. ENISA, FIRST, US-CERT, CISA),
- publiczne kanały dystrybucji danych np. MISP, bazy podatności (np. CVE, NVD),
- organizacje branżowe w formie feedów zagrożeń (np. MITRE ATT&CK, CISA Known Exploited Vulnerabilities),
- portale branżowe polskie i zagraniczne (np. blogi zajmujące się cyberbezpieczeństwem).

Włączając nowe źródła informacji, zespół powinien kierować się jasno określonymi kryteriami oceny (zob. parametr P-12). Każde nowe źródło powinno zostać opisane w rejestrze, zawierającym co najmniej:

- nazwę i typ źródła (np. komercyjne, społecznościowe, open source),
- charakter dostarczanych informacji (np. IOC, TTP, podatności, alerty),
- sposób pozyskiwania danych (np. kanał dostępu, format, częstotliwość aktualizacji),
- ocenę wiarygodności (np. duża, średnia, mała),

- informację o właścicielu wewnętrznym (osobie odpowiedzialnej za nadzór nad źródłem),
- datę ostatniego przeglądu przydatności oraz zalecany termin kolejnego.

W praktyce, szczególnie na początkowym etapie funkcjonowania zespołu, do prowadzenia takiego rejestru wystarczający będzie dobrze zaprojektowany arkusz kalkulacyjny (np. Excel). Przykładowy wygląd rejestru źródeł informacji przedstawia **załącznik nr 3.**

Należy jednak pamiętać, że samo pozyskanie danych to dopiero pierwszy krok. Równie istotne jest ich wprowadzenie do środowiska operacyjnego (integracja z innymi narzędziami i procesami), które często wymaga dużego nakładu pracy, odpowiednich narzędzi i kompetencji. W wielu przypadkach jest to zadanie na pełny etat, szczególnie przy korzystaniu z wielu źródeł równolegle. Kluczowe jest również zapewnienie analizy zebranych danych (zob. parametr P-5), tak aby realnie wspierały one procesy wykrywania zagrożeń i reagowania na nie.

Zintegrowany system komunikacji (T-3)

Wartość parametru dla dojrzałości zespołu na poziomie Basic: 1.

Skuteczne zarządzanie incydentami wymaga stałej, sprawnej i uporządkowanej wymiany informacji pomiędzy członkami zespołu CSIRT, niezależnie od miejsca pracy, aktualnego dyżuru czy dostępności poszczególnych osób. System umożliwiający ciągłe dzielenie się informacjami stanowi jedno z kluczowych narzędzi zapewniających zespołowi realizację tego zadania. Zgłoszenia o zagrożeniach lub potencjalnych incydentach mogą napływać kanałami zarówno oficjalnymi (e-mail, formularze), jak i nieformalnymi (np. szyfrowane komunikatory), a kontakt z partnerami i innymi zespołami CSIRT może obejmować zarówno bieżącą wymianę informacji, jak i pilne konsultacje techniczne. Rozproszenie komunikacji między różnymi kanałami może prowadzić do utraty ciągłości operacyjnej, spadku efektywności działań oraz braku wspólnego kontekstu dla zespołu.

Dlatego rekomendujemy utworzenie **wewnętrznego systemu komunikacji**, który zapewniałby co najmniej:

- wspólny dostęp wszystkich członków zespołu do wiadomości i aktualnych wątków spraw,
- możliwość tworzenia tematycznych kanałów dyskusyjnych (np. incydenty, zagrożenia, współpraca z CSIRT-ami poziomu krajowego i sektorowymi),
- przeszukiwanie treści i przeglądanie archiwalnych informacji,

- kontrolę uprawnień i logowanie dostępu,
- automatyczne tworzenie kopii zapasowych.

Do takiego systemu powinny trafiać istotne informacje pochodzące z innych źródeł, np.:

- zgłoszenia incydentów (wraz z linkiem do ticketu z systemu rejestracji),
- informacje uzyskane w ramach współpracy z innymi CSIRT-ami lub społecznościami cyberbezpieczeństwa,
- alerty ze źródeł typu threat intelligence,
- korespondencja e-mail z podmiotami znajdującymi się w *constituency*.

Dzięki temu wszyscy członkowie zespołu zaangażowani w daną sprawę będą mogli na bieżąco monitorować prowadzone działania. Przyczyni się to także do budowania wspólnej świadomości sytuacyjnej. Rekomendujemy stosowanie rozwiązań typu self-hosted, które zapewniają pełną kontrolę nad infrastrukturą i danymi. W przypadku korzystania z infrastruktury komunikacyjnej organizacji macierzystej (np. systemów pocztowych dostarczanych przez firmę zewnętrzną), należy pamiętać o potencjalnych problemach związanych z filtrami antyspamowymi. Zgłoszenia incydentów zawierające złośliwe oprogramowanie lub przykłady phishingu mogą być automatycznie usuwane, zanim trafią do zespołu. Rekomendujemy wówczas wydzielenie odrębnej skrzynki CSIRT-u lub wprowadzenie wyjątków konfiguracyjnych, ponieważ wyłączenie filtrów antyspamowych dla całej organizacji może być niemożliwe lub zmniejszy jej bezpieczeństwo, czego co do zasady chcemy uniknąć.

System śledzenia incydentów (T-4)

Wartość parametru dla dojrzałości zespołu na poziomie Basic: 2.

Efektywna obsługa zgłoszeń incydentów wymaga odpowiedniego narzędzia, które umożliwia rejestrację, śledzenie i dokumentowanie działań podejmowanych przez zespół CSIRT. Nawet w zespołach o niewielkiej liczbie obsługiwanych podmiotów zarządzanie incydentami wyłącznie przy użyciu prostych narzędzi, jak arkusze kalkulacyjne, szybko prowadzi do problemów z kontrolą przebiegu obsługi i komunikacją. Dlatego rekomendujemy wykorzystanie dedykowanego systemu typu ticketowego, przeznaczonego do pracy w obszarze cyberbezpieczeństwa, który zapewni uporządkowany przepływ informacji, możliwość monitorowania postępu prac oraz rozliczalność działań.

Tego typu systemy pozwalają nie tylko na lepszą organizację pracy zespołu, lecz także na spełnienie wymagań związanych z przechowywaniem i przetwarzaniem informacji wrażliwych. W przypadku CSIRT-ów funkcjonujących w urzędach obsługujących organ właściwy dopuszczalne jest korzystanie z systemów zgłoszeń awarii używanych przez jednostkę macierzystą. Należy jednak pamiętać, że wiele takich systemów nie uwzględnia specyfiki przetwarzania danych o incydentach bezpieczeństwa (mogą występować ograniczenia w zakresie poufności, możliwości kontroli dostępu czy szyfrowania danych – typowym przykładem jest brak wsparcia dla PGP/GPG).

Spośród dostępnych narzędzi warto wymienić sprawdzone i popularne rozwiązania, takie jak:

- RTIR, https://bestpractical.com/rtir – Request Tracker for Incident Response,
- OTRS, https://otrs.com/ – Open Source Ticket Request System,
- TheHive, https://strangebee.com/thehive/, https://github.com/TheHive-Project/TheHive – darmowa i otwartoźródłowa platforma do obsługi incydentów bezpieczeństwa.

Wybór konkretnego narzędzia powinien być uzależniony od katalogu świadczonych usług (zob. O-5), skali działalności oraz zdolności technicznych zespołu. Zalecamy wdrożenie rozwiązania, które pozwoli na:

- przechowywanie pełnej historii zgłoszenia,
- przypisywanie incydentów do konkretnych członków zespołu,
- śledzenie statusu oraz czasu reakcji,

- integrację z innymi narzędziami używanymi przez zespół (np. CTI, systemy ticketowe partnerów, narzędzia opisane w kolejnych parametrach T).

Dodatkowo rekomendujemy rozbudowę wybranego rozwiązania o dodatkowe skrypty automatyzujące wybrane procesy w obsłudze incydentów.

Odporne połączenia głosowe i komunikacja tekstowa (T-5, T-6)

Wartość parametru dla dojrzałości zespołu na poziomie Basic: 2.

Komunikacja głosowa, realizowana zarówno tradycyjnie, poprzez połączenia telefoniczne, jak i za pośrednictwem komunikatorów, oraz możliwość przesyłania wiadomości (w tym e-mail i komunikatory tekstowe) są istotnymi elementami codziennej pracy zespołu. Dlatego tak istotne jest zapewnienie wysokiej dostępności narzędzi wspierających, tak by ewentualne awarie nie wpłynęły na zdolności operacyjne CSIRT-u. W przeciwieństwie do potrzeby konsolidacji wewnętrznej wymiany informacji w jednym systemie (zob. T-3) odporność komunikacji można osiągnąć poprzez świadome rozproszenie kanałów i środków komunikacji.

Odpowiednio do możliwości zespołu zalecamy utrzymywanie kilku niezależnych narzędzi komunikacji. Do wyboru są:

- tradycyjne połączenia telefoniczne (linie stacjonarne, komórkowe) – zwłaszcza, gdy zespół korzysta z usług więcej niż jednego operatora,
- telefonia IP,
- szyfrowane komunikatory,
- e-mail (z bezpiecznym systemem backupu i dostępnością hot-standby).

System poczty elektronicznej, jako podstawowy kanał odbioru zgłoszeń, powinien być zaprojektowany z myślą o odporności, najlepiej poprzez wdrożenie redundantnej infrastruktury lub mechanizmów szybkiego przełączania (hot-standby) wraz z niezawodnymi mechanizmami backupu, spełniającymi wymagania ciągłości działania (np. określonymi dla parametru O-7). W przypadku komunikatorów szyfrowanych, gdzie dane nie są przechowywane w chmurze, istotne jest opracowanie własnych rozwiązań archiwizacyjnych.

Aby osiągnąć dojrzałość na poziomie 2., CSIRT powinien przygotować wewnętrznie udokumentowaną listę wykorzystywanych środków komunikacji i sposobów działa-

nia w przypadku awarii/niedostępności któregoś z nich. Ten wymóg można z powodzeniem zrealizować w ramach repozytorium wiedzy, o którym jest mowa w parametrze T-1.

Stały dostępu do internetu (T-7)

Wartość parametru dla dojrzałości zespołu na poziomie Basic: 2.

Ciągły i niezawodny dostęp do internetu jest warunkiem koniecznym funkcjonowania zespołu. Bez niego w praktyce nie jest możliwa realizacja zadań CSIRT-u. Optymalnym i rekomendowanym przez nas rozwiązaniem jest pełna, również fizyczna, redundancja dostępu do internetu. W wielu przypadkach wystarczającym zabezpieczeniem może być jednak tańsze rozwiązanie, np. zapasowe łącze oparte na innej technologii (np. światłowód + LTE). Ponieważ większość zespołów korzysta z infrastruktury organizacji macierzystej, warto zadbać o to, by również CSIRT był w niej klasyfikowany jako jednostka o krytycznych wymaganiach dotyczących niezawodności łącza internetowego.

Narzędzia do zapobiegania incydentom (T-8)

Wartość parametru dla dojrzałości zespołu na poziomie Basic: 2.

W celu skutecznego zapobiegania incydentom bezpieczeństwa, zespół CSIRT powinien dysponować jasno określonym i wdrożonym zestawem narzędzi prewencyjnych. Narzędzia te stanowią pierwszą linię obrony dla obsługiwanych podmiotów (*constituency*) i odgrywają kluczową rolę w identyfikacji oraz eliminacji potencjalnych zagrożeń.

Ze względu na rosnącą liczbę dostępnych rozwiązań istotne jest, aby zespół CSIRT aktywnie uczestniczył w procesie wyboru, integracji i zarządzania automatyzacją (orkiestracji) tych narzędzi, aby dostosować je do specyfiki i potrzeb obsługiwanych podmiotów.

Przykładowe narzędzia wspierające działania prewencyjne zespołu CSIRT, szczególnie w zakresie skanowania infrastruktury podmiotów, obejmują:

- OpenVAS, https://www.openvas.org/ – otwartoźródłowy skaner podatności umożliwiający identyfikację znanych luk w zabezpieczeniach systemów i aplikacji.
- Komercyjne narzędzia do oceny podatności, oferujące szeroki zakres testów bezpieczeństwa i raportów.

- Wyszukiwarki urządzeń podłączonych do internetu umożliwiające identyfikację serwerów, kamer IP, routerów i innych urządzeń oraz analizę ich banerów usługowych, oferujące zaawansowane możliwości filtrowania i analizy danych zebranych z publicznie dostępnych źródeł.
- Artemis, https://github.com/CERT-Polska/Artemis – otwartoźródłowe narzędzie opracowane przez CERT Polska służące do skanowania w poszukiwaniu podatności i błędów konfiguracyjnych w publicznie dostępnych systemach internetowych.

Regularne korzystanie z tych narzędzi pozwala na skuteczne monitorowanie infrastruktury, identyfikację nieautoryzowanych usług oraz ocenę potencjalnych zagrożeń wynikających z ekspozycji zasobów w internecie. Dzięki temu CSIRT może proaktywnie reagować na pojawiające się incydenty i minimalizować ryzyko dla podmiotów *constituency*.

Podobnie jak w przypadku pozostałych parametrów dojrzałości na poziomie 2. CSIRT powinien mieć wewnętrznie udokumentowaną listę wykorzystywanych narzędzi. Ten wymóg można z powodzeniem zrealizować w ramach repozytorium wiedzy.

Narzędzia do wykrywania incydentów (T-9)

Wartość parametru dla dojrzałości zespołu na poziomie Basic: 2.

Aby CSIRT mógł skutecznie wykrywać incydenty bezpieczeństwa, musi mieć jasno zdefiniowany i wdrożony zestaw narzędzi wspierających ten proces. Narzędzia te są „oczami i uszami" zespołu, ponieważ dostarczają informacji o zagrożeniach i incydentach, zarówno tych potencjalnych, jak i już zaistniałych.

Jednym z kluczowych narzędzi wspierających zespół CSIRT w procesie wykrywania incydentów jest intuicyjny formularz zgłoszeniowy. Odpowiednio zaprojektowany, umożliwia szybkie i efektywne przekazywanie informacji o zdarzeniach bezpieczeństwa i jest istotnym elementem pierwszej linii obrony.

Dobrze przygotowany formularz powinien łączyć w sobie prostotę z funkcjonalnością, tak aby już na etapie pierwotnego zgłoszenia można było uzyskać dane niezbędne do wstępnej analizy incydentu. Ważne jest, aby każdy członek zespołu CSIRT znał ten formularz oraz aby jego struktura i sposób wykorzystania były udokumentowane w wewnętrznym repozytorium wiedzy zespołu.

CERT Polska oferuje sprawdzony formularz zgłaszania incydentów dostępny pod adresem https://incydent.cert.pl, który od lat wspiera użytkowników w efektywnym raportowaniu zdarzeń cyberbezpieczeństwa.

Przykładowe inne narzędzia wspierające wykrywanie incydentów:

- IntelMQ, https://github.com/certtools/intelmq – system do przetwarzania informacji o zagrożeniach, umożliwiający automatyczne zbieranie, przetwarzanie i dystrybucję danych o incydentach.
- OpenCTI, https://filigran.io/solutions/open-cti/ – platforma umożliwiająca analizę informacji o zagrożeniach w czasie rzeczywistym oraz integrację z innymi systemami w celu szybkiego reagowania na potencjalne zagrożenia.

Regularne korzystanie z powyższych narzędzi pozwala zespołom CSIRT na proaktywne monitorowanie *constituency*. Dzięki temu możliwe jest skuteczne zapobieganie incydentom bezpieczeństwa i minimalizowanie ryzyka dla obsługiwanych organizacji. Warto tu wspomnieć o tym, że w związku z przyjętym przez nas założeniu o koordynacyjnym charakterze zespołu CSIRT, świadomie nie uwzględniliśmy narzędzi klasy SIEM (Security Information and Event Management), EDR (Endpoint Detection and Recovery) czy NDR (Network Detection and Recovery).

Narzędzia do rozwiązywania incydentów (T-10)

Wartość parametru dla dojrzałości zespołu na poziomie Basic: 2.

Rozwiązywanie lub wsparcie w rozwiązywaniu incydentów stanowi istotę działalności każdego zespołu CSIRT, dlatego konieczne jest posiadanie odpowiedniego zestawu narzędzi wspierających analizę, podejmowanie działań zaradczych oraz przywracanie zaatakowanych systemów do działania. Zestaw ten powinien być jasno zdefiniowany, udokumentowany, na bieżąco aktualizowany i dostosowany do specyfiki obsługiwanych incydentów i charakteru usług świadczonych przez CSIRT.

CSIRT powinien być aktywnie zaangażowany w dobór, konfigurację i eksploatację narzędzi – niezależnie od tego, czy korzysta z nich bezpośrednio, czy tylko odbiera wyniki ich działania (np. z systemów obsługiwanych przez inne jednostki). Kluczowe jest, aby zespół miał realny wpływ na rozwój i doskonalenie wykorzystywanych rozwiązań.

Warto zwrócić uwagę, że na rynku jest obecnie bardzo duży wybór narzędzi, co sprawia, że jeszcze większego znaczenia nabiera ich efektywna integracja i zarządzanie

nimi jako spójnym środowiskiem pracy. Umiejętność budowy prostych integracji, automatyzacji powtarzalnych czynności i stosowania lekkiej orkiestracji staje się istotnym elementem dojrzałości technicznej zespołu. Tam, gdzie gotowe rozwiązania nie oferują wszystkich niezbędnych funkcji, zespół powinien rozważyć tworzenie własnych rozszerzeń, np. skryptów, parserów czy prostych interfejsów pośredniczących.

Warto również podkreślić, że zestaw narzędzi do rozwiązywania incydentów obejmuje zarówno oprogramowanie, jak i dedykowane urządzenia. W niektórych przypadkach może to oznaczać konieczność utworzenia specjalistycznych laboratoriów, np. do analizy złośliwego oprogramowania czy informatyki śledczej.

Przykładowe narzędzia wspierające proces rozwiązywania incydentów:

- Sysinternals Suite, https://learn.microsoft.com/en-us/sysinternals/downloads/sysinternals-suite – zbiór narzędzi diagnostycznych dla systemu Windows, takich jak Process Explorer, Autoruns czy TCPView, które wspierają analizę zachowania procesów, usług i połączeń sieciowych.
- Wireshark, https://www.wireshark.org/ – analizator ruchu sieciowego umożliwiający szczegółową inspekcję pakietów, co jest przydatne w identyfikacji nieautoryzowanych komunikacji i anomalii w ruchu sieciowym.
- ELK Stack (Elasticsearch, Logstash, Kibana), https://www.elastic.co/elastic-stack – platforma do gromadzenia, przetwarzania i wizualizacji logów, wspierająca analizę zdarzeń i identyfikację wzorców zachowań.
- CAPE Sandbox https://capev2.readthedocs.io/en/latest/, Cuckoo Sandbox https://github.com/cuckoosandbox – otwartoźródłowe środowisko do dynamicznej analizy złośliwego oprogramowania, umożliwiające obserwację jego działania w kontrolowanym środowisku.

Procesy (P)

Część „Procesy” (P) na poziomie ENISA Basic koncentruje się na wprowadzeniu podstawowych procesów operacyjnych i wspierających, które umożliwiają zespołowi CSIRT realizację jego mandatu (O-1) oraz świadczenie zadeklarowanych usług (O-5).

SIM3 traktuje pojęcie procesu bardzo szeroko, obejmując nim również czynności, które w ugruntowanej terminologii zarządzania należałoby zaklasyfikować jako procedury, polityki lub standardy postępowania.

W praktyce CSIRT-y często opracowują procedury operacyjne, które zawierają zarówno elementy procesu, jak i procedury.
Każda procedura operacyjna, opracowana na podstawie opisywanych w tej części parametrów, powinna być udokumentowana i dostępna wewnętrznie, np. w postaci wpisu w wiki lub innym repozytorium wiedzy zespołu. Dla wybranych parametrów wymagane jest również formalne zatwierdzenie przez kierownictwo zespołu cyberbezpieczeństwa.

Rekomendujemy, by procedury operacyjne zawierały następujące elementy:

1. Nazwa procedury – powinna być jednoznaczna i zawierać odniesienie do procesu oraz aktywności.
2. Cel procedury – krótki opis, co procedura ma osiągnąć, np. *Zapewnienie szybkiego i zgodnego z wymaganiami ustawowymi oraz uzgodnieniami przekazania informacji o incydencie poważnym do właściwego CSIRT-u poziomu krajowego*.
3. Zakres stosowania – określenie, w jakich sytuacjach (do jakich sytuacji, systemów, incydentów lub jednostek) procedura ma zastosowanie?, czy obowiązuje zawsze, czy tylko przy spełnieniu określonych warunków (jakich)?.
4. Kroki postępowania z przypisaniem odpowiedzialności:
    - wskazanie ról zaangażowanych w realizację procedury (np. kierownik zespołu, specjalista ds. komunikacji),
    - kroki postępowania (czynności operacyjne) – lista lub krótki opis (jeśli nazwa czynności nie jest zrozumiała sama przez się) w kolejności logicznej, w tym wyjątki/alternatywne ścieżki (jeśli występują),
    - przypisanie odpowiedzialności zgodnie z macierzą RASCI[20], np.

[20] R – Responsible (wykonuje), A – Accountable (odpowiedzialny), S – Support (wspiera), C – Consulted (konsultowany), I – Informed (informowany).

Tabela 6. Macierz RASCI przypisująca odpowiedzialność członkom zespołu

Nr	Czynność operacyjna	R	A	S	C	I
1	Odbiór zgłoszenia o incydencie od podmiotu constituency	Analityk cyberbezpieczeństwa	Kierownik CSIRT	—	—	—
2	Kwalifikacja incydentu	Analityk cyberbezpieczeństwa	Kierownik CSIRT	—	Dział prawny	—
3	Powiadomienie właściwego CSIRT-u poziomu krajowego	Analityk cyberbezpieczeństwa	—	Specjalista ds. komunikacji	—	Kierownik CSIRT
4	Zamknięcie, archiwizacja zgłoszenia i aktualizacja rejestru	—	—	—	—	Analityk cyberbezpieczeństwa

W przypadku złożonych procedur rekomendujemy również przygotowanie diagramów, np. w notacji BPMN.

5. Wejścia i wyjścia (Input/Output):
   - wejścia: jakie informacje, dane, zgłoszenia muszą być dostępne, by rozpocząć procedurę,
   - wyjścia: co powstaje w wyniku jej wykonania (np. raport, alert, powiadomienie, metryka).
6. Wymagane zasoby – sprzęt, oprogramowanie, dostęp do systemów, konta, klucze, dokumentacja – wszystko, co jest niezbędne do wykonania procedury. Może to być oddzielna lista lub w opisie czynności operacyjnych można użyć nazw konkretnych zasobów.
7. Powiązania i zależności:
   - inne procedury operacyjne w ramach procesu, które są wywoływane lub kontynuowane,
   - powiązania z procesami organizacyjnymi, np. konsultacja z działem prawnym.
8. Wymogi czasowe i jakościowe (opcjonalnie):
   - jeśli dla tej procedury obowiązują konkretne SLA, należy je wskazać, np. *przekazanie ostrzeżenia, zgłoszenia lub sprawozdań do CSIRT NASK musi nastąpić w ciągu 8 godzin od otrzymania zgłoszenia*,

- jeśli dla danej czynności operacyjnej istnieją ograniczenia czasowe, również należy je wskazać, np. czas oczekiwania na odpowiedź innego działu lub czas wykonywania czynności analitycznych.

9. Wersjonowanie i zatwierdzenie:
   - data zatwierdzenia, numer wersji, właściciel procedury,
   - podpis kierownika zespołu CSIRT lub innego zatwierdzającego (dla procedur operacyjnych na poziomie dojrzałości 3).
10. Załączniki (opcjonalnie) – wzory dokumentów, formularzy, checklisty (jeśli są używane lub wymagane do osiągnięcia wyniku procedury).

Eskalacja na poziom zarządzania (P-1)

Wartość parametru dla dojrzałości zespołu na poziomie Basic: 3.

Zespół CSIRT powinien dysponować jasno określonym i udokumentowanym procesem eskalacji incydentów do wyższych poziomów zarządzania – zarówno w ramach własnej organizacji, jak i w przypadku *constituency* (np. kierownictwo operatorów usług kluczowych). Proces ten powinien umożliwiać szybką i bezpośrednią komunikację z decydentami w sytuacjach, które mogą skutkować poważnym naruszeniem ciągłości działania, znacznymi stratami reputacyjnymi lub sytuacją kryzysową. Eskalacja incydentów do kierownictwa wyższego szczebla jest kluczowa dla alokacji odpowiednich zasobów i podejmowania strategicznych decyzji. Brak takiego procesu grozi opóźnieniami w reakcji na krytyczne zagrożenia i pogłębieniem się kryzysu.

Eskalacja powinna opierać się na ustalonej klasyfikacji incydentów (zob. parametr O-8), w szczególności na ich wpływie i pilności. W procesie należy wskazać nie tylko poziomy eskalacji i progi uruchamiające działania, lecz także sposób realizacji – z uwzględnieniem sytuacji, w których standardowe punkty kontaktowe nie są dostępne lub nie reagują w odpowiednim czasie. Choć formalne wymagania ENISA nie narzucają gotowości do całodobowej eskalacji, należy mieć na uwadze, że może być ona konieczna także poza standardowymi godzinami pracy. Dlatego proces eskalacji powinien być zaprojektowany tak, aby umożliwić szybkie i bezpośrednie poinformowanie odpowiednich decydentów o incydentach o wysokiej pilności i wpływie, niezależnie od pory dnia. Kluczowe dla tego procesu jest by łańcuch eskalacyjny był możliwie najkrótszy oraz uwzględniał wcześniej przygotowane mechanizmy powiadamiania (uzgodnione środki i kanały przekazywania informacji czy nawet słowa kodowe) tak, aby gdy wymaga tego sytuacja, zespół CSIRT mógł skutecznie inicjować działania na poziomie strategicznym.

W celu osiągnięcia poziomu dojrzałości 3 dla tego parametru proces, poza udokumentowaniem, powinien być też zatwierdzony przez co najmniej kierownika CSIRT-u.

Eskalacja do zespołu prasowego[21] (P-2)

Wartość parametru dla dojrzałości zespołu na poziomie Basic: 2.

Bezpośrednia lub pośrednia interakcja z mediami również będzie elementem pracy zespołu CSIRT. Zespół powinien mieć zdolność do obsługi zapytań prasowych, zwłaszcza w trakcie incydentu. Najlepszym sposobem osiągnięcia tej zdolności byłoby wyznaczenie osoby pełniącej funkcję rzecznika prasowego zespołu lub osoby/osób upoważnionych do kontaktu z dziennikarzami. Na początkowym etapie funkcjonowania CSIRT-u rekomendujemy jednak, aby główną rolę w kontaktach z mediami odgrywała jednostka organizacji odpowiedzialna za kontakt z mediami (zespołu prasowego). Dlatego zespół cyberbezpieczeństwa powinien opracować i wdrożyć wewnętrzny proces umożliwiający sprawne przekazanie informacji o incydencie lub zagrożeniu do tej jednostki. Dotyczy to zwłaszcza sytuacji, w których zdarzenie może potencjalnie wpłynąć na reputację podmiotów constituency lub wymaga ono pilnego komunikatu prasowego z uwagi na potencjalnie duże, negatywne skutki. Kluczowe jest przy tym, aby zespół prasowy organizacji miał przynajmniej podstawową wiedzę na temat cyberbezpieczeństwa oraz aby rozumiał specyfikę incydentów obsługiwanych przez CSIRT. Dobrym rozwiązaniem może być wyznaczenie jednej osoby w zespole prasowym jako punktu kontaktowego do spraw CSIRT – z zapewnieniem jej dodatkowych szkoleń, bieżącej komunikacji z zespołem (w tym również mniej sformalizowanymi kanałami) oraz udziału w ćwiczeniach.

Proces eskalacji powinien określać:

- kto i w jakich sytuacjach inicjuje kontakt z zespołem prasowym;
- zakres przekazywanych informacji i sposób ich uzgadniania (np. notatka sytuacyjna, briefing techniczny);
- tryb eskalacji poza godzinami pracy (jeśli konieczne);
- sposób współpracy w przygotowywaniu komunikatów publicznych (przygotowywaniu i zatwierdzaniu treści).

Proces eskalacji do zespołu prasowego, obejmujący m.in. zasady roboczej współpracy z zespołem prasowym, powinien zostać co najmniej wewnętrznie udokumentowany i stosowany.

[21] Parametr ten koresponduje bezpośrednio z parametrem O-6.

Eskalacja do działu prawnego (P-3)

Wartość parametru dla dojrzałości zespołu na poziomie Basic: 2.

Zespół CSIRT powinien mieć możliwość szybkiego i bezpośredniego skonsultowania się z przedstawicielami działu prawnego organizacji – zwłaszcza w sytuacjach, gdy incydent lub zagrożenie może wywołać potencjalnie istotne skutki prawne, wiąże się z wątpliwościami interpretacyjnymi lub wymaga odpowiedzi na formalne wnioski organów ścigania.

Proces eskalacji do zespołu prasowego, umożliwiający skorzystanie ze wsparcia działu prawnego powinien zostać co najmniej wewnętrznie udokumentowany i stosowany.

W związku z tym zalecamy, aby w opisie procesu:

- wskazać konkretne sytuacje, w których konsultacja z prawnikiem jest obowiązkowa, np. odpowiedź na wniosek organu ścigania lub współpraca z organami ściągania np. przy zabezpieczeniu danych jako potencjalnych dowodów, przygotowanie zawiadomienia o podejrzeniu popełnienia przestępstwa czy opracowanie treści oficjalnych komunikatów związanych z incydentem od strony prawnej,
- ustalić zasady konsultacji przez dział prawny dokumentów wychodzących z CSIRT-u (np. odpowiedzi na pisma lub formalne powiadomienia dla podmiotów constituency),
- wskazać tryb postępowania poza godzinami pracy, np. listę kontaktową osób dyżurujących lub mechanizm eskalacji w trybie pilnym.

Na początkowym etapie funkcjonowania CSIRT-u rekomendujemy, aby zespół utrzymywał bieżącą współpracę z wyznaczonym prawnikiem organizacji, który będzie pełnił funkcję „punktu kontaktowego ds. CSIRT". Podobnie jak w przypadku współpracy z zespołem prasowym należy uwzględnić potrzebę podnoszenia jego świadomości w zakresie specyfiki cyberbezpieczeństwa i możliwych scenariuszy, w które byłby zaangażowany dział prawny. Dobrą praktyką jest również organizowanie wspólnych spotkań lub szkoleń zespołu CSIRT i działu prawnego, aby dzielić się doświadczeniami i budować wzajemne zrozumienie.

Procesy: zapobiegania incydentom (P-4), wykrywania incydentów (P-5), rozwiązywania incydentów (P-6), szczególnych incydentów (P-7)

Wartość parametru dla dojrzałości zespołu na poziomie Basic: 2.

Zespół CSIRT powinien stworzyć zestaw procesów operacyjnych opisujących działania podejmowane na różnych etapach cyklu życia incydentu – od zapobiegania, przez wykrycie, aż po rozwiązanie i obsługę szczególnych przypadków. Procesy te muszą być ściśle powiązane z katalogiem świadczonych usług (patrz parametr O-5), kompetencjami personelu (zob. parametry H) oraz wykorzystywanymi narzędziami (zob. parametry T-2, T-8, T-9 i T-10).

W praktyce możliwe – i często uzasadnione – jest łączenie niektórych procesów, np. wykrywania i rozwiązywania incydentów (P-5 i P-6) w ramach jednego zintegrowanego procesu obsługi incydentu. Kluczowe jest jednak to, aby wszystkie istotne elementy zostały odpowiednio opisane i przypisane do właściwych ról oraz narzędzi.

Proces zapobiegania incydentom (P-4) powinien obejmować działania proaktywne, takie jak przygotowywanie i dystrybucja biuletynów ostrzegawczych, informowanie o podatnościach i dostępnych poprawkach, udostępnianie zaleceń oraz działania edukacyjne wspierające świadomość zagrożeń wśród podmiotów constituency.

Proces wykrywania incydentów (P-5) opisuje, jak zespół identyfikuje potencjalne zdarzenia, zarówno na podstawie własnych źródeł, jak i zgłoszeń od podmiotów constituency. Proces powinien obejmować zasady triażu[22] (ang. *triage*) oraz weryfikacji wiarygodności i krytyczności informacji.

[22] Triaż to termin wywodzący się z medycyny i oznaczający praktykę stosowaną w sytuacjach, gdy przy ograniczonych zasobach istnieje konieczność „kolejkowania" pacjentów, tzn. zapewnienia im opieki kolejno według krytyczności ich stanu. W przypadku incydentów cyberbezpieczeństwa jest to wstępna ocena zgłoszenia incydentu, mająca na celu określenie jego charakteru, krytyczności i pilności obsługi. Proces ten opiera się zwykle na przyjętym systemie klasyfikacji incydentów (zob. parametr O-8) i pozwala zespołowi CSIRT na skuteczne zarządzanie zgłoszeniami oraz priorytetyzację działań.

Tabela 7. Przykładowa tabela triażu

Priorytet obsługi	Opis wpływu incydentu
1 – incydent wymaga podjęcia natychmiastowych działań	**Krytyczny** – natychmiastowy, bardzo poważny wpływ na funkcjonowanie podmiotu/podmiotów constituency
2 – działania powinny być podjęte w krótkim czasie	**Wysoki** – poważny wpływ na funkcjonowanie podmiotu/podmiotów constituency
3 – obsługa w ramach zwykłego cyklu reagowania	**Średni** – umiarkowany wpływ na funkcjonowanie podmiotu/podmiotów constituency
4 – nie wymaga pilnej reakcji (zostanie obsłużony w dogodnym czasie)	**Niski** – niewielki wpływ lub brak wpływu na funkcjonowanie podmiotu/podmiotów constituency

Proces rozwiązywania incydentów (P-6) określa sposób reagowania, analizy technicznej, komunikacji z podmiotami, wdrażania działań naprawczych i zamykania incydentów. Istotnym elementem tego procesu jest gromadzenie doświadczeń (lessons learned).

Procesy szczególnych incydentów (P-7) dotyczą specyficznych kategorii zagrożeń, które ze względu na swoją powszechność, wpływ na podmioty constituency lub wymagany sposób obsługi zasługują na odrębne, bardziej szczegółowe lub standaryzowane traktowanie. Rekomendujemy identyfikację takich incydentów w kontekście typowego profilu zagrożeń dla podmiotów constituency oraz opracowanie szczegółowych procedur postępowania.

Wszystkie wymienione procesy powinny być spisane w formie operacyjnych procedur, dostępnych dla członków zespołu i powiązane z systemem szkoleń (H-4 do H-6). Na poziomie dojrzałości Basic wymagany jest co najmniej ich wewnętrzny opis – niekoniecznie formalnie zatwierdzony, ale ustalony i znany zespołowi. Warto jednak dążyć do ich zatwierdzenia przez kierownictwo oraz do okresowej aktualizacji.

Audyt i zbieranie informacji zwrotnej (P-8)

Wartość parametru dla dojrzałości zespołu na poziomie Basic: 3.

Wszystkie zespoły CSIRT potrzebują zapewnienia jakości w krytycznych i wrażliwych aspektach swojej działalności. CSIRT powinien posiadać udokumentowany i zatwierdzony, co najmniej przez kierownictwo zespołu, proces audytu i informacji zwrotnej, który umożliwia systematyczną ocenę skuteczności działań zespołu oraz identyfikację obszarów wymagających poprawy. Proces ten może obejmować zarówno samoo-

cenę zespołu, jak i – tam, gdzie to uzasadnione – okresowe audyty/przeglądy realizowane przez kierownictwo zespołu lub wewnętrzne komórki audytu. Zakres audytów i poziom ich formalizacji powinny być dostosowane do aktualnych potrzeb, skali działania zespołu oraz poziomu dojrzałości. Najważniejsze jest, aby wyniki tych audytów/przeglądów były wykorzystywane jako źródło informacji wspierających doskonalenie usług i wewnętrznych procedur operacyjnych.

Rekomendujemy podnadto zapewnienie regularnego zbierania informacji zwrotnej zarówno od członków zespołu CSIRT, jak i od podmiotów znajdujących się w *constituency* – np. za pomocą krótkich ankiet ewaluacyjnych lub podczas cyklicznych spotkań.

Alarmowy kontakt z zespołem (P-9)

Wartość parametru dla dojrzałości zespołu na poziomie Basic: 2.

Zespół CSIRT powinien zapewniać możliwość nawiązania szybkiego i skutecznego kontaktu w sytuacjach wymagających natychmiastowej reakcji również poza standardowymi godzinami pracy zespołu (oczywiście dostępność alarmowa w trybie pracy 24/7 jest zapewniona z definicji). Taką sytuacją może być np. gwałtowna, niekorzystna zmiana statusu incydentu (eskalacja) lub informacja o incydencie dotykającym wiele podmiotów.

Zespół powinien przygotować dokument z opisem procesu alarmowego kontaktu, zawierający:

- listę numerów telefonów, adresów e-mail i/lub innych kanałów kontaktu wykorzystywanych w trybie alarmowym,
- wskazanie, komu i na jakich zasadach dostępne są dane kontaktowe (np. tylko CSIRT-y krajowe lub sektorowe, wybrani przedstawiciele podmiotów z *constituency*).

W pozostałych przypadkach należy zapewnić, aby formularz do zgłaszania incydentów (zob. również parametr T-9) był nieprzerwanie dostępny i zgodnie z UoKSC zapewniał możliwość przekazania zgłoszenia w wymaganym czasie. Warto zwrócić uwagę na fakt, że wymagania czasowe dotyczące dostępności formularza lub zespołu mogą wynikać z ustaleń zawartych w umowach (SLA) lub z wewnętrznych procesów organizacyjnych, które określają dopuszczalny czas reakcji na zgłoszenie oraz sposób i termin udzielania wsparcia. Zespół CSIRT powinien zatem przewidzieć w swoim modelu operacyjnym, w jaki sposób spełni te wymagania, w szczególności

w kontekście godzin swojej dostępności. Zalecamy także, aby proces alarmowego kontaktu zawierał mechanizmy zapobiegające jego ewentualnemu nadużywaniu – reagowanie poza godzinami pracy powinno być zarezerwowane wyłącznie dla rzeczywistych sytuacji wymagających niezwłocznej interwencji.

Obecność w internecie (P-10)

Wartość parametru dla dojrzałości zespołu na poziomie Basic: 2

Internet jest podstawowym kanałem komunikacji w kontekście obsługi incydentów i budowania zaufania ze strony podmiotów znajdujących się w *constituency*. Dlatego zespół CSIRT powinien posiadać udokumentowane zasady obecności w internecie, obejmujące trzy główne obszary: obsługę standardowych aliasów e-mail, stronę internetową oraz obecność w mediach społecznościowych.

Zgodnie ze standardami i dobrymi praktykami CSIRT powinien zapewnić obsługę standardowych adresów e-mail, takich jak: security@[domena], abuse@[domena] oraz cert@[domena], które służą do zgłaszania incydentów i nadużyć oraz do kontaktu ogólnego w sprawach bezpieczeństwa. Powinny one być skonfigurowane w sposób umożliwiający szybkie przekazanie wiadomości do zespołu CSIRT. Zgłoszenia wysłane na te adresy nie mogą pozostawać bez odpowiedzi.

Rekomendujemy, by CSIRT miał własną stronę internetową lub dedykowaną sekcję na stronie organizacji macierzystej. Powinna ona w jasny i przejrzysty sposób przedstawiać mandat zespołu (zob. parametr O-1), zakres świadczonych usług (zob. parametr O-5), uproszczony opis *constituency* (zob. parametr O-2), a także przejrzyste instrukcje kontaktu, w tym godziny pracy, metody zgłaszania incydentów oraz kontaktowe adresy e-mail. Rekomendujemy, aby wszystkie powyższe informacje zebrać i opublikować na stronie internetowej zespołu w formacie zgodnym z RFC 2350. Dodatkowo strona powinna spełniać wymagania ustawy z dnia 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych oraz zawierać klauzulę informacyjną dotyczącą przetwarzania danych osobowych zgodnie z RODO.

Obecność w mediach społecznościowych (np. LinkedIn, X, Facebook) nie jest obligatoryjna, jednak jej zasadność powinna zostać świadomie oceniona przez zespół. W przypadku prowadzenia takich kanałów należy określić zasady publikacji treści, ich zakres oraz odpowiedzialność (zob. również parametry O-6 i P-2). Warto również zdecydować, czy CSIRT sam prowadzi profil, czy robi to zespół prasowy organizacji i zapewnić odpowiednią koordynację.

Zasady obecności zespołu CSIRT w internecie powinny być udokumentowane i dostępne dla członków zespołu. Dobrą praktyką jest zatwierdzenie tych zasad przez kierownictwo organizacji.

Bezpieczne przetwarzanie informacji (P-11)

Wartość parametru dla dojrzałości zespołu na poziomie Basic: 2.

W swojej codziennej pracy, a w szczególności w trakcie obsługi incydentów zespół CSIRT przetwarza informacje wrażliwe. Informacje te mogą pochodzić zarówno od podmiotów znajdujących się w jego *constituency*, jak i od partnerów zewnętrznych. Mogą to być dane osobowe, poświadczenia (w tym dane uwierzytelniające), informacje o podatnościach czy techniczne szczegóły dotyczące incydentów. W niektórych przypadkach ujawnienie lub przedwczesne opublikowanie tych informacji (np. zanim zostaną wdrożone działania naprawcze) może zwiększyć poziom zagrożenia lub pogłębić skutki incydentu. Dlatego zespół cyberbezpieczeństwa musi posiadać proces (lub szczegółowe zasady postępowania) zapewniający poufność, integralność i dostępność przetwarzanych informacji, zwłaszcza tych dotyczących obsługi incydentów. Dobre praktyki obejmują zabezpieczenie zarówno kanałów komunikacji (np. szyfrowana poczta, VPN), jak i systemów wykorzystywanych do przetwarzania informacji (np. hostowane lokalnie systemy ticketowe – por. parametr T-4). Dostęp do informacji wrażliwych powinien być ograniczony wyłącznie do uprawnionych osób, a członkowie zespołu muszą być świadomi, które dane podlegają szczególnej ochronie i jakie środki techniczne i organizacyjne należy w tym celu zastosować (np. maskowanie haseł, ograniczenia kopiowania, kontrola dostępu). Proces powinien również uwzględniać wymagania prawne, w szczególności dotyczące ochrony danych osobowych oraz zasady dalszego udostępniania informacji – zespół powinien wiedzieć, które informacje mogą być przekazywane dalej (np. do organów ścigania, innych operatorów usług kluczowych, innych CSIRT-ów), a które muszą pozostać wyłącznie do użytku wewnętrznego. Zespół musi znać i stosować protokół TLP (Traffic Light Protocol), który reguluje zasady dalszego udostępniania informacji zależnie od ich oznaczenia. Polskie tłumaczenie oznaczeń TLP jest dostępne pod adresem https://cert.pl/tlp.

Do osiągnięcia poziomu 2. wymagane jest, aby zasady bezpiecznej obsługi informacji były wewnętrznie spisane i znane wszystkim członkom zespołu. Dobrą praktyką jest również ich formalne zatwierdzenie przez kierownictwo zespołu lub organizacji, przy czym niezbędne jest, by opisywany proces korespondował lub najlepiej był częścią składową polityki, o której mowa w parametrze O-10.

Zarządzanie źródłami informacji (P-12)

Wartość parametru dla dojrzałości zespołu na poziomie Basic: 2.

Zespół CSIRT musi posiadać proces pozwalający na skuteczne zarządzanie źródłami informacji o zagrożeniach w cyberprzestrzeni. Celem tego procesu jest zapewnienie zespołowi dostępu do aktualnych, wiarygodnych i adekwatnych danych, niezbędnych do wykrywania potencjalnych zagrożeń, reagowania na nie oraz prowadzenia działań prewencyjnych.

Zarządzanie źródłami informacji powinno obejmować cały ich cykl życia – od identyfikacji i oceny wiarygodności, poprzez włączenie do środowiska operacyjnego (np. integrację z systemami ticketowymi, analitycznymi lub platformami *threat intelligence*, jeśli są wykorzystywane), bieżący monitoring jakości i aktualności dostarczanych informacji, aż po decyzję o ich usunięciu, gdy przestaną spełniać kryteria przydatności. W kontekście procesu zarządzania źródłami informacji należy mieć świadomość ryzyka wynikającego z działań opartych na niesprawdzonych lub zmanipulowanych danych, dlatego na początkowym etapie rekomendujemy korzystanie z oficjalnych lub sprawdzonych źródeł (por. parametr T-2). Istotne jest również zwracanie uwagi na częstość aktualizacji oraz zgodność informacji z profilem działalności zespołu (charakterystyką constituency oraz katalogiem świadczonych usług), tak by dane zbierane i przekazywane podmiotom w constituency miały możliwie największą wartość operacyjną.

Do osiągnięcia poziomu 2. wymagane jest, aby proces zarządzana źródłami informacji był wewnętrznie udokumentowany i znany wszystkim członkom zespołu. W związku z tym rekomendujemy, by zespół posiadał udokumentowane:

- listę aktywnie wykorzystywanych źródeł informacji (zob. parametr T-2 i **załącznik nr 3**),
- zasady włączania nowych źródeł, w tym uproszczone np. dla źródeł rekomendowanych przez zaufane podmioty branżowe lub partnerskie,
- podstawowe kryteria oceny wiarygodności i aktualności informacji (np. częstotliwość publikacji i aktualizacji, zgodność z profilem działalności, reputacja dostawcy informacji, ekspercka ocena przydatności).

Komunikacja z podmiotami constituency (P-13)

Wartość parametru dla dojrzałości zespołu na poziomie Basic: 2.

Zespół CSIRT powinien aktywnie docierać do swojego *constituency* nie tylko w kontekście obsługi incydentów, lecz także poprzez działania zwiększające widoczność zespołu, budujące świadomość zagrożeń oraz promujące dobre praktyki w zakresie cyberbezpieczeństwa. Obejmuje to działania takie jak prowadzenie kampanii informacyjnych, organizowanie szkoleń, warsztatów, publikowanie raportów, poradników czy ostrzeżeń dotyczących aktualnych zagrożeń, a także udział w konferencjach branżowych i współpraca z mediami. Dobór form komunikacji powinien być dostosowany do charakterystyki constituency (w szczególności liczby i dojrzałości podmiotów). W przypadku większych grup odbiorców mogą dominować media społecznościowe i platformy e-learningowe, natomiast w mniejszym constituency skuteczniejsza może być bezpośrednia komunikacja (np. e-mail). Istotnym elementem procesu jest zapewnienie dwukierunkowości kontaktu – zespół CSIRT powinien umożliwiać członkom *constituency* przekazywanie informacji zwrotnych, uwag i sugestii (zob. parametr P-8). Taka interakcja nie tylko wspiera rozwój zespołu, lecz także ułatwia identyfikację potrzeb i oczekiwań constituency. Proces P-13 jest przykładem miękkiego oddziaływania, ale wbrew pozorom jest równie ważny jak procesy ściśle operacyjne, gdyż katalizuje i ułatwia proaktywne postawy wśród podmiotów *constituency* oraz sprzyja budowaniu relacji zaufania, co jest niezbędne w trakcie reagowania na incydenty poważne. Zespół CSIRT powinien być tego świadomy i faktycznie podejmować takie inicjatywy.

Zasady planowania i podejmowania inicjatyw zewnętrznych, w których uczestniczy zespół cyberbezpieczeństwa, powinny być wewnętrznie udokumentowane.

Raportowanie do organu nadzorującego (P-14)

Wartość parametru dla dojrzałości zespołu na poziomie Basic: 3.

Regularne przekazywanie kierownictwu organizacji kluczowych informacji o działalności zespołu CSIRT, obsługiwanych incydentach, zagrożeniach oraz o stanie bezpieczeństwa constituency wspiera podejmowanie strategicznych decyzji, alokację zasobów oraz zapewnia zgodność z przepisami i wytycznymi krajowymi lub sektorowymi. Raporty mogą mieć formę okresowych zestawień (np. kwartalnych lub rocznych) dotyczących liczby i rodzaju obsłużonych incydentów, czasu reakcji, trendów zagrożeń czy wytycznych dotyczących poprawy bezpieczeństwa. Rekomendujemy wcześniej-

sze ustalenie formatu i częstotliwość raportów wspólnie z zarządem organizacji. Pozwoli to na dopasowanie raportów do potrzeb decyzyjnych oraz zmniejszy ryzyko nieadekwatnych lub nieczytelnych treści. Kierownictwo organizacji powinno mieć możliwość przekazania uwag, a zespół CSIRT powinien uwzględniać je w dalszej działalności. Poza danymi statystycznymi rekomendujemy uwzględnienie w raportach także kontekstu i interpretacji przedstawionych danych oraz potencjalnych przeszkód utrudniających działanie. Warto także opisać potrzeby zespołu (np. w zakresie zasobów, współpracy, kompetencji). Ponadto, biorąc pod uwagę odbiorców raportu, rekomendujemy wykorzystanie w szerszym zakresie wykresów, tabel i infografik tak, aby ułatwić odbiór i skrócić czas niezbędny do analizy materiału.

Proces raportowania musi być udokumentowany i zatwierdzony przez kierownictwo zespołu.

Raportowanie do *constituency* (P-15)

Wartość parametru dla dojrzałości zespołu na poziomie Basic: 2.

Regularne przekazywanie do *constituency* informacji o działalności zespołu, w szczególności statystyk dotyczących incydentów bezpieczeństwa, ma na celu budowanie transparentności, wzmacnianie zaufania oraz podnoszenie świadomości na temat aktualnych zagrożeń oraz skuteczności działań zespołu. Zespół CSIRT powinien prowadzić ewidencję incydentów i okresowo raportować określonym grupom odbiorców (np. operatorom usług kluczowych lub całej społeczności constituency) informacje statystyczne. Warto zawczasu ustalić strukturę raportu i zakres publikowanych danych. Raporty mogą obejmować m.in. liczbę obsłużonych incydentów, ich klasyfikację zgodnie z przyjętą taksonomią (por. parametr O-8), źródła zgłoszeń czy średni czas reakcji. Aby zapewnić spójność i efektywność procesu raportowania, rekomendujemy gromadzenie danych statystycznych w sposób możliwie zautomatyzowany, przy użyciu narzędzi opisanych w parametrach T-4, T-5, T-10. W opinii CERT Polska samo przedstawienie statystyk jest niewystarczające. Warto uwzględnić komentarz analityczny i praktyczne rekomendacje. Udokumentowane zasady powinny precyzować, które dane są zbierane, jak są przetwarzane oraz w jaki sposób, z jaką częstotliwością i komu (którym odbiorcom) są udostępniane.

Spotkania wewnętrzne (P-16)

Wartość parametru dla dojrzałości zespołu na poziomie Basic: 2.

Odbywające się cyklicznie spotkania zespołu CSIRT wspierają wewnętrzną komunikację, pozwalają na bieżąco omawiać incydenty, planować działania oraz usprawniać współpracę operacyjną. Ich celem jest również identyfikowanie problemów i wyciąganie wniosków z dotychczasowych działań, a także budowanie spójności zespołu, zwłaszcza w przypadku pracy rozproszonej lub hybrydowej.

Proces spotkań wewnętrznych powinien uwzględniać ich częstotliwość, skład uczestników, zakres omawianych tematów oraz sposób dokumentowania ustaleń i przekazywania ich zespołowi. Nawet przy niewielkich zespołach takie spotkania stanowią podstawowy element dobrej koordynacji. Mogą się one odbywać w trybie stacjonarnym, zdalnym lub hybrydowym, ważne, by dostosować ich formę i częstotliwość do potrzeb operacyjnych oraz dostępności członków zespołu. Zalecamy, aby spotkania odbywały się przynajmniej raz w tygodniu, a w sytuacjach wymagających intensywnej współpracy – częściej. W praktyce do osiągnięcia poziomu dojrzałości 2 wystarczające jest zaplanowanie cyklicznego spotkania całego zespołu w grupowym kalendarzu (np. raz w tygodniu), z predefiniowaną agendą obejmującą m.in. przegląd incydentów, postępy w działaniach operacyjnych, sprawy organizacyjne (np. potrzeby w zakresie szkoleń lub narzędzi) i wnioski z ostatnich działań. Wystarczy również, by ustalenia były notowane w formie krótkiego podsumowania udostępnianego wszystkim członkom zespołu.

Współpraca z zespołami partnerskimi (P-17)

Wartość parametru dla dojrzałości zespołu na poziomie Basic: 2.

Efektywna współpraca z innymi zespołami bezpieczeństwa (tzw. zespołami partnerskimi, ang. *peer teams*) to fundament skutecznego działania CSIRT-u, zwłaszcza w kontekście szybkiego reagowania na incydenty, wymiany wiedzy operacyjnej oraz wzmacniania praktycznej współpracy między zespołami. Partnerami mogą być inne CSIRT-y, CSIRT-y poziomu krajowego i sektorowe, ale także zespoły SOC dużych organizacji czy centra ISAC. Relacje takie mogą być zarówno formalnie określone, np. poprzez przynależność do zrzeszeń zespołów CSIRT (jak TF-CSIRT, FIRST), uzgodnienia typu MoU, jak i nieformalne, np. oparte na zaufaniu i wieloletniej współpracy. Budowanie efektywnych relacji roboczych zwiększa skuteczność działań zespołu, umożliwia szybsze reagowanie na nowe zagrożenia oraz wspiera rozwój kompetencji członków CSIRT.

Do osiągnięcia poziomu 2. niezbędne jest, aby zespół CSIRT udokumentował, do jakich zespołów partnerskich lub zrzeszeń należy wraz z ich krótkim opisem. Powinien także spisać zasady współpracy, obejmujące np. określenie kanałów kontaktu, reguł udostępniania informacji (jakie informacje mogą być wymieniane, na jakich warunkach i w jakim kontekście, w tym z użyciem oznaczeń TLP), lub wskazać zasady, którymi posługują się zrzeszenia. Dobrze byłoby, gdyby te zasady zostały zaakceptowane i przyjęte przez zarząd organizacji.

Spis rysunków

Spis tabel

Załączniki

Załącznik 1. Przykładowy opis usługi

Przykład opisu usługi „Analiza artefaktów i dowodów cyfrowych” (usługa 6.3 z katalogu FIRST „CSIRT Services Framework” – Artifact and forensic evidence analysis).

Element	Opis
Nazwa usługi	Analiza artefaktów i dowodów cyfrowych
Cel usługi	Wsparcie podmiotów kluczowych i ważnych w identyfikacji przyczyn, metod działania i skutków incydentów bezpieczeństwa poprzez badanie dostarczonych/zebranych artefaktów oraz dowodów cyfrowych
Opis funkcji (zakres)	Usługa obejmuje: analizę nośników i plików (media/surface analysis) oraz analizę dynamiczną i analizę porównawczą
Rezultat	Raport zawierający wyniki analizy, wnioski dotyczące mechanizmu działania zagrożenia oraz rekomendacje do dalszych działań operacyjnych lub strategicznych
Zakres odbiorców	Podmioty w constituency, organizacja, inne CSIRT-y – zgodnie z mandatem i ustaleniami współpracy
Dostępność czasowa	Standardowo w godzinach pracy CSIRT-u; w przypadku incydentów poważnych – dostępność rozszerzona (dyżury/analityk on-call)
Sposób zgłoszenia/uruchomienia	Poprzez zgłoszenie incydentu zawierające artefakty lub przekazanie ich ustalonym kanałem (system zgłoszeniowy, formularz, bezpieczny transfer)
Ograniczenia	Usługa nie obejmuje inżynierii wstecznej (reverse engineering), analizy fizycznych nośników (np. dysków) ani świadczenia opinii biegłych. Zespół nie realizuje analiz w trybie natychmiastowym (real-time)
Uwagi dodatkowe	Usługa może być zintegrowana z procesem lessons learned lub wykorzystywana do budowania świadomości sytuacyjnej w constituency

Załącznik 2. Przykładowa architektura i wymagania dla środowiska wewnętrznego CSIRT

Element	Charakter dostępu	VLAN	Minimalne, rekomendowane parametry urządzeń	Uwagi
Serwer pocztowy	Public	VLAN1	Specyfikacja zgodna z rekomendowaną przez dostawcę dla wybranego rozwiązania.	Dostęp publiczny dla innych serwerów pocztowych, dostęp administracyjny (MGMT) z VLAN4; brak filtrowania na aliasach do np. systemu ticketowego.
Wirtualizacja	Internal admin	VLAN2	Min. 3 hosty, 64/128GB na host; procesor serwerowy klasy Xeon lub równoważny, min. 16 rdzeni, taktowanie bazowe ≥ 2.0 GHz, wsparcie dla DDR5 CPU; 2 CPU na host; Uplinki min. 10 Gb/s.	Dostęp MGMT; zasoby storage podłączone do sieci maszyn wirtualnych za pośrednictwem przełącznika skonfigurowanego w trybie dostępowym (access) i przypisanych do odpowiednich VLAN-ów.
Firewall	Internal admin	VLAN3	Sieć dostępowa dla serwerów powinna zapewniać przepustowość na poziomie co najmniej 10 Gb/s; firewall powinien składać się z dwóch urządzeń pracujących w trybie klastra wysokiej dostępności (HA), z możliwością synchronizacji sesji i konfiguracji pomiędzy węzłami.	Dostęp MGMT przez VLAN3; pozostałe VLAN-y wpięte do infrastruktury routującej; połączenie z resztą środowiska zabezpieczone za pomocą IPsec.
Przełącznik access	Internal admin	VLAN4	2 przełączniki w konfiguracji HA (np. stacking lub MLAG), z redundantnym zasilaniem i uplinkami 10Gb/s; min. 30 portów.	
Przełącznik mgmt	Internal admin	VLAN4	1Gb/s na port, min 24 porty; 2 przełączniki w HA (np. stacking lub MLAG), z redundantnym zasilaniem i uplinkami 10Gb/s.	
VM / system ticketowy	Internal	VLAN5	CPU: minimm 4vcpu RAM: minimum 8GB Storage: minimum 70GB storage na bazę i załączniki (w zależności od liczby oraz charakteru zgłoszeń, należy przewidzieć stopniowy wzrost wolumenu danych).	Dostęp do interfejsu użytkownika (UI) dla pracowników; połączenie z serwerem pocztowym (odbiór/zapis zgłoszeń); dostęp administracyjny za pomocą SSH.
„Brudny" internet	Internal	VLAN6	Mobilny dostęp do internetu z dynamicznie przydzielanym adresem IP (np. LTE/5G) – prędkość transmisji (pobierania/wysyłania) dostosowana do potrzeb zespołu i oferty dostawców.	Dostęp głównie dla systemów automatycznych, ale również dla członków zespołu CSIRT, np. w celu ręcznej analizy potencjalnych incydentów bezpieczeństwa.

VM/formularz zgłaszania incydentów	Public	VLAN7	–	Dostęp do API RT.
Storage VM	Internal admin	VLAN8 (alternatywnie w VLAN2)	Min. 3TB SSD; połączenie z macierzą zależne od posiadanych kompetencji lub infrastruktury: - FibreChannel wymaga dedykowanych kart sieciowych i przełączników - ISCSI możliwa jest komunikacja za pomocą istniejących kart sieciowych (SFP+ 10G i wyżej) i przełączników (przepustowość interfejsów min. 10 Gb/s).	Dostęp MGMT powinien być realizowany poprzez dedykowany VLAN (np. VLAN 2), z zapewnieniem możliwości połączenia z warstwą wirtualizacji.
NDR (lub inne systemy bezpieczeństwa)	Internal admin	VLAN9	Min. 10 Gb/s.	Dostęp MGMT dla administratorów; span port z przełączników.
Opcjonalnie (w zależności od świadczonych przez CSIRT usług (zob. Parametr O-5)				
Zarządzanie kontenerami	Internal	VLAN10	Specyfikacja node'ów zgodna z zaleceniami producenta.	Jeden VLAN dla całego klastra (wszystkich node).
Obiektowe, lokalne repozytorium danych	Internal	VLAN11	Liczba węzłów: min. 4 serwery na klaster, zasoby dyskowe: minimum 4 dyski SSD na serwer.	W przypadku potrzeby replikacji danych do drugiego centrum danych wymagane są dwa niezależne klastry (łącznie 8 serwerów); wszystkie node w jednym VLAN; dostęp głównie dla systemów automatycznych, ale może być również potrzeba dostępu bezpośrednio dla pracowników CSIRT, np. w celu analiz.
		VLAN N		Dodatkowe VLAN w zależności od potrzeb, np. VPN dla użytkowników CSIRT.

Załącznik 3. Przykładowy rejestr źródeł informacji

Nazwa źródła	Typ źródła	Charakter informacji	Forma dostępu	Częstotliwość aktualizacji	Wiarygodność	Data dodania	Data przeglądu	Uwagi	Odpowiedzialny
n6	Oficjalne (usługa CERT Polska)	IoC	Portal WWW + API	Codzienna	Duża	2021-01-15	2025-04-01	Głównie dla PL, za darmo	AB
CISA KEV Catalog	Oficjalne (instytucja rządowa USA)	Podatności aktywnie wykorzystywane	JSON	Codzienna	Duża	2023-10-03	2025-03-15	Przydatne API. Można skorzystać z GitHub	CD
Serwis typu pastebin	Społecznościowe /komercyjne	Wycieki danych	Automatyczny monitoring (skrypt)	Nieregularna	Mała	2023-12-01	2025-01-10	Wymaga dodatkowej weryfikacji autentyczności i wiarygodności	EF
Skaner plików pod kątem malware	Komercyjne	IoC, malware	API JSON	Ciągła	Duża	2022-05-01	2025-04-10	Jest również wersja darmowa	EF
FIRST mailing list	Społecznościowe	Ostrzeżenia, informacje o zagrożeniach (TLP: CLEAR)	e-mail	Nieregularna	Duża	2025-02-12	-		CD
Wyszukiwarka urządzeń dostępnych w internecie	Społecznościowe /komercyjne	Potencjalne zagrożenia (otwarte porty, banerów usług, podatności)	Portal WWW lub API	Ciągła	Średnia	2024-10-10	-	Trzeba pamiętać o znanych fałszywych alarmach (z ang. *false positive)*	EF
MWDB	Oficjalne (usługa CERT Polska)	IoC, TTP, powiązania między kampaniami	Portal WWW	Ciągła	Wysoka	2022-08-26	2024-08-13	Za darmo	AB
Artemis	Oficjalne (usługa CERT Polska)	Wyniki skanów podatności i błędów konfiguracyjnych	Portal WWW	Na żądanie	Wysoka	2023-11-30	2024-12-06		AB