NSC NARODOWE STANDARDY CYBERBEZPIECZEŃSTWA	Narodowy Standard Cyberbezpieczeństwa		
Nazwa standardu	Symbol	Wersja	Data wydania
Podręcznik postępowania z incydentami naruszenia bezpieczeństwa komputerowego	NSC 800-61	1.0	14/10/2021

Podręcznik postępowania z incydentami naruszenia bezpieczeństwa komputerowego

PEŁNOMOCNIK RZĄDU DS. CYBERBEZPIECZEŃSTWA

Warszawa 2021

Szanowni Państwo,

Departament Cyberbezpieczeństwa Kancelarii Prezesa Rady Ministrów udostępnia do wykorzystania w Państwa działalności zestaw publikacji specjalnych. Stanowią one rekomendację w postaci Narodowych Standardów Cyberbezpieczeństwa, o których mowa w kierunku interwencji 6.1 celu szczegółowego 2 Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019 – 2024, *Opracowanie i wdrożenie Narodowych Standardów Cyberbezpieczeństwa oraz promowanie dobrych praktyk i zaleceń*. Mimo, że prezentowane standardy zostały opracowane na podstawie publikacji amerykańskiego National Institute of Science and Technology (NIST), to posiadają one mapowanie na obowiązujące w polskim systemie prawnym Polskie Normy, stosowane w zarządzaniu bezpieczeństwem informacji przez podmioty krajowego systemu cyberbezpieczeństwa, w tym podmioty realizujące zadania publiczne, operatorów usług kluczowych i dostawców usług cyfrowych.

Zaprezentowane publikacje stanowią przewodniki metodyczne, które ułatwiają zbudowanie efektywnego systemu zarządzania bezpieczeństwem informacji w oparciu o praktykę, jaka w tym zakresie stosowana jest administracji federalnej USA.

Na prezentowany zestaw publikacji składają się następujące pozycje:[1]

- NSC[2] 199, *Standardy kategoryzacji bezpieczeństwa* – na podstawie FIPS 199;
- NSC 200, *Minimalne wymagania bezpieczeństwa informacji i systemów informatycznych podmiotów publicznych* – na podstawie FIPS 200;
- NSC 500-92, *Architektura referencyjna chmury obliczeniowej – rekomendacje* – na podstawie NIST SP 500-292;
- NSC 800-18, *Przewodnik do opracowywania planów bezpieczeństwa systemów informatycznych w podmiotach publicznych* – na podstawie NIST SP 800- 18;
- NSC 800-30, *Przewodnik dotyczący postępowania w zakresie szacowania ryzyka w podmiotach realizujących zadania publiczne* – na podstawie NIST SP 800-30;
- NSC 800-34, *Poradnik planowania awaryjnego* – na podstawie NIST SP 800-34;

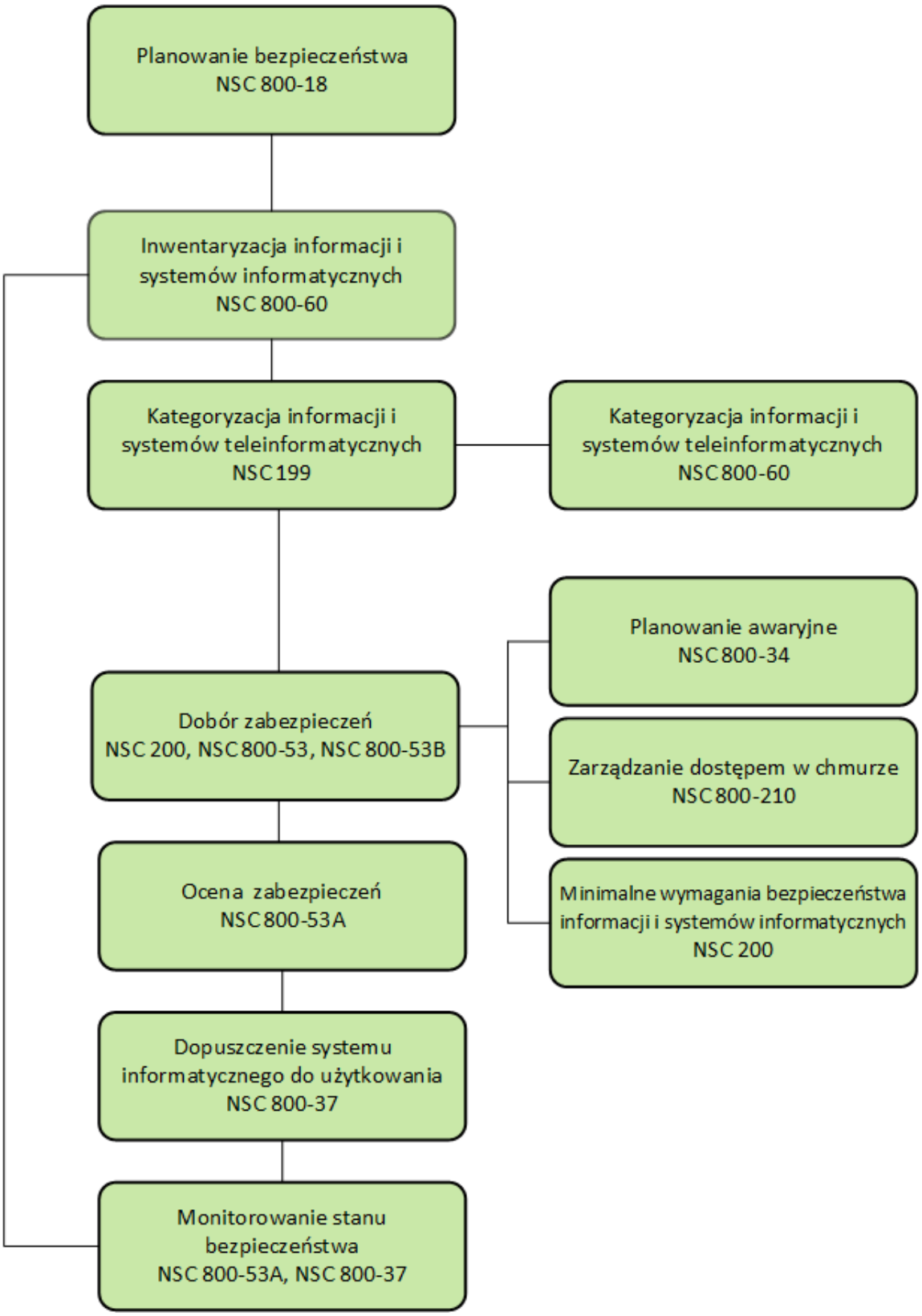
[1] Wymienione są podstawowe dokumenty. Każdy z nich może się odwoływać w rozdziale *Referencje* do szeregu powiązanych publikacji, które składają się na całościowy proces osiągania cyberbezpieczeństwa.

[2] NSC – Narodowy Standard Cyberbezpieczeństwa.

- NSC 800-37, *Ramy zarządzania ryzykiem w organizacjach i systemach informatycznych. Bezpieczeństwo i ochrona prywatności w cyklu życia systemu* – na podstawie NIST SP 800-37;
- NSC 800-53, *Zabezpieczenia i ochrona prywatności systemów informatycznych oraz organizacji* – na podstawie NIST SP 800-53;
- NSC 800-53A, *Ocena środków bezpieczeństwa i ochrony prywatności systemów informatycznych oraz organizacji. Tworzenie skutecznych planów oceny* – na podstawie NIST SP 800-53A;
- NSC 800-53B, *Zabezpieczenia bazowe systemów informatycznych oraz organizacji* – na podstawie NIST SP 800-53B;
- NSC 800-60, *Wytyczne w zakresie określania kategorii bezpieczeństwa informacji i kategorii bezpieczeństwa systemu informatycznego* – na podstawie NIST SP 800-60;
- NSC 800-61, *Podręcznik postępowania z incydentami naruszenia bezpieczeństwa komputerowego* – na podstawie NIST SP 800-61;
- NSC 800-210, *Ogólne wytyczne dotyczące kontroli dostępu do systemów chmury obliczeniowej* – na podstawie NIST SP 800-210.

Korzystając z tych publikacji można stosunkowo łatwo zbudować system zarządzania bezpieczeństwem informacji i sprawować nad nim niezbędną kontrolę.

Cykl zarządzania bezpieczeństwem bazujący na publikacjach NIST wykorzystuje następujące dokumenty:


Planowanie bezpieczeństwa
NSC 800-18
Inwentaryzacja informacji i systemów informatycznych
NSC 800-60
Kategoryzacja informacji i systemów teleinformatycznych
NSC 199
Kategoryzacja informacji i systemów teleinformatycznych
NSC 800-60
Planowanie awaryjne
NSC 800-34
Dobór zabezpieczeń
NSC 200, NSC 800-53, NSC 800-53B
Zarządzanie dostępem w chmurze
NSC 800-210
Ocena zabezpieczeń
NSC 800-53A
Minimalne wymagania bezpieczeństwa informacji i systemów informatycznych
NSC 200
Dopuszczenie systemu informatycznego do użytkowania
NSC 800-37
Monitorowanie stanu bezpieczeństwa
NSC 800-53A, NSC 800-37

WSPÓLNE FUNDAMENTY BEZPIECZEŃSTWA I OCHRONY PRYWATNOŚCI

National Institute of Standards and Technology (NIST) opracował wiele standardów i wytycznych w celu zapewnienia wspólnego podejścia do problematyki bezpieczeństwa informacji i systemów teleinformatycznych administracji federalnej USA. Podstawową rolę w podejściu do zagadnień związanych z zapewnieniem bezpieczeństwa informacji, bezpieczeństwa systemów teleinformatycznych oraz ochrony prywatności odgrywa elastyczny i spójny sposób zarządzania ryzykiem związanym z bezpieczeństwem i prywatnością operacji organizacyjnych i majątku, osób fizycznych, innych organizacji i Państwa. Zarządzanie ryzykiem stanowi podstawę do wdrożenia stosownych zabezpieczeń w systemach informacyjnych, ocenę tych zabezpieczeń, wzajemną akceptację dowodów oceny bezpieczeństwa i ochrony prywatności oraz decyzji autoryzacyjnych, a także dzięki jednolitemu podejściu, ułatwia wymianę informacji i współpracę pomiędzy różnymi podmiotami.

NIST kontynuuje współpracę z sektorem publicznymi i prywatnym w celu stworzenia map i relacji pomiędzy opracowanymi przez siebie standardami i wytycznymi, a tymi które zostały opracowane przez inne organizacje (np. ISO), co zapewnia zgodność w przypadku, gdy regulacje wymagają stosowania tych innych standardów.

Publikacje NIST, co do zasady, nie są objęte restrykcjami wynikającymi z autorskich praw majątkowych. Są powszechnie dostępne oraz dozwolone do użytku poza administracją federalną USA. Charakteryzują się pragmatycznym podejście do zagadnień związanych z bezpieczeństwem informacji, systemów teleinformatycznych oraz ochrony prywatności, przez co ułatwiają podmiotom opracowanie i eksploatację systemu zarządzania tym bezpieczeństwem.

Biorąc pod uwagę wszystkie powyższe aspekty, autorzy niniejszej publikacji polecają opracowania NIST jako godne zaufania i rekomendują stosowanie ich przez polskie podmioty w opracowywaniu systemów zarządzania bezpieczeństwem informacji, wdrażaniu zabezpieczeń i ocenie ich działania.

Podmioty, urządzenia lub materiały prezentowane są w niniejszym dokumencie w celu odpowiedniego opisania procedury lub koncepcji eksperymentalnej. Identyfikacja taka nie ma na celu nakłaniania do nich lub ich poparcia, nie ma też na celu sugerowania, że te podmioty, materiały lub sprzęt są najlepsze z dostępnych w tym obszarze.

W niniejszym Narodowym Standardzie Cyberbezpieczeństwa (NSC) mogą znajdować się odniesienia do innych publikacji opracowywanych obecnie przez Pełnomocnika Rządu ds. Cyberbezpieczeństwa zgodnie z przypisanymi mu obowiązkami ustawowymi. Informacje zawarte w tej publikacji, w tym koncepcje, praktyki i metodologie, mogą być wykorzystywane przez organizacje jeszcze przed ukończeniem innych towarzyszących temu standardowi publikacji. W związku z tym, do czasu ukończenia każdej publikacji, obowiązują aktualne wymagania, wytyczne i procedury, jeśli takie istnieją. W celach planistycznych i wprowadzania zmian, organizacje będą mogły uważnie śledzić rozwój tych nowych publikacji opracowywanych przez Pełnomocnika Rządu ds. Cyberbezpieczeństwa.

Niniejsza publikacja, ***Podręcznik postępowania z incydentami naruszenia bezpieczeństwa komputerowego***, opracowana została za zgodą National Institute of Science and Technology (NIST) na podstawie specjalnej publikacji NSC 800-61, Rev. 2.

Tam, gdzie to było możliwe i nie budziło kontrowersji, nazwy ról i kluczowych uczestników procesu zarządzania ryzykiem zostały podane w języku polskim. Pozostałe role i funkcje zostały przedstawione w języku angielskim. Do wszystkich tych ról / funkcji zastosowano akronimy terminologii angielskiej.

Terminologia angielska i akronimy występujące w publikacji zdefiniowane są w dokumencie NSC 7298, ***Słownik kluczowych pojęć z zakresu cyberbezpieczeństwa.***

Podziękowania

Zespół opracowujący Podręcznik pragnie złożyć podziękowania swoim współpracownikom, którzy dokonali opracowania niniejszego dokumentu i mają swój wkład w dostosowanie do warunków krajowego systemu cyberbezpieczeństwa.

Szczególne podziękowania należą się Pani Annie oraz Panu Witoldowi Sobolewskiemu z Rapid Response Team firmy VS DATA, którzy byli współautorami pierwszej wersji Podręcznika. Podziękowania należą się także pozostałym osobom Z RR biorącym udział w pracach nad podręcznikiem.

Autorzy chcieliby również wyrazić swoje podziękowania dla Pana dr hab. Jerzego Kosińskiego oraz Pana dr hab. Grzegorza Krasnodębskiego z Morskiego Centrum Cyberbezpieczeństwa funkcjonującego w ramach Wydziału Dowodzenia i Operacji Morskich Akademii Marynarki Wojennej im. Bohaterów Westerplatte w Gdyni za ich nieocenioną pomoc w trakcie prac nad wstępnym projektem niniejszego podręcznika.

SPIS TREŚCI

STRESZCZENIE

Reakcja na incydenty bezpieczeństwa komputerowego stała się ważnym elementem programów technologii informatycznych (IT). Cyber ataki stały się nie tylko bardziej liczne i różnorodne, ale również bardziej szkodliwe i uciążliwe. Często pojawiają się nowe typy incydentów bezpieczeństwa. Działania prewencyjne oparte na wynikach oceny ryzyka mogą zmniejszyć liczbę incydentów, jednakże nie wszystkim incydentom można zapobiec. Zdolność reagowania na incydenty jest więc niezbędna do szybkiego wykrywania incydentów, minimalizowania strat i zniszczeń, mitygowania wykorzystanych podatności oraz przywracania usług IT. W tym celu niniejsza publikacja zawiera wytyczne dotyczące obsługi incydentu, w szczególności analizowania danych związanych z incydentem oraz określania właściwej reakcji na każdy incydent. Wytyczne mogą być stosowane niezależnie od poszczególnych platform sprzętowych, systemów operacyjnych, protokołów oraz aplikacji.

Ponieważ skuteczna reakcja na incydent jest złożonym przedsięwzięciem, ustanowienie skutecznej zdolności reagowania na incydent wymaga znacznego przygotowania i posiadania stosownych zasobów. Konieczny jest ciągły monitoring ataków. Ustanowienie jasnych procedur priorytetyzacji obsługi incydentów jest krytyczne, tak samo jak implementowanie efektywnych metod gromadzenia, analizowania oraz raportowania danych. Niezbędne jest również zbudowanie relacji i ustanowienie odpowiednich środków komunikacji z innymi wewnętrznymi grupami (np. kadrowymi, prawnymi) oraz z zewnętrznymi podmiotami (np. innymi zespołami reagowania na incydent, organami ścigania).

Niniejsza publikacja wspiera organizacje w ustalaniu możliwości reagowania na incydenty bezpieczeństwa komputerowego oraz w skutecznej i efektywnej obsłudze incydentów. Odzwierciedla zmiany w atakach i incydentach. Zrozumienie zagrożeń i identyfikacja nowoczesnych ataków na ich wczesnym etapie jest kluczem do zapobiegania kolejnym naruszeniom, a proaktywna wymiana informacji na temat symptomów tych ataków między organizacjami, jest coraz skuteczniejszym sposobem ich identyfikacji.

Wdrożenie poniższych wymagań i zaleceń powinno ułatwić wydajną i skuteczną reakcję organizacji na incydenty.

Organizacje muszą stworzyć, zapewnić i obsługiwać formalną zdolność reagowania na incydenty. Aktualne przepisy prawa nakładają obowiązek zgłaszania incydentów przez podmioty krajowego systemu cyberbezpieczeństwa do jednego z trzech zespołów CSIRT

poziomu krajowego - Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego[3] (*ang. Computer Security Incident Response Teams – CSIRT)*.[4]

ZGŁASZANIE INCYDENTÓW W POLSCE

CSIRT GOV – zespół odpowiedzialny za koordynację obsługi incydentów m.in. w administracji rządowej oraz u operatorów infrastruktury krytycznej (w tym także u tych operatorów usług kluczowych, którzy w tym samym czasie są także operatorami infrastruktury krytycznej). Zgłoszenia należy przekazywać na adres mailowy: incydent@csirt.gov.pl. Na stronie internetowej dostępny jest formularz zgłoszenia. W sprawach pilnych możliwy jest kontakt z oficerem dyżurnym pod numerem: +48 22 58 59 373;

CSIRT MON – zespół odpowiedzialny za koordynację obsługi incydentów w sektorze militarnym. Zgłoszenia należy przekazywać na adres mailowy: csirt-mon@ron.mil.pl. Formularz do zgłoszenia jest dostępny tutaj. W sprawach pilnych możliwy jest kontakt z dyżurnym pod tel.: +48 261 87 16 41;

CSIRT NASK – zespół odpowiedzialny za koordynację incydentów m.in. u operatorów usług kluczowych, administracji samorządowej, w sektorze prywatnym oraz zgłaszanych przez osoby indywidualne. Zgłoszenie incydentu/podatności można dokonać w formie elektronicznej. Najlepiej zrobić to za pośrednictwem formularza online na stronie https://incydent.cert.pl, który podpowie, jakie informacje należy zawrzeć w zgłoszeniu. Alternatywnie, można wysłać zgłoszenie pocztą elektroniczną na adres cert@cert.pl. Ponadto, w sprawach pilnych można skontaktować się telefonicznie z dyżurem w CSIRT NASK po numerem tel. +48 22 380 82 74.

Każda organizacja przetwarzająca informacje powinna ustanowić zdolności reagowania na incydenty, wyznaczyć główny i dodatkowy punkt kontaktowy (*ang. Poit of Contact - PoC*) ze stosownym CSIRT i zgłaszać wszystkie incydenty zgodnie z polityką reagowania organizacji na

[3] Ustawa o krajowym systemie cyberbezpieczeństwa z dnia 05 lipca 2018 r. (Dz. U. 2018 poz. 1560).

[4] Terminologia angielska i akronimy występujące w publikacji zdefiniowane są w dokumencie NSC 7298, Słownik kluczowych pojęć z zakresu cyberbezpieczeństwa.

incydenty. Każda organizacja we własnym zakresie jest odpowiedzialna za określenie sposobu spełnienia tych wymagań.

Utworzenie zdolności reagowania na incydenty powinno obejmować następujące działania:

- Tworzenie polityki i planu reagowania na incydenty.
- Opracowanie procedur obsługi i raportowania incydentów.
- Ustalanie wytycznych dotyczących komunikowania się ze stronami zewnętrznymi w sprawie incydentów.
- Wybór struktury zespołu i modelu zatrudnienia.
- Nawiązanie relacji i linii komunikacji pomiędzy zespołem reagowania na incydenty a innymi grupami, zarówno wewnętrznymi (np. działem prawnym), jak i zewnętrznymi (np. organami ścigania).
- Określenie, jakie usługi powinien świadczyć zespół reagowania na incydenty.
- Zatrudnianie i szkolenie zespołu reagowania na incydenty.

Organizacje powinny ograniczać częstość występowania incydentów poprzez skuteczne zabezpieczanie sieci, systemów i aplikacji.

Zapobieganie problemom jest często mniej kosztowne i skuteczniejsze niż reagowanie na nie po ich wystąpieniu. Z tego powodu zapobieganie incydentom jest ważnym uzupełnieniem zdolności reagowania na incydenty. Jeśli zabezpieczenia są niewystarczające, może dojść do dużej liczby incydentów. Mogłoby to spowodować przeciążenie zasobów i zdolności reagowania, co spowodowałoby opóźnione lub niepełne odtworzenie i prawdopodobnie bardziej rozległe szkody i dłuższe okresy niedostępności usług i danych. Obsługa incydentów może być skuteczniejsza, jeśli organizacje uzupełniają swoje zdolności reagowania na incydenty odpowiednimi zasobami, aby aktywnie utrzymywać bezpieczeństwo sieci, systemów i aplikacji. Obejmuje to szkolenie personelu IT w zakresie przestrzegania standardów bezpieczeństwa organizacji oraz uświadamianie użytkownikom zasad i procedur dotyczących właściwego korzystania z sieci, systemów i aplikacji.

Organizacje powinny udokumentować swoje wytyczne dotyczące interakcji z innymi organizacjami w zakresie incydentów.

Podczas obsługi incydentu organizacja będzie musiała komunikować się ze stronami zewnętrznymi, takimi jak inne zespoły reagowania na incydenty, organy ścigania, media, dostawcy i poszkodowane organizacje. Ponieważ taka komunikacja często musi przebiegać

szybko, organizacje powinny z góry określić wytyczne dotyczące komunikacji, tak aby tylko odpowiednie informacje były udostępniane właściwym stronom.

Organizacje powinny być ogólnie przygotowane do obsługi każdego incydentu, ale powinny skupić się na przygotowaniu do obsługi incydentów wykorzystujących typowe wektory ataku.

Incydenty mogą wystąpić na niezliczone sposoby, więc nie jest możliwe opracowanie szczegółowych instrukcji postępowania w przypadku każdego incydentu. Niniejsza publikacja definiuje kilka typów incydentów w oparciu o typowe wektory ataków. kategorie te nie mają na celu zapewnienia ostatecznej klasyfikacji incydentów, ale mają służyć jako podstawa do zdefiniowania bardziej szczegółowych procedur postępowania. Różne rodzaje incydentów wymagają różnych strategii reagowania. Wektory ataku to:

- **Nośniki zewnętrzne / wymienne:** Atak przeprowadzony z nośnika wymiennego (np. Pendrive, CD) lub urządzenia peryferyjnego.
- **Przejęcie**: Atak wykorzystujący metody brute-force w celu złamania, degradacji lub zniszczenia systemów, sieci lub usług.
- **Web:** Atak wykonany z witryny internetowej lub aplikacji internetowej.
- **E-mail:** Atak przeprowadzony za pośrednictwem wiadomości e-mail lub załącznika.
- **Niewłaściwe użytkowanie:** wszelkie incydenty wynikające z naruszenia zasad dopuszczalnego użytkowania organizacji przez autoryzowanego użytkownika, z wyłączeniem powyższych kategorii.
- **Utrata lub kradzież sprzętu:** utrata lub kradzież urządzenia komputerowego lub nośnika używanego przez organizację, na przykład laptopa lub smartfona.
- **Inne:** Atak, który nie pasuje do żadnej z pozostałych kategorii.

Organizacje powinny podkreślać znaczenie wykrywania i analizy incydentów w całej organizacji.

W organizacji każdego dnia mogą wystąpić miliony możliwych oznak incydentów, rejestrowanych głównie przez logowanie i oprogramowanie zabezpieczające komputer. Automatyzacja potrzebna jest do przeprowadzenia wstępnej analizy danych i wybrania zdarzeń, które są przedmiotem weryfikacji przez człowieka. Oprogramowanie do korelacji zdarzeń może mieć wielką wartość w automatyzacji procesu analizy. Jednak skuteczność procesu zależy od jakości danych, które do niego trafiają. Organizacje powinny ustanowić

standardy i procedury rejestrowania, aby zapewnić gromadzenie odpowiednich informacji przez dzienniki i oprogramowanie zabezpieczające oraz regularne przeglądanie danych.

Organizacje powinny stworzyć pisemne wytyczne dotyczące priorytetyzacji incydentów.

Priorytetyzacja obsługi poszczególnych incydentów jest krytycznym punktem decyzyjnym w procesie reagowania na incydent. Skuteczne udostępnianie informacji może pomóc organizacji zidentyfikować sytuacje, które są poważniejsze i wymagają natychmiastowej uwagi. Incydentom należy nadawać priorytety na podstawie odpowiednich czynników, takich jak funkcjonalny wpływ incydentu (np. obecny i prawdopodobny przyszły negatywny wpływ na funkcje biznesowe), wpływ incydentu na informacje (np. wpływ na poufność, integralność i dostępność informacji organizacji) oraz możliwości odtworzenia po incydencie (np. czas i rodzaje zasobów, które należy przeznaczyć na odtworzenie po incydencie).

Organizacje powinny wykorzystać wyciągnięte wnioski, aby uzyskać wartość z incydentów.

Po obsłużeniu poważnego incydentu organizacja powinna zorganizować spotkanie, na którym przedstawione zostaną wnioski, mające na celu dokonanie przeglądu skuteczności procesu obsługi incydentu i zidentyfikowania niezbędne ulepszenia istniejących zabezpieczeń i praktyk bezpieczeństwa. W przypadku mniej znaczących incydentów, o ile pozwalają na to czas i zasoby, można również organizować tego rodzaju okresowe spotkania. Informacje zebrane ze wszystkich spotkań na temat zdobytego doświadczenia powinny być wykorzystane do określenia i skorygowania słabości systemowych oraz braków w zakresie zasad i procedur Raporty uzupełniające generowane dla każdego rozwiązanego incydentu, mogą być ważne nie tylko dla celów dowodowych, ale także jako odniesienie w obsłudze przyszłych incydentów i szkoleniu nowych członków zespołu.

WSTĘP

Cel i zakres

Niniejsza publikacja ma na celu pomóc organizacjom w ograniczaniu ryzyka związanego z incydentami związanymi z bezpieczeństwem komputerowym, dostarczając praktycznych wskazówek dotyczących skutecznego i wydajnego reagowania na incydenty. Zawiera wskazówki dotyczące tworzenia skutecznego programu reagowania na incydenty, ale głównym celem dokumentu jest wykrywanie, analizowanie, ustalanie priorytetów i obsługa incydentów. Zachęca się organizacje do dostosowywania zalecanych wytycznych i rozwiązań, aby spełniały ich specyficzne wymagania dotyczące bezpieczeństwa i misji.

Odbiorcy

Dokument został stworzony dla administratorów systemów i sieci, pracowników zajmujących się bezpieczeństwem, personelu wsparcia technicznego, *chief information security officers (CISOs), chief information officers (CIOs)*, menedżerów programów bezpieczeństwa komputerowego i innych osób, które są odpowiedzialne za przygotowanie i reagowanie na incydenty bezpieczeństwa.[5]

Struktura dokumentu

Publikacja jest podzielona na następujące sekcje i dodatki:

- Część 1 określa uprawnienia, cel i zakres oraz odbiorców do których jest skierowany dokument.
- Część 2 omawia potrzebę reagowania na incydenty, zarysowuje możliwe struktury zespołów reagowania na incydenty i wskazuje inne grupy w organizacji, które mogą uczestniczyć w obsłudze incydentu.
- Rozdział 3 zawiera przegląd podstawowych etapów obsługi incydentu i porady dotyczące skuteczniejszej obsługi incydentów, w szczególności wykrywania i analizy incydentów.

[5] Opis ról / funkcji zawarty jest w dokumencie NSC 7298, *Słownik kluczowych pojęć z zakresu cyberbezpieczeństwa* oraz w publikacji NSC 800-37, *Ramy zarządzania ryzykiem w organizacjach i systemach informatycznych. Bezpieczeństwo i ochrona prywatności w cyklu życia systemu*.

.

- Rozdział 4 analizuje potrzebę koordynacji reagowania na incydent i wymiany informacji.
- Załącznik A zawiera przykładowe scenariusze reagowania na incydenty i pytania do wykorzystania w dyskusjach zespołu na temat reagowania na incydenty.
- Załącznik B zawiera listy sugerowanych danych, które należy gromadzić dla każdego incydentu.
- Załączniki C i D zawierają odpowiednio słownik i listę skrótów.
- Załącznik E określa zasoby, które mogą być przydatne w planowaniu i podejmowaniu reakcji na incydenty.
- Załącznik F zawiera często zadawane pytania dotyczące reagowania na incydent.
- Załącznik G wymienia główne kroki, które należy wykonać podczas postępowania z kryzysem związanym z incydentem bezpieczeństwa komputerowego.
- Załącznik H zawiera historię zmian zawierającą istotne zmiany względem poprzedniej wersji.

ORGANIZACJA ZDOLNOŚCI REAGOWANIA NA INCYDENT BEZPIECZEŃSTWA KOMPUTEROWEGO

Zorganizowanie skutecznej zdolności reagowania na incydent bezpieczeństwa komputerowego (*ang. Computer Security Incident Response Capability - CSIRC*) obejmuje kilka ważnych decyzji i działań. Jednym z pierwszych rozważań powinno być stworzenie specyficznej dla danej organizacji katalogu zdarzeń traktowanych jako *incydent* tak, aby zakres tego pojęcia był jasny. Organizacja powinna zdecydować, jakie usługi powinien świadczyć zespół reagowania na incydenty, rozważyć, które struktury zespołu i modele mogą świadczyć te usługi, a także wybrać i wdrożyć jeden lub więcej zespołów reagowania na incydenty. Tworzenie planu, polityki i procedur reagowania na incydenty jest ważną częścią tworzenia zespołu, tak aby reakcja na incydent była wykonywana skutecznie, wydajnie i konsekwentnie, a zespół posiadał uprawnienia do wykonywania niezbędnych działań. Plan, zasady i procedury powinny odzwierciedlać interakcje zespołu z innymi zespołami w organizacji, a także ze stronami zewnętrznymi, takimi jak organy ścigania, media i inne organizacje reagowania na incydenty. Ta Rozdział zawiera nie tylko wskazówki, które powinny być pomocne dla organizacji, które tworzą możliwości reagowania na incydenty, ale także porady dotyczące utrzymania i ulepszania istniejących możliwości.

Zdarzenia i incydenty

Zdarzenie to każde obserwowalne zjawisko w systemie lub sieci. Zdarzenia obejmują np. połączenie użytkownika do współdzielonych plików, serwer odbierający żądanie dotyczące strony internetowej, użytkownika wysyłającego wiadomość e-mail oraz zaporę blokującą próbę połączenia. Zdarzenia niepożądane to zdarzenia o negatywnych konsekwencjach, takie jak np. awarie systemu, przepełnienie systemu pakietami, nieautoryzowane użycie uprawnień systemowych, nieautoryzowany dostęp do wrażliwych danych oraz wykonanie złośliwego oprogramowania niszczącego dane. W tym przewodniku omówiono tylko niepożądane zdarzenia w zakresie cyberbezpieczeństwa związane z działalnością człowieka wobec systemu teleinformatycznego, a nie te spowodowane klęskami żywiołowymi, awariami zasilania itp.

Incydent bezpieczeństwa komputerowego to naruszenie lub bezpośrednie zagrożenie naruszeniem[6] zasad bezpieczeństwa komputerowego, zasad dopuszczalnego użytkowania lub standardowych praktyk bezpieczeństwa. Przykłady incydentów[7] to:

- Atakujący nakazuje botnetowi wysyłanie dużej liczby żądań połączeń do serwera WWW, powodując jego awarię.
- Użytkownicy są nakłaniani do otwierania „kwartalnego raportu" wysyłanego pocztą elektroniczną, który w rzeczywistości zawiera złośliwe oprogramowanie. Uruchomienie narzędzia spowodowało zainfekowanie ich komputerów i nawiązanie połączeń z zewnętrznym hostem.
- Osoba atakująca uzyskuje wrażliwe dane i grozi, że zostaną one ujawnione publicznie, jeśli organizacja nie zapłaci określonej kwoty pieniędzy.
- Użytkownik udostępnia lub ujawnia poufne informacje innym osobom za pośrednictwem usług wymiany plików w trybie peer-to-peer.

2.2. Potrzeba reagowania na incydent

Ataki często zagrażają bezpieczeństwu danych osobowych i biznesowych, dlatego niezwykle ważne jest, aby reagować szybko i skutecznie w przypadku naruszenia bezpieczeństwa.

[6] „Bezpośrednie zagrożenie naruszeniem" odnosi się do sytuacji, w której organizacja ma faktyczne podstawy, aby przypuszczać, że wkrótce nastąpi określony incydent. Na przykład opiekunowie oprogramowania antywirusowego mogą otrzymać biuletyn od dostawcy oprogramowania, ostrzegający ich o nowym złośliwym oprogramowaniu, które szybko rozprzestrzenia się w Internecie.

[7] W pozostałej części tego dokumentu terminy „incydent" i „incydent związany z bezpieczeństwem komputera" stosowane są zamiennie.

Koncepcja reagowania na incydent bezpieczeństwa komputerowego została szeroko zaakceptowana i wdrożona. Jedną z zalet posiadania zdolności reagowania na incydenty jest to, że wspiera ona systematyczne reagowanie na incydenty (tj. zgodnie ze spójną metodologią obsługi incydentów) tak, aby podejmowane były odpowiednie działania. Reagowanie na incydent pomaga personelowi zminimalizować utratę lub kradzież informacji oraz zakłócenia usług spowodowane incydentami. Inną korzyścią płynącą z reagowania na incydenty jest możliwość wykorzystania informacji uzyskanych podczas obsługi incydentów w celu lepszego przygotowania się do obsługi przyszłych incydentów oraz zapewnienia lepszej ochrony systemów i danych. Zdolność reagowania na incydent pomaga również we właściwym rozwiązywaniu problemów prawnych, które mogą pojawić się podczas incydentów.

Oprócz biznesowych powodów ustanowienia zdolności reagowania na incydent, organizacje powinny przestrzegać prawa, przepisów i polityki, kierując skoordynowaną, skuteczną obroną przed zagrożeniami bezpieczeństwa informacji .

2.3. Tworzenie zasad, planów i procedur reagowania na incydenty

W tej rozdziale omówione są zasady, plany i procedury związane z reagowaniem na incydenty, z naciskiem na interakcje z organizacjami zewnętrznymi.

2.3.1. Elementy zasad

Zasady określające reagowanie na incydenty są wysoce zindywidualizowane w danej organizacji. Jednak większość zasad zawiera te same elementy kluczowe:

- Oświadczenie o zaangażowaniu w zarządzanie.
- Cele i zadania zasad.
- Zakres zasad (do kogo i do czego mają zastosowanie oraz w jakich okolicznościach).
- Struktura organizacyjna i definicja ról, obowiązków i poziomów uprawnień. Powinna obejmować uprawnienia zespołu reagowania na incydenty do konfiskowania lub odłączania sprzętu i monitorowania podejrzanych działań, wymagania dotyczące zgłaszania określonych rodzajów incydentów, wymagania i wytyczne dotyczące komunikacji zewnętrznej i wymiany informacji (np. co komu można udostępnić, kiedy oraz jakimi kanałami) oraz punkty przekazania i eskalacji w procesie zarządzania incydentami.
- Ustalanie priorytetów lub oceny wagi incydentów.

- Miary wydajności (omówione w rozdziale 3.4.2).

2.3.2. Elementy planu

Organizacje powinny stosować formalne, ukierunkowane i skoordynowane podejście do reagowania na incydent, w tym posiadać plan reagowania na incydenty, który zawiera plan działań w zakresie wdrażania zdolności reagowania na incydent. Każda organizacja opracowuje plan, który spełnia jej unikalne wymagania, odnoszące się do misji, rozmiaru, struktury i funkcji organizacji. Plan powinien określać niezbędne zasoby i wsparcie zarządzania.

Plan reagowania na incydenty powinien zawierać następujące elementy:

- Misja organizacji.
- Strategie i cele stawiane przed organizacją.
- Aprobatę wyższego kierownictwa.
- Organizacyjne podejście do reagowania na incydenty
- Sposób komunikacji zespołu reagowania na incydenty z resztą organizacji i innymi organizacjami.
- Wskaźniki pomiaru zdolności i skuteczności reagowania na incydenty.
- Harmonogram doskonalenia zdolności reagowania na incydenty.
- Opis, w jaki sposób program wpisuje się w ogół organizacji.

Misja, strategie i cele organizacji w zakresie reagowania na incydenty powinny być pomocne w określeniu struktury jej zdolności do reagowania na incydent. W planie należy również omówić strukturę programu reagowania na incydent. W rozdziale 2.4.1 omówione są rodzaje struktur.

Po opracowaniu planu i uzyskaniu zatwierdzenia kierownictwa, organizacja powinna wdrożyć plan i dokonywać jego przeglądu co najmniej raz w roku, aby upewnić się, że postępuje zgodnie z planem działania i doskonalenia zdolności oraz realizacji celów w zakresie reagowania na incydenty.

2.3.3. Elementy procedur

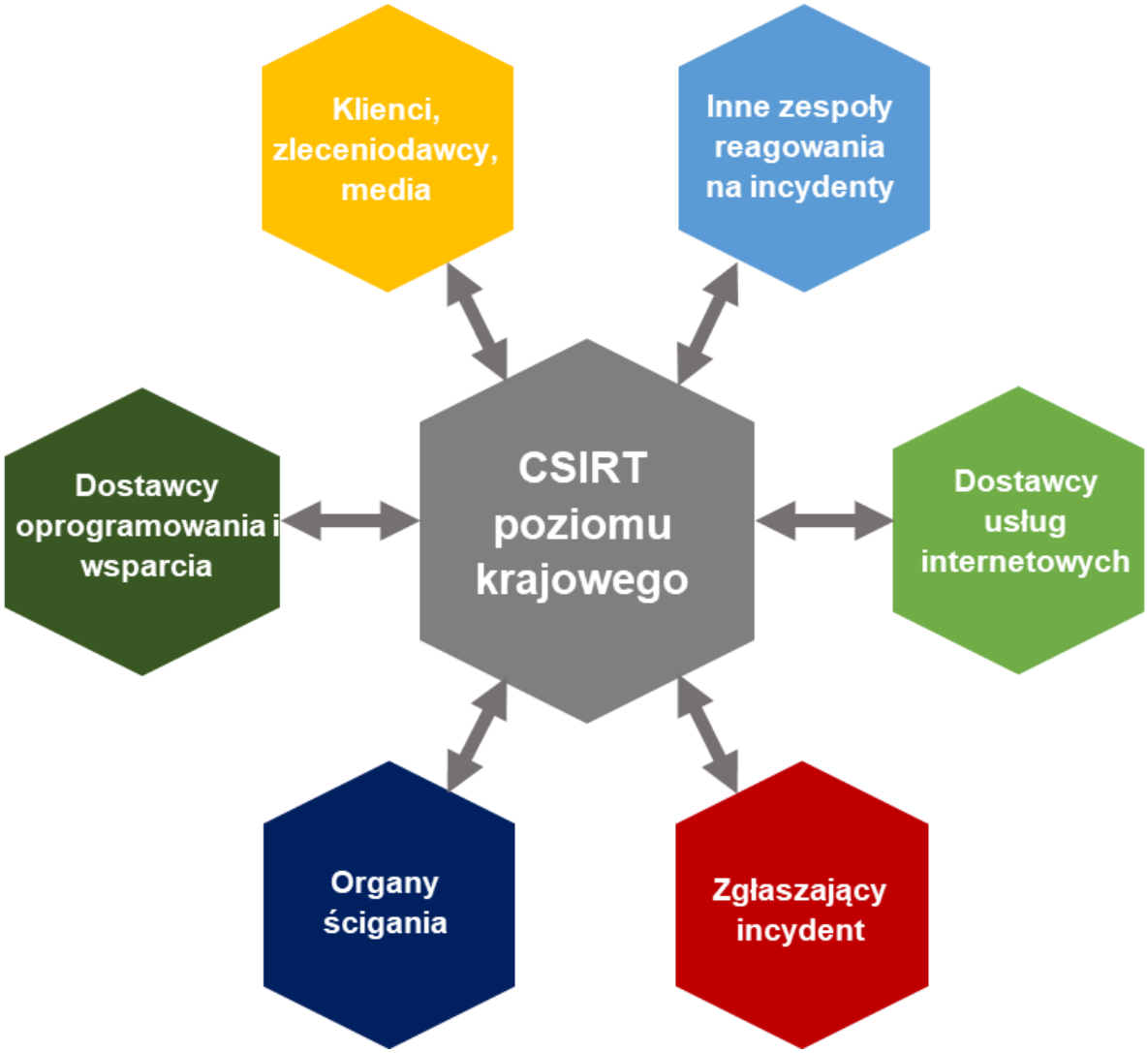
Procedury powinny być oparte na zasadach i planie reagowania na incydent. Standardowe procedury operacyjne (*ang. Standard Operating Procedures - SOP*) nakreślają konkretne procesy techniczne, techniki, listy kontrolne i formularze używane przez zespół reagowania

na incydenty. SOP powinny być wystarczająco kompleksowe i szczegółowe, aby zapewnić odzwierciedlenie priorytetów organizacji w operacjach reagowania na incydenty. Ponadto przestrzeganie ustandaryzowanych odpowiedzi powinno zminimalizować błędy, szczególnie te, które mogą być spowodowane stresującymi sytuacjami związanymi z obsługą incydentu. SOP powinny zostać przetestować w celu zweryfikowania ich dokładności i przydatności, a następnie rozesłać do wszystkich członków zespołu. Należy zapewnić szkolenie dla użytkowników SOP. Dokumenty SOP mogą służyć jako narzędzie instruktażowe. Sugerowane elementy SOP przedstawiono w rozdziale 3.

2.3.4. Wymiana informacji z podmiotami zewnętrznymi

Organizacje często muszą komunikować się ze stronami zewnętrznymi w sprawie incydentów i powinny to robić, gdy jest to stosowne, na przykład kontaktując się z organami ścigania, odpowiadając na zapytania mediów, w celu uzyskania opinii ekspertów zewnętrznych. Dodatkowym przykładem jest omawianie incydentów z innymi zaangażowanymi stronami, takimi jak dostawcy usług internetowych (*ang. Internet Service Provider - ISP*), dostawcy podatnego oprogramowania lub inne zespoły reagowania na incydenty. Organizacje mogą również aktywnie udostępniać informacje o wskaźnikach incydentów współpracownikom, aby usprawnić wykrywanie i analizę incydentów. Przed wystąpieniem incydentu, zespół reagowania na incydenty powinien omówić udostępnianie informacji np. z biurem spraw publicznych organizacji, działem prawnym i kierownictwem w celu ustalenia zasad i procedur dotyczących udostępniania informacji. W przeciwnym razie wrażliwe informacje dotyczące incydentów mogą zostać przekazane nieupoważnionym stronom, co może prowadzić do dodatkowych zakłóceń i strat finansowych. Zespół powinien dokumentować wszystkie kontakty i komunikację ze stronami zewnętrznymi dla celów ustalenia odpowiedzialności i dowodowych.

Poniższe sekcje zawierają wytyczne dotyczące komunikowania się z kilkoma typami stron zewnętrznych, jak pokazano na rysunku 2-1. Dwukierunkowe strzałki wskazują, że każda ze stron może zainicjować komunikację. Dodatkowe informacje na temat komunikowania się ze stronami zewnętrznymi zawiera rozdział 4, a omówienie komunikacji z udziałem podwykonawców reagowania na incydenty podane jest w rozdziale 2.4.



Rysunek 2-1. Komunikacja z podmiotami zewnętrznymi.

2.3.4.1. Media

Zespół reagowania na incydenty powinien ustanowić procedury komunikacji z mediami, które są zgodne z polityką organizacji dotyczącą interakcji z mediami i ujawniania informacji[8]. W celu omówienia incydentu z organizacjami medialnymi często korzystne jest wyznaczenie pojedynczego punktu kontaktowego (PoC) i przynajmniej jednego kontaktu zapasowego.

[88] Na przykład organizacja może wymagać, aby członkowie jej biura ds. publicznych i działu prawnego, uczestniczyli we wszystkich rozmowach z mediami dotyczących incydentów.

W celu przygotowania wyznaczonych kontaktów oraz innych osób, które mogą komunikować się z mediami, zalecane jest przeprowadzenie poniższych działań:

- Dokonywanie szkoleń dotyczącego interakcji z mediami w zakresie incydentów, które powinny obejmować nieujawnianie wrażliwych informacji, takich jak techniczne szczegóły środków zaradczych, których znajomość może pomóc napastnikom, oraz pozytywne aspekty przekazywania ważnych informacji opinii publicznej w sposób pełny i skuteczny.
- Ustanowienie procedur kontaktów z mediami w sprawie zgłaszania problemów i delikatnych kwestii związanych z konkretnym incydentem, przed omówieniem go z mediami.
- Utrzymywanie opisu aktualnego stanu incydentu, tak aby komunikacja z mediami była spójna i aktualna.
- Przypominanie całemu personelowi o ogólnych procedurach obsługi zapytań mediów.
- Przeprowadzanie pozorowanych wywiadów i konferencji prasowych podczas ćwiczeń związanych z obsługą incydentów. Przykładowe pytania do kontaktu z mediami:
  - Kto was zaatakował? Dlaczego?
  - Kiedy to się stało? Jak to się stało? Czy stało się tak, ponieważ stosujecie złe praktyki w zakresie bezpieczeństwa?
  - Jak rozległy jest ten incydent? Jakie kroki podejmujecie, aby ustalić, co się stało i zapobiec przyszłym zdarzeniom?
  - Jakie są skutki tego incydentu? Czy ujawniono jakiekolwiek dane osobowe? Jaki jest szacunkowy koszt tego incydentu?

2.3.4.2. Organy ścigania

Jednym z powodów, dla których wiele incydentów związanych z bezpieczeństwem nie kończy się wyrokami skazującymi, jest fakt, że niektóre organizacje nie kontaktują się we właściwy sposób z organami ścigania. Zespół reagowania na incydenty powinien zapoznać się z różnymi przedstawicielami organów ścigania przed wystąpieniem incydentu, aby omówić warunki, w jaki sposób należy im zgłaszać incydenty, sposób zgłaszania, jakie dowody należy zebrać i w jaki sposób powinny być one zabezpieczane.

Z organami ścigania należy kontaktować się za pośrednictwem wyznaczonych osób w sposób zgodny z wymogami prawa i procedurami organizacji. Wiele organizacji woli wyznaczyć

jednego członka zespołu reagowania na incydenty jako główny PoC z organami ścigania. Osoba ta powinna znać procedury zgłaszania do wszystkich odpowiednich organów ścigania i być dobrze przygotowana do wydawanie zaleceń, z którą agencją, jeśli rzeczywiście istnieje taka konieczność, należy się skontaktować. Należy pamiętać, że organizacja zazwyczaj nie powinna kontaktować się z wieloma agencjami, ponieważ może to spowodować konflikty jurysdykcyjne. Zespół reagowania na incydenty powinien zrozumieć, jakie są potencjalne problemy z jurysdykcją (np. lokalizacja fizyczna - organizacja z siedzibą w danym obiekcie ma serwer znajdujący się w innej lokalizacji, który został zaatakowany przez atakującego z innego miejsca).

2.3.4.3. Organizacje zgłaszające incydenty

Każda organizacja powinna wyznaczyć główną i dodatkową osobę kontaktową z CSIRT i zgłaszać wszystkie incydenty zgodnie z polityką organizacyjną dotyczącą reagowania na incydenty. Organizacje powinny stworzyć politykę określającą, kto jest wyznaczony do zgłaszania incydentów oraz w jaki sposób incydenty powinny być zgłaszane. Wymagania, kategorie i ramy czasowe dotyczące zgłaszania incydentów do CSIRT znajdują się na stronach internetowych odpowiednich CSIRT. Wszystkie organizacje publiczne powinny zapewnić, że ich procedury reagowania na incydenty są zgodne z wymogami raportowania CSIRT oraz procedury te są odpowiednio przestrzegane. Zachęca się wszystkie organizacje do zgłaszania incydentów do odpowiednich zespołów CSIRT. Jeśli organizacja nie ma własnego zespołu CSIRT, z którym można się skontaktować, może zgłaszać incydenty innym organizacjom, w tym Centrom Wymiany Informacji i Analiz (*ang. Information Sharing and Analysis Center - ISAC*). Jedną z funkcji tych branżowych grup z sektora prywatnego jest udostępnianie swoim członkom ważnych informacji związanych z bezpieczeństwem komputerowym. Należy podkreślić, że niektóre kategorie incydentów, określone w ustawie o krajowym systemie cyberbezpieczeństwa, podlegają zgłoszeniom do CSIRT poziomu krajowego, określonego dla danego podmiotu w przepisach tej ustawy.

Utworzone będą centra analizy i wymiany informacji dla sektorów przemysłu, takich jak komunikacja, sektor elektryczny, usługi finansowe, technologie informacyjne oraz badania i edukacja[9].

2.3.4.4. Inne podmioty zewnętrzne

Organizacja może chcieć omówić kwestie incydentów z innymi grupami, w tym z wymienionymi poniżej. Kontaktując się z takimi podmiotami zewnętrznymi, organizacja

[9] Odwiedź stronę internetową Krajowego Biura ISAC pod adresem http://www.isaccouncil.org/, aby zapoznać się z listą ISAC.

może chcieć współpracować z CSIRT NASK, jako *zaufanym wprowadzającym*, który pośredniczy w relacji. Jest prawdopodobne, że inni doświadczają podobnych problemów, a *zaufany wprowadzający* może upewnić się, że wszelkie takie wzorce zostały zidentyfikowane i wzięte pod uwagę.

- **Dostawca usług internetowych organizacji.** Organizacja może potrzebować pomocy swojego dostawcy usług internetowych w celu zablokowania poważnego ataku sieciowego lub śledzenia jego źródła.
- **Właściciele adresów IP, z których przeprowadzane są ataki.** Jeśli ataki pochodzą z przestrzeni adresowej IP organizacji zewnętrznej, osoby zajmujące się incydentami mogą chcieć skomunikować się z wyznaczonymi osobami kontaktowymi ds. bezpieczeństwa danej organizacji, aby powiadomić ich o działaniu lub zwrócić się o zebranie dowodów. Zdecydowanie zaleca się koordynowanie takiej komunikacji z właściwym dla danego podmiotu CSIRT poziomu krajowego.
- **Dostawcy oprogramowania.** Osoby obsługujące incydenty mogą chcieć skontaktować się z dostawcą oprogramowania w temacie podejrzanej aktywności. Kontakt ten może obejmować pytania dotyczące znaczenia niektórych wpisów w dzienniku lub znanych fałszywych alarmów dla niektórych sygnatur wykrywania naruszeń, w przypadku których może być konieczne ujawnienie minimalnych informacji dotyczących incydentu. W niektórych przypadkach może być konieczne podanie dodatkowych informacji - na przykład, jeśli wydaje się, że serwer został zagrożony przez nieznaną lukę w zabezpieczeniach oprogramowania. Dostawcy oprogramowania mogą również dostarczać informacje o znanych zagrożeniach (np. nowych atakach), aby pomóc organizacjom zrozumieć obecne środowisko zagrożeń.
- **Inne zespoły reagowania na incydenty.** W organizacji może wystąpić incydent podobny do tego, którym zajmują się inne zespoły. Aktywne udostępnianie informacji może ułatwić skuteczniejszą i wydajniejszą obsługę incydentu (np. ostrzeganie z wyprzedzeniem, zwiększanie gotowości, rozwój świadomości sytuacyjnej).
- **Dotknięte podmioty zewnętrzne.** Incydent może bezpośrednio wpłynąć na podmioty zewnętrzne - na przykład organizacja zewnętrzna może skontaktować się z organizacją i twierdzić, że atakuje ją jeden z użytkowników organizacji. Innym sposobem wywierania wpływu na podmioty zewnętrzne jest uzyskanie przez atakującego dostępu do dotyczących go wrażliwych informacji, takich jak dane karty kredytowej. W niektórych jurysdykcjach organizacje są zobowiązane do powiadomienia wszystkich stron, których dotyczy taki incydent. Niezależnie od

okoliczności, lepiej byłoby, gdyby organizacja powiadomiła strony zewnętrzne, których to dotyczy, o incydencie, zanim zrobią to media lub inne organizacje zewnętrzne. Osoby zarządzające powinny uważać, aby podawać tylko odpowiednie informacje - zainteresowane strony mogą zażądać szczegółów dotyczących dochodzeń wewnętrznych, które nie powinny być ujawniane publicznie.

Obsługujący incydent powinni rozumieć, w jaki sposób ich działania związane z obsługą incydentów powinny różnić się w przypadku podejrzenia naruszenia danych osobowych, takie jak powiadomienie właściwych stron, zgodnie z przepisami o ochronie danych osobowych.

2.4. Struktura zespołu reagowania na incydenty

Zespół reagowania na incydenty powinien być dostępny dla każdego, kto odkryje lub podejrzewa, że miał miejsce incydent z udziałem organizacji. Jeden lub więcej członków zespołu, w zależności od wielkości incydentu i dostępności personelu, powinien zająć się incydentem. Osoby zajmujące się incydentem analizują dane z incydentu, określają wpływ incydentu i podejmują odpowiednie działania, aby ograniczyć szkody i przywrócić normalne funkcjonowanie usługi. Sukces zespołu reagowania na incydenty zależy od udziału i współpracy poszczególnych osób w całej organizacji. Ta Rozdział identyfikuje takie osoby, omawia modele zespołów reagowania na incydenty i zawiera porady dotyczące wyboru odpowiedniego modelu.

2.4.1. Model zespołu

Możliwe struktury zespołu reagowania na incydenty obejmują:

- **Centralny zespół reagowania na incydenty.** Pojedynczy zespół reagowania na incydenty obsługuje incydenty w całej organizacji. Ten model jest skuteczny dla małych organizacji i organizacji o minimalnej różnorodności geograficznej pod względem zasobów obliczeniowych.
- **Rozproszone zespoły reagowania na incydenty.** Organizacja ma wiele zespołów reagowania na incydenty, z których każdy jest odpowiedzialny za określony logiczny lub fizyczny segment organizacji. Model ten jest skuteczny dla dużych organizacji (np. jeden zespół na oddział) oraz dla organizacji z dużymi zasobami obliczeniowymi w odległych lokalizacjach (np. jeden zespół na region geograficzny, jeden zespół na główny obiekt). Zespoły jednak powinny być częścią jednej, skoordynowanej jednostki, aby proces reagowania na incydenty był spójny w całej organizacji, a informacje były współdzielone między zespołami. Jest to szczególnie ważne,

ponieważ wiele zespołów może zidentyfikować elementy tego samego incydentu lub może obsługiwać podobne incydenty.

Zespoły reagowania na incydenty mogą również korzystać z dowolnego z trzech modeli zatrudnienia:

- **Pracownicy.** Organizacja wykonuje wszystkie prace związane z reagowaniem na incydenty przy ograniczonym wsparciu technicznym i administracyjnym ze strony wykonawców.
- **Częściowo zlecone na zewnątrz (podwykonawcy).** Organizacja zleca część swoich prac związanych z reagowaniem na incydenty. W rozdziale 2.4.2 omówiono główne czynniki, które należy wziąć pod uwagę przy wykorzystywaniu podwykonawców. Chociaż obowiązki reagowania na incydenty można podzielić na wiele sposobów między organizację i jednego lub więcej podwykonawców, kilka ustaleń stało się powszechnych:
  - Najbardziej rozpowszechnionym rozwiązaniem jest zlecanie przez organizację 24-godzinnego na dobę, 7 dni w tygodniu (24/7) monitorowania systemów wykrywania włamań, zapór i innych urządzeń zabezpieczających, zewnętrznemu dostawcy usług w zakresie zarządzania bezpieczeństwem *(ang. Managed Security Services Provider - MSSP*). MSSP identyfikuje i analizuje podejrzane działania i zgłasza każde wykryty incydent zespołowi reagowania na incydenty organizacji.
  - Niektóre organizacje wykonują podstawowe prace w zakresie reagowania na incydenty we własnym zakresie i wzywają wykonawców do pomocy w obsłudze incydentów, szczególnie tych, które są poważniejsze lub bardziej rozpowszechnione.
- **Pełne podwykonawstwo.** Organizacja całkowicie zleca swoje prace związane z reagowaniem na incydenty, wykonawcy obecnemu w jej obiekcie. Ten model jest najczęściej stosowany, gdy organizacja potrzebuje pełnoetatowego zespołu reagowania na incydenty w swojej lokalizacji, ale nie ma wystarczającej liczby wykwalifikowanych pracowników. Zakłada się, że organizacja będzie dysponowała pracownikami nadzorującymi pracę podwykonawców.

2.4.2. Wybór modelu zespołu

Wybierając odpowiednią strukturę i modele kadrowe dla zespołu reagowania na incydenty, organizacje powinny wziąć pod uwagę następujące czynniki:

- **Potrzeba dostępności 24/7.** Większość organizacji potrzebuje całodobowej dostępności pracowników reagujących na incydenty. Zwykle oznacza to, że z osobami zajmującymi się incydentami można skontaktować się telefonicznie, ale może to również oznaczać, że wymagana jest obecność w obiekcie. Dostępność w czasie rzeczywistym jest najlepsza do reagowania na incydenty, ponieważ im dłużej trwa incydent, tym większy potencjał wystąpienia szkód i strat. Kontakt w czasie rzeczywistym jest często potrzebny podczas pracy z innymi organizacjami, na przykład w celu śledzenia źródła ataku.
- **Pełnoetatowi i niepełnoetatowi członkowie zespołu.** Organizacje z ograniczonymi funduszami, personelem lub potrzebami reagowania na incydenty mogą potrzebować tylko niepełnoetatowych członków zespołu reagowania na incydenty, służącego bardziej jako wirtualny zespół reagowania na incydenty. W sytuacji awaryjnej członkowie zespołu oraz osoby, które mogą im pomóc, szybko są o tym powiadamiani. Istniejąca grupa, taka jak dział pomocy technicznej IT, może działać jako pierwszy punkt kontaktowy w celu zgłaszania incydentów. Członkowie pomocy technicznej mogą zostać przeszkoleni w zakresie przeprowadzania wstępnego dochodzenia i gromadzenia danych, a następnie ostrzegania zespołu reagowania na incydenty, jeśli okaże się, że wystąpił poważny incydent.
- **Morale pracowników.** Reagowanie na incydenty jest bardzo stresujące, podobnie jak obowiązki dyżurne większości członków zespołu. Ta kombinacja sprawia, że członkowie zespołu reagowania na incydenty narażeni są na nadmierny stres. Wiele organizacji będzie również miało trudności ze znalezieniem chętnych, dostępnych, doświadczonych i odpowiednio wykwalifikowanych osób, zwłaszcza w zakresie całodobowego wsparcia. Rozdzielenie ról, w szczególności zmniejszenie ilości pracy administracyjnej, za którą odpowiadają członkowie zespołu, może znacząco podnieść morale.
- **Koszt.** Koszt jest głównym czynnikiem, zwłaszcza jeśli pracownicy mają obowiązek przebywania w lokalizacji organizacji 24 godziny na dobę, 7 dni w tygodniu. Organizacje mogą nie uwzględniać w budżetach kosztów związanych z reagowaniem na incydenty, takich jak zapewnienie funduszy na szkolenia i utrzymanie umiejętności. Ponieważ zespół reagowania na incydenty pracuje z wieloma aspektami IT, jego członkowie potrzebują znacznie szerszej wiedzy niż większość pracowników IT. Muszą także wiedzieć, jak korzystać z narzędzi reagowania na incydenty, takich jak oprogramowanie do informatyki śledczej. Inne koszty, które można przeoczyć, to fizyczne bezpieczeństwo obszarów roboczych zespołu i sposobów komunikacji.

- **Doświadczenie personelu.** Obsługa incydentów wymaga specjalistycznej wiedzy i doświadczenia w kilku obszarach technicznych. Zakres i dogłębność wymaganej wiedzy różni się w zależności od stopnia ryzyka w organizacji. Podwykonawcy mogą posiadać głębszą wiedzę, niż pracownicy organizacji, na temat wykrywania włamań, kryminalistyki, luk w zabezpieczeniach, exploitów[10] i innych aspektów bezpieczeństwa. Ponadto dostawcy usług MSSP mogą być w stanie skorelować zdarzenia występujące wśród klientów tak, aby mogli identyfikować nowe zagrożenia szybciej niż jakikolwiek klient indywidualny. Jednak pracownicy techniczni w organizacji mają zwykle znacznie lepszą wiedzę o środowisku organizacji niż podwykonawcy, co może być korzystne w identyfikowaniu fałszywych alarmów związanych z zachowaniem specyficznym dla organizacji i krytycznością celów. Rozdział 2.4.3 zawiera dodatkowe informacje na temat zalecanych umiejętności członków zespołu.

Rozpatrując podwykonawstwo, organizacje powinny mieć na uwadze następujące kwestie:

- **Obecna i przyszła jakość pracy.** Organizacje powinny brać pod uwagę nie tylko aktualną jakość (zakres i szczegółowość) pracy podwykonawców, ale także wysiłki mające na celu zapewnienie jakości przyszłej pracy - na przykład minimalizowanie rotacji i wypalenia zawodowego oraz zapewnienie solidnego programu szkoleniowego dla nowych pracowników. Organizacje powinny pomyśleć o tym, jak mogłyby obiektywnie ocenić jakość pracy podwykonawcy.
- **Podział obowiązków.** Organizacje często niechętnie udzielają podmiotom zewnętrznym uprawnień do podejmowania decyzji operacyjnych dotyczących środowiska (np. odłączanie serwera WWW). Ważne jest, aby udokumentować odpowiednie działania dla tych punktów decyzyjnych. Na przykład, jeden ze zlecanych modeli rozwiązuje ten problem, zobowiązując zewnętrzny zespół do dostarczenia danych o incydencie do wewnętrznego zespołu organizacji wraz z zaleceniami dotyczącymi dalszej obsługi incydentu. Ostatecznie zespół wewnętrzny podejmuje decyzje operacyjne, a podwykonawca nadal zapewnia wsparcie w razie potrzeby.
- **Wrażliwe informacje ujawnione wykonawcy** Ujawnianie wrażliwych informacji może zostać ograniczone przez podział obowiązków związanych z reagowaniem na incydenty i ograniczenie dostępu do wrażliwych informacji. Na przykład, wykonawca może określić, jaki identyfikator użytkownika został użyty w incydencie (np. ID

[10] Program mający na celu wykorzystanie istniejących błędów w oprogramowaniu.

123456), ale nie wiedzieć, jaka osoba jest powiązana z identyfikatorem użytkownika. Następnie pracownicy mogą przejąć dochodzenie. Umowy o zachowaniu poufności (*ang. Non-Disclosure Agreement - NDA*) są jedną z możliwych opcji ochrony informacji wrażliwych.

- **Brak wiedzy szczegółowej o organizacji.** Dokładna analiza i priorytetyzacja incydentów zależą od konkretnej wiedzy o środowisku organizacji. Organizacja powinna dostarczać podwykonawcy regularnie aktualizowane dokumenty, które określają, jakimi incydentami jest zaniepokojona, które zasoby są krytyczne i jaki powinien być poziom reakcji w różnego rodzaju okolicznościach. Organizacja powinna również zgłaszać wszystkie zmiany i aktualizacje wprowadzone w jej infrastrukturze IT, konfiguracji sieci i systemach. W przeciwnym razie wykonawca musi jak najtrafniej odgadnąć, jak należy postępować z każdym incydentem, co nieuchronnie prowadzi do niewłaściwej obsługi incydentów i frustracji po obu stronach. Brak wiedzy specyficznej dla organizacji może również stanowić problem, gdy reakcja na incydent nie jest zlecana na zewnątrz, jeśli komunikacja między zespołami wewnątrz organizacji jest słaba lub organizacja po prostu nie zbiera niezbędnych informacji.
- **Brak korelacji.** Bardzo ważna jest korelacja między wieloma źródłami danych. Jeśli system wykrywania włamań zarejestruje próbę ataku na serwer WWW, ale zleceniodawca nie ma dostępu do dzienników serwera, może nie być w stanie określić, czy atak się powiódł. Aby być wydajnym, podwykonawca będzie wymagał uprawnień administracyjnych zdalnego dostępu za pośrednictwem bezpiecznego kanału do krytycznych systemów i dzienników urządzeń zabezpieczających. Zwiększy to koszty administracyjne, wprowadzi dodatkowe punkty dostępu i zwiększy ryzyko nieuprawnionego ujawnienia wrażliwych informacji.
- **Obsługa incydentów w wielu lokalizacjach.** Skuteczna reakcja na incydenty często wymaga fizycznej obecności w obiektach organizacji. Jeśli podwykonawca znajduje się poza siedzibą firmy, należy rozważyć, gdzie się znajduje, jak szybko może zapewnić zespół reagowania na incydenty w dowolnym zakładzie i ile to będzie kosztować. Należy rozważyć wizyty na obiekcie organizacji - być może istnieją pewne obiekty lub obszary, w których podwykonawca nie powinien mieć pozwolenia na pracę.
- **Utrzymywanie wewnętrznych umiejętności reagowania na incydenty.** Organizacje, które całkowicie zlecają reagowanie na incydenty na zewnątrz, powinny dążyć do utrzymania w lokalizacji podstawowych umiejętności reagowania na incydenty. Mogą zaistnieć sytuacje, w których podwykonawca jest niedostępny, dlatego organizacja

powinna być przygotowana do prowadzenia własnej obsługi incydentów. Personel techniczny organizacji musi również być w stanie zrozumieć znaczenie, implikacje techniczne i wpływ zaleceń zleceniodawcy.

2.4.3. Personel reagowania na incydent

Za reagowanie na incydenty powinien odpowiadać jeden pracownik z co najmniej jednym wyznaczonym zastępcą. W modelu w pełni zlecanym na zewnątrz, osoba ta nadzoruje i ocenia pracę podwykonawcy. Wszystkie inne modele zazwyczaj mają kierownika zespołu i jednego lub więcej zastępców, którzy przejmują władzę pod nieobecność kierownika zespołu. Kierownicy zwykle wykonują różnorodne zadania, w tym działają jako łącznik z wyższym kierownictwem oraz innymi zespołami i organizacjami, rozładowują sytuacje kryzysowe oraz zapewniają zespołowi niezbędny personel, zasoby i umiejętności. Menedżerowie powinni być biegli technicznie i posiadać doskonałe umiejętności komunikacyjne, w szczególności umiejętność komunikowania się z różnymi grupami odbiorców. Kierownicy są ostatecznie odpowiedzialni za zapewnienie prawidłowego wykonywania działań związanych z reagowaniem na incydenty.

Oprócz kierownika zespołu i jego zastępcy, niektóre zespoły mają również kierownika technicznego - osobę o dużych umiejętnościach technicznych i doświadczeniu w reagowaniu na incydenty, która przejmuje nadzór i ostateczną odpowiedzialność za jakość pracy technicznej zespołu. Pozycji kierownika technicznego nie należy mylić z pozycją kierownika incydentu. Większe zespoły często wyznaczają kierownika incydentu jako główny PoC do obsługi konkretnego incydentu. Kierownik incydentu jest odpowiedzialny za obsługę incydentu. W zależności od wielkości zespołu reagowania na incydenty i skali incydentu, kierownik incydentu może w rzeczywistości nie zajmować się żadną faktyczną obsługą incydentu, ale koordynować działania obsługujące incydent, zbierać informacje od opiekunów, dostarczać aktualizacje incydentów innym grupom oraz upewnić się, że potrzeby zespołu są spełnione.

Członkowie zespołu reagowania na incydenty powinni posiadać doskonałe umiejętności techniczne, takie jak administrowanie systemem, administrowanie siecią, programowanie, wsparcie techniczne lub wykrywanie włamań. Każdy członek zespołu powinien mieć dobre umiejętności rozwiązywania problemów i umiejętność krytycznego myślenia. Nie jest konieczne, aby każdy członek zespołu był ekspertem technicznym - w dużym stopniu będzie to podyktowane względami praktycznymi i finansowymi - ale posiadanie co najmniej jednej wysoce biegłej osoby w każdym głównym obszarze technologii (np. często atakowanych systemów operacyjnych i aplikacji) jest koniecznością. Pomocne może być również, jeśli

niektórzy członkowie zespołu specjalizują się w określonych obszarach technicznych, takich jak wykrywanie włamań do sieci, analiza złośliwego oprogramowania lub kryminalistyka. Często przydatne jest również tymczasowe zatrudnienie specjalistów technicznych, którzy zwykle nie są częścią zespołu.

Ważne jest, aby przeciwdziałać wypaleniu zawodowemu pracowników, zapewniając im możliwości uczenia się i rozwoju. Sugestie dotyczące budowania i utrzymywania umiejętności są następujące:

- Budżetować wystarczające środki, aby utrzymać, wzmocnić i poszerzyć biegłość w obszarach technicznych i bezpieczeństwa, a także mniej technicznych tematach, takich jak prawne aspekty reagowania na incydenty. Powinno to obejmować wysyłanie personelu na konferencje i zachęcanie do udziału w konferencjach zapewnienie dostępności referencji technicznych, które sprzyjają głębszemu zrozumieniu technicznemu, a także okazjonalne zapraszanie ekspertów zewnętrznych (np. wykonawców) posiadających dogłębną wiedzę techniczną w potrzebnych obszarach, o ile pozwala na to finansowanie.
- Zapewnić członkom zespołu możliwości wykonywania innych zadań, takich jak tworzenie materiałów edukacyjnych, prowadzenie warsztatów uświadamiających na temat bezpieczeństwa i prowadzenie badań.
- Rozważać możliwość rotacji członków personelu do i z zespołu reagowania na incydenty oraz uczestniczenia w wymianach, podczas których członkowie zespołu tymczasowo zamieniają się miejscami z innymi (np. administratorami sieci), aby zdobyć nowe umiejętności techniczne.
- Utrzymywać wystarczającą liczbę pracowników, aby członkowie zespołu mogli mieć nieprzerwany czas wolny od pracy (np. urlopy).
- Stworzyć program mentorski, aby starszy personel techniczny mógł pomóc mniej doświadczonemu personelowi w nauce obsługi incydentów.
- Opracować scenariusze obsługi incydentów i poprosić członków zespołu o omówienie, jak by sobie z nimi poradzili. Załącznik A zawiera zestaw scenariuszy i listę pytań do wykorzystania podczas dyskusji nad scenariuszami.

Członkowie zespołu reagowania na incydenty powinni mieć inne umiejętności oprócz wiedzy technicznej. Umiejętności pracy zespołowej mają fundamentalne znaczenie, ponieważ współpraca i koordynacja są niezbędne do skutecznej reakcji na incydent. Każdy członek zespołu powinien mieć również dobre umiejętności komunikacyjne. Umiejętności mówienia

są ważne, ponieważ zespół będzie wchodził w interakcje z wieloma różnymi osobami, a umiejętności pisania są ważne, gdy członkowie zespołu przygotowują porady i procedury. Chociaż nie każdy w zespole musi mieć dobre umiejętności pisania i mówienia, przynajmniej kilka osób w każdym zespole powinno je posiadać, aby zespół mógł dobrze reprezentować się przed innymi.

2.4.4. Współzależność wewnątrz organizacji

Ważne jest, aby zidentyfikować inne grupy w ramach organizacji, które mogą potrzebować uczestniczenia w obsłudze incydentów, tak, aby można było zwrócić się do nich o współpracę, zanim będzie potrzebna. Każdy zespół reagowania na incydenty opiera się na wiedzy, ocenie i umiejętnościach innych, w tym:

- **Kierownictwa.** Kierownictwo ustala politykę reagowania na incydenty, budżet i obsadę personalną. Ostatecznie kierownictwo jest odpowiedzialne za koordynowanie reakcji na incydenty wśród różnych interesariuszy, minimalizowanie szkód i zgłaszanie ich do zespołów reagowania i do innych stron.
- **Pionu ochrony informacji.** Pracownicy ds. bezpieczeństwa informacji mogą być potrzebni na niektórych etapach obsługi incydentów (zapobieganie, powstrzymywanie, eliminowanie i przywracanie) - na przykład do zmiany środków bezpieczeństwa sieci (np. zestawów reguł zapory).
- **Działu wsparcia IT.** Eksperci techniczni IT (np. administratorzy systemów i sieci) nie tylko posiadają niezbędne umiejętności, aby pomagać, ale także zazwyczaj najlepiej rozumieją technologię, którą zarządzają na co dzień. Zrozumienie to może zapewnić podjęcie odpowiednich działań w odniesieniu do systemu, którego dotyczy luka, na przykład odłączenie zaatakowanego systemu.
- **Działu prawnego.** Eksperci prawni powinni przejrzeć plany, zasady i procedury reagowania na incydenty, aby zapewnić ich zgodność z prawem i wytycznymi, w tym z prawem do prywatności. Ponadto należy zasięgnąć porady radcy prawnego lub działu prawnego, jeśli istnieją powody by przypuszczać, że incydent może mieć konsekwencje prawne, w tym zebranie dowodów, wniesienie oskarżenia przeciwko podejrzanemu lub postępowanie sądowe, lub jeśli potrzeba zawarcia porozumienia o współpracy (*ang. Memorandum of Understanding - MOU*) lub innych wiążących umów obejmujących ograniczenia odpowiedzialności za udostępnianie informacji.

- **Działu spraw publicznych i relacji z mediami.** W zależności od charakteru i skutków incydentu może zaistnieć potrzeba poinformowania mediów, a co za tym idzie, opinii publicznej.
- **Działu zasobów ludzkich.** Jeśli podejrzewa się, że pracownik spowodował incydent, może zostać zaangażowany dział kadr - na przykład w celu pomocy w postępowaniu dyscyplinarnym.
- **Działu planowania ciągłości działania.** Organizacje powinny zapewnić, że zasady i procedury reagowania na incydenty oraz procesy ciągłości biznesowej są zsynchronizowane. Incydenty bezpieczeństwa komputerowego podważają stabilność biznesową organizacji. Specjaliści ds. planowania ciągłości działania powinni być świadomi incydentów i ich skutków, aby mogli dopracować oceny wpływu na działalność, oceny ryzyka i plany ciągłości działania. Ponadto, ponieważ planiści ciągłości działania mają rozległą wiedzę w zakresie minimalizowania zakłóceń operacyjnych w trudnych okolicznościach, mogą być cenni w planowaniu reakcji na określone sytuacje, takie jak odmowa świadczenia usługi (*ang. Denial Of Service - DoS*).
- **Bezpieczeństwo fizyczne i zarządzanie obiektami.** Niektóre incydenty związane z bezpieczeństwem komputerowym mają miejsce w wyniku naruszenia bezpieczeństwa fizycznego lub obejmują skoordynowane ataki logiczne i fizyczne. Zespół reagowania na incydenty może również potrzebować dostępu do obiektów podczas obsługi incydentu - na przykład w celu odzyskania zagrożonej stacji roboczej z zamkniętego biura.

2.5. Usługi zespołu reagowania na incydenty

Głównym celem zespołu reagowania na incydenty jest reakcja na incydenty, jednakże rzadko zdarza się, aby zespół reagował tylko na incydenty. Poniżej znajdują się przykłady innych usług, które zespół może oferować:

- **Wykrywanie naruszenia.** Pierwszy poziom zespołu reagowania na incydenty często przejmuje odpowiedzialność za wykrywanie włamań[11]. Zespół generalnie odnosi korzyści, ponieważ będzie przygotowany do szybszej i dokładniejszej analizy

[11] Więcej informacji na temat technologii IDPS (*ang. Intrusion Detection and Prevention Systems*) można znaleźć w publikacji NIST SP 800-94, Przewodnik po systemach wykrywania i zapobiegania włamaniom (IDPS).

incydentów, w oparciu o wiedzę, jaką posiada na temat technologii wykrywania włamań.

- **Dystrybucja porad.** Zespół może wydawać porady w organizacji dotyczące nowych luk i zagrożeń.[12] W stosownych przypadkach do rozpowszechniania informacji należy używać metod zautomatyzowanych, Zalecenia są często najbardziej potrzebne, gdy pojawiają się nowe zagrożenia, takie jak ataki typu phishing np. z zainfekowanymi plikami pdf (pseudo faktury). Tylko jedna grupa w organizacji powinna rozpowszechniać porady dotyczące bezpieczeństwa komputerowego, aby uniknąć powielania wysiłków i rozpowszechniania sprzecznych informacji.
- **Edukacja i świadomość.** Edukacja i świadomość optymalizują zasoby - im więcej użytkownicy i personel techniczny wiedzą o wykrywaniu, raportowaniu i reagowaniu na incydenty, tym mniej obciążony powinien być zespół reagowania na incydenty. Informacje te można przekazywać na wiele sposobów: warsztaty, strony internetowe, biuletyny, plakaty, a nawet naklejki na monitorach i laptopach.
- **Udostępnianie informacji.** Zespoły reagowania na incydenty często uczestniczą w grupach wymiany informacji, takich jak ISAC lub partnerstwa regionalne. W związku z tym zespoły reagowania na incydenty często zarządzają działaniami organizacji w zakresie udostępniania informacji o incydentach, takimi jak agregowanie informacji związanych z incydentami i efektywne udostępnianie tych informacji innym organizacjom, a także zapewnianie, że w ramach organizacji udostępniane są właściwe informacje.

2.6. Rekomendacje

Poniżej podsumowano najważniejsze rekomendacje przedstawione w tej rozdziale, dotyczące organizowania możliwości obsługi incydentów bezpieczeństwa komputerowego.

- **Ustanowienie formalnej zdolności reagowania na incydenty.** Organizacje powinny być przygotowane do szybkiego i skutecznego reagowania w przypadku naruszenia zabezpieczeń komputerowych.

[12] Zespoły powinny publikować porady, aby nie obwiniać żadnej osoby ani organizacji za problemy związane z bezpieczeństwem. Zespoły powinny spotykać się z doradcami prawnymi, aby omówić ewentualną potrzebę wyłączenia odpowiedzialności w poradach, stwierdzając, że zespół i organizacja nie ponoszą odpowiedzialności za dokładność porady. Jest to najbardziej istotne, gdy alerty mogą być wysyłane do wykonawców, dostawców i innych pracowników niebędących pracownikami, którzy są użytkownikami zasobów IT organizacji.

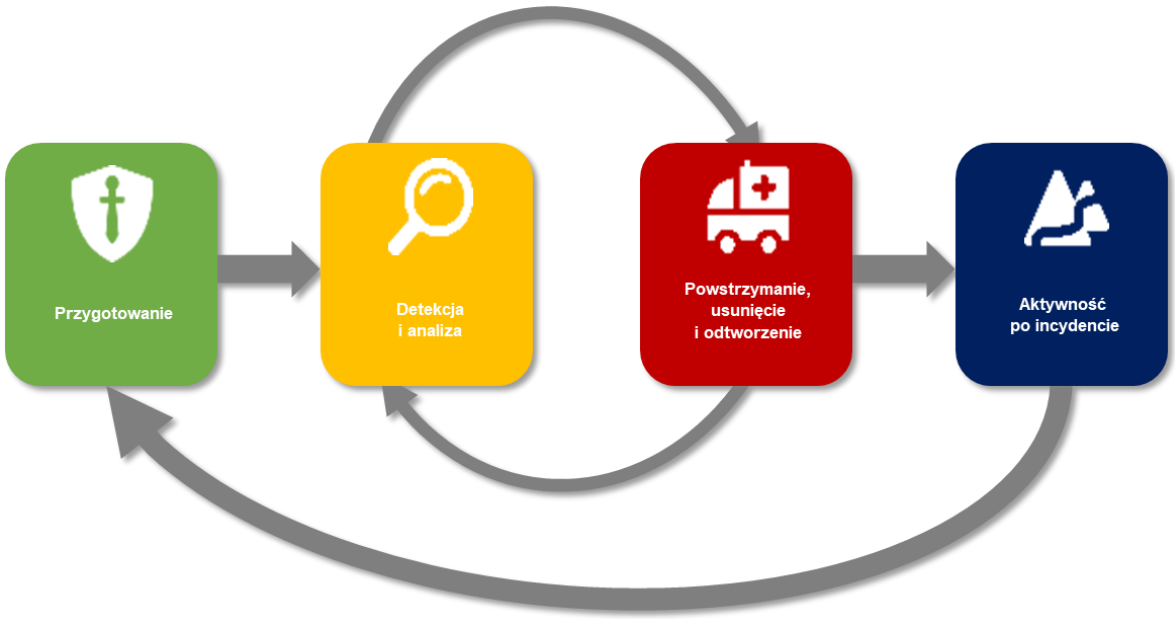
- **Stworzenie zasad reagowania na incydenty.** Polityka reagowania na incydenty jest podstawą programu reagowania na incydenty ustala strukturę organizacyjną reagowania na incydenty, definiuje role i obowiązki oraz wymienia między innymi wymagania dotyczące zgłaszania incydentów.
- **Opracowanie planu reagowania na incydenty w oparciu o zasady reagowania na incydenty.** Plan reagowania na incydenty zawiera plan działań wdrażania programu reagowania na incydenty w oparciu o politykę organizacji. Plan wskazuje zarówno krótko-, jak i długoterminowe cele programu, w tym wskaźniki pomiaru programu. Plan reagowania na incydenty powinien również wskazywać, jak często osoby zajmujące się incydentami powinny być szkolone oraz wymagania dotyczące tych osób.
- **Opracowanie procedury reagowania na incydenty.** Procedury reagowania na incydenty zapewniają szczegółowe kroki reagowania na incydenty. Procedury powinny obejmować wszystkie fazy procesu reagowania na incydenty. Procedury powinny opierać się na polityce i planie reagowania na incydenty.
- **Ustalenie zasad i procedur dotyczących udostępniania informacji związanych z incydentami.** Organizacja powinna przekazywać odpowiednie szczegóły incydentów stronom zewnętrznym, takim jak media, organy ścigania i organizacje zgłaszające incydenty. Zespół reagowania na incydenty powinien omówić to z biurem spraw publicznych organizacji, działem prawnym i kierownictwem w celu ustalenia zasad i procedur dotyczących wymiany informacji. Zespół powinien przestrzegać istniejących zasad organizacji dotyczących interakcji z mediami i innymi podmiotami zewnętrznymi.
- **Przekazywanie odpowiednich informacji o incydentach odpowiedniej organizacji.** Niektóre organizacje są zobowiązane do zgłaszania określonej kategorii incydentów do CSIRT poziomu krajowego. Raportowanie jest korzystne, ponieważ CSIRT wykorzystują zgłoszone dane do dostarczania stronom raportującym informacji o nowych zagrożeniach i trendach incydentów.
- **Uwzględnianie właściwych czynników przy wyborze modelu zespołu reagowania na incydenty.** Organizacje powinny dokładnie rozważyć zalety i wady każdego możliwego modelu struktury zespołu i modelu personelu w kontekście potrzeb organizacji i dostępnych zasobów.
- **Wybór osób z odpowiednimi umiejętnościami do zespołu reagowania na incydenty.** Wiarygodność i biegłość zespołu zależą w dużej mierze od umiejętności technicznych

i zdolności krytycznego myślenia jego członków. Krytyczne umiejętności techniczne obejmują administrowanie systemem, administrowanie siecią, programowanie, wsparcie techniczne i wykrywanie włamań. Do efektywnej obsługi incydentów potrzebne są również umiejętności pracy zespołowej i komunikacji. Wszystkim członkom zespołu należy zapewnić niezbędne szkolenie.

- **Identyfikacja innych grup w organizacji, które mogą uczestniczyć w obsłudze incydentu.** Każdy zespół reagowania na incydenty opiera się na wiedzy, osądzie i umiejętnościach innych zespołów, w tym na zarządzaniu, zabezpieczaniu informacji, wsparciu IT, prawach, sprawach publicznych i zarządzaniu obiektami.
- **Określenie, jakie usługi powinien oferować zespół.** Chociaż głównym celem zespołu jest reagowanie na incydenty, większość zespołów wykonuje dodatkowe funkcje. Przykłady obejmują monitorowanie czujników wykrywających włamania, rozpowszechnianie porad dotyczących bezpieczeństwa i edukowanie użytkowników w zakresie bezpieczeństwa.

3. OBSŁUGA INCYDENTU

Proces reakcji na incydent składa się z kilku faz. Faza początkowa obejmuje utworzenie i szkolenie zespołu reagowania na incydenty oraz pozyskanie niezbędnych narzędzi i zasobów. Przygotowując się, organizacja stara się również ograniczyć liczbę incydentów, które wystąpią, wybierając i wdrażając zestaw zabezpieczeń opartych na wynikach ocen ryzyka. Jednak nawet po wdrożeniu środków bezpieczeństwa pozostaje ryzyko szczątkowe. Wykrywanie naruszeń bezpieczeństwa jest zatem niezbędne, aby zaalarmować organizację o każdym zdarzeniu. Mając na uwadze powagę incydentu, organizacja może złagodzić skutki incydentu poprzez jego powstrzymanie i ostateczną odbudowę po nim. Na tym etapie działania, organizacje często wracają do wykrywania i analizy - na przykład w celu sprawdzenia, czy dodatkowe hosty są zainfekowane przez złośliwe oprogramowanie podczas usuwania incydentu ze złośliwym oprogramowaniem. Po odpowiednim rozwiązaniu incydentu organizacja opracowuje raport, w którym wyszczególnia przyczynę i koszt incydentu oraz kroki, jakie organizacja powinna podjąć, aby zapobiec incydentom w przyszłości. W tej rozdziale opisano szczegółowo główne etapy procesu reagowania na incydenty - przygotowanie, wykrywanie, analizę, powstrzymywanie, eliminację i odzyskiwanie oraz działania po incydencie. Rysunek 3-1 ilustruje cykl życia reakcji na incydent.



Rysunek 3-1. Cykl życia reakcji na incydent.

3.1. Przygotowanie

Metodologie reagowania na incydenty zwykle kładą nacisk na przygotowanie - nie tylko ustanawianie zdolności reagowania na incydent, aby organizacja była gotowa do reagowania na incydent, ale także zapobieganie incydentom poprzez zapewnienie, że systemy, sieci i aplikacje są wystarczająco bezpieczne. Chociaż zespół reagowania na incydenty zazwyczaj nie jest odpowiedzialny za zapobieganie incydentom, ma on fundamentalne znaczenie dla powodzenia programów reagowania na incydenty. Ta Rozdział zawiera podstawowe porady dotyczące przygotowań do obsługi incydentów i zapobiegania incydentom.

3.1.1. Przygotowanie do obsługi incydentu

Poniższe listy zawierają przykłady dostępnych narzędzi i zasobów, które mogą być przydatne podczas obsługi incydentów. Listy te mogą być punktem wyjścia do dyskusji o tym, jakich narzędzi i zasobów potrzebują osoby obsługujące incydenty w organizacji. Na przykład, smartfony są jednym ze sposobów na zapewnienie elastycznych mechanizmów komunikacji

i koordynacji w sytuacjach kryzysowych. Organizacja powinna mieć wiele (oddzielnych i różnych) środków komunikacji i koordynacji na wypadek awarii jednego mechanizmu.

Komunikacja i urządzenia do obsługi incydentów:

- **Dane kontaktowe** członków zespołu i innych osób w organizacji i poza nią (głównych i zapasowych osób kontaktowych), takich jak organy ścigania i inne zespoły reagowania na incydenty. Informacje mogą obejmować numery telefonów, adresy e-mail, publiczne klucze do szyfrowania (zgodnie z oprogramowaniem szyfrującym opisanym poniżej) oraz instrukcje dotyczące weryfikacji tożsamości kontaktu
- **Informacje o dyżurach** dla innych zespołów w organizacji, w tym informacje o eskalacji.
- **Sposoby zgłaszania incydentów**, takie jak numery telefonów, adresy e-mail, formularze online i bezpieczne systemy komunikatorów internetowych, których użytkownicy mogą używać do zgłaszania podejrzanych incydentów. Co najmniej jeden mechanizm powinien umożliwiać anonimowe zgłaszanie incydentów.
- **System monitorowania spraw** do śledzenia informacji o incydentach, statusu itp.
- **Smartfony**, używane przez członków zespołu poza godzinami pracy oraz do komunikacji w miejscu pracy.
- **Oprogramowanie szyfrujące** używane do komunikacji między członkami zespołu, wewnątrz organizacji i stronami zewnętrznymi.
- **Centrum kierowania** dla centralnej komunikacji i koordynacji. Jeśli stałe centrum kierowania jest zbędne lub niepraktyczne, zespół powinien stworzyć procedurę rezerwowania pomieszczenia tymczasowego centrum kierowania w przypadku wystąpienia takiej potrzeby.
- **Bezpieczne magazyn** do przechowywania dowodów i innych wrażliwych materiałów

Sprzęt i oprogramowanie do analizy incydentów:

- **Stacje robocze[13] do informatyki śledczej i/lub urządzenia do tworzenia kopii zapasowych** w celu tworzenia obrazów dysków, zachowywania plików dziennika i zapisywania innych istotnych danych dotyczących incydentów.

[13] Stacje robocze do informatyki śledczej zostały specjalnie zaprojektowane, aby pomóc osobom zajmującym się incydentami w pozyskiwaniu i analizowaniu danych. Te stacje robocze zazwyczaj zawierają zestaw wymiennych dysków twardych, których można używać do przechowywania dowodów.

- **Laptopy** do analizy danych, przechwytywania pakietów i pisania raportów.
- **Zapasowe stacje robocze, serwery i sprzęt sieciowy lub zwirtualizowane odpowiedniki**, które mogą być używany do wielu celów, takich jak przywracanie kopii zapasowych i testowanie złośliwego oprogramowania.
- **Czyste nośniki wymienne.**
- **Przenośna drukarka** do drukowania kopii plików dziennika i innych dowodów z systemów niezwiązanych z siecią.
- **Sniffery[14] pakietów i analizatory protokołów** do przechwytywania i analizowania ruchu sieciowego.
- **Oprogramowanie do informatyki śledczej** do analizy obrazów dysków.
- **Nośniki wymienne** z zaufanymi wersjami programów, które mają być używane do gromadzenia dowodów z systemów.
- **Akcesoria do gromadzenia dowodów**, w tym notatniki w twardej oprawie, aparaty cyfrowe, nagrywarki audio, formularze kontroli pochodzenia produktu, torby i etykiety do przechowywania dowodów oraz taśma dowodowa, celem zachowania dowodów w razie podjęcia działań prawnych.

Zasoby do analizy incydentów:

- **Listy portów**, w tym najczęściej używane porty i porty koni trojańskich.
- **Dokumentacja systemów operacyjnych**, aplikacji, protokołów oraz produktów do wykrywania włamań i programów antywirusowych.
- **Diagramy sieciowe i listy krytycznych zasobów**, takich jak serwery baz danych.
- **Bieżące poziomy podstawowe** oczekiwanej aktywności sieci, systemu i aplikacji.
- **Kryptograficzne hashe** krytycznych plików[15] w celu przyspieszenia analizy, weryfikacji i usuwania incydentów.

Oprogramowanie do łagodzenia skutków incydentów:

[14] Program komputerowy lub urządzenie, którego zadaniem jest przechwytywanie i ewentualnie analizowanie danych przepływających w sieci.

[15] Projekt National Software Reference Library (NSRL) prowadzi zapisy skrótów różnych plików, w tym systemu operacyjnego, aplikacji i plików graficznych. Skrót można pobrać ze strony http://www.nsrl.nist.gov/.

- **Dostęp do obrazów** „czystego: systemu operacyjnego i instalacji aplikacji w celu przywracania i odzyskiwania systemu.

Wiele zespołów reagowania na incydenty tworzy *zestaw startowy*, który jest przenośną walizką zawierającą materiały, które mogą być potrzebne podczas śledztwa. Zestaw startowy powinien być zawsze gotowy do użycia. Zestawy startowe zawierają wiele takich samych elementów, jak wymienione na powyższych listach punktowanych. Na przykład, każdy zestaw startowy zazwyczaj zawiera laptop z odpowiednim oprogramowaniem (np. snifferami pakietów, informatyki śledczej). Inne ważne materiały obejmują urządzenia do tworzenia kopii zapasowych, czyste nośniki oraz podstawowy sprzęt i kable sieciowe. Ponieważ celem posiadania zestawu startowego jest ułatwienie szybszych odpowiedzi, zespół powinien unikać pożyczania przedmiotów z zestawu.

Każda osoba obsługująca incydent powinna mieć dostęp do co najmniej dwóch urządzeń komputerowych (np. laptopów). Jeden, taki jak ten z zestawu startowego, powinien być używany do wykrywania pakietów, analizy złośliwego oprogramowania i wszystkich innych działań, które mogą spowodować skażenie laptopa wykonującego te operacje. Laptop powinien zostać wyczyszczony, a całe oprogramowanie ponownie zainstalowane, zanim zostanie użyty do obsługi innego incydentu. Należy pamiętać, że jest to laptop specjalnego przeznaczenia i prawdopodobnie będzie używał oprogramowania innego niż standardowe narzędzia i konfiguracje przedsiębiorstwa, a jeśli to możliwe, osoby zajmujące się obsługą incydentów powinny mieć możliwość określenia podstawowych wymagań technicznych dla tych specjalnego przeznaczenia laptopów dochodzeniowych. Oprócz laptopa do śledztwa, każda osoba zajmująca się incydentem powinna mieć również standardowy laptop, smartfon lub inne urządzenie komputerowe do pisania raportów, czytania wiadomości e-mail i wykonywania innych obowiązków niezwiązanych z praktyczną analizą incydentów.

Ćwiczenia obejmujące symulowane incydenty mogą być również bardzo przydatne w przygotowaniu personelu do obsługi incydentów.

3.1.2. Zapobieganie incydentom

Utrzymywanie liczby incydentów na odpowiednio niskim poziomie jest bardzo ważne dla ochrony procesów biznesowych organizacji. Jeśli środki bezpieczeństwa są niewystarczające, może dojść do większej liczby incydentów, przytłaczających zespół reagowania na incydenty. Może to prowadzić do powolnych i niepełnych odpowiedzi, co przekłada się na większy negatywny wpływ na biznes (np. większe szkody, dłuższe okresy niedostępność usług i danych).

Niniejszy dokument nie obejmuje konkretnych porad dotyczących zabezpieczania sieci, systemów i aplikacji. Chociaż zespoły reagowania na incydenty generalnie nie są odpowiedzialne za zabezpieczanie zasobów, mogą być zwolennikami rozsądnych praktyk bezpieczeństwa. Zespół reagowania na incydenty może być w stanie zidentyfikować problemy, istnienia których organizacja nie byłaby świadoma. Zespół może odegrać kluczową rolę w ocenie ryzyka i szkoleniu poprzez identyfikację luk. Istnieją inne dokumenty zawierające porady dotyczące ogólnych koncepcji bezpieczeństwa oraz wytycznych dotyczących systemu operacyjnego i aplikacji[16]. Poniższe rozważania zawierają krótki przegląd niektórych głównych zalecanych praktyk zabezpieczania sieci, systemów i aplikacji:

- **Szacowanie ryzyka.** Okresowe oceny ryzyka systemów i aplikacji powinny określać, jakie ryzyka stwarzają kombinacje zagrożeń i podatności.[17] Powinno obejmować to zrozumienie odpowiednich zagrożeń, w tym zagrożeń specyficznych dla organizacji. Każdemu ryzyku należy nadać priorytet, a ryzyko można ograniczać, przenosić lub akceptować do czasu osiągnięcia akceptowalnego ogólnego poziomu ryzyka. Kolejną korzyścią wynikającą z regularnego przeprowadzania ocen ryzyka jest identyfikacja krytycznych zasobów, co pozwala personelowi na zwrócenie uwagi na monitorowanie i reagowanie na te zasoby.[18]
- **Bezpieczeństwo hosta.** Wszystkie hosty powinny być odpowiednio zabezpieczone przy użyciu standardowych konfiguracji. Oprócz utrzymywania każdego hosta odpowiednio zaktualizowanego za pomocą poprawek, hosty powinny być skonfigurowane zgodnie z zasadą najniższych uprawnień - przyznając użytkownikom tylko te uprawnienia, które są niezbędne do wykonywania ich autoryzowanych zadań. Hosty powinny mieć włączone przeprowadzanie audytu i powinny rejestrować istotne zdarzenia związane z bezpieczeństwem.[19] Bezpieczeństwo hostów i ich konfiguracji powinno być stale monitorowane. Wiele organizacji korzysta z list kontrolnych konfiguracji systemu operacyjnego i aplikacji wyrażonych w protokołach

[16] Przykładowo: http://csrc.nist.gov/publications/PubsSPs.html zawiera łącza do standardów cyberbezpieczeństwa dotyczących bezpieczeństwa informacji, które obejmują dokumenty dotyczące systemów operacyjnych i podstawowych zasad bezpieczeństwa aplikacji.

[17] Wytyczne dotyczące oceny ryzyka są dostępne w NSC 800-30, Przewodnik dotyczący postępowania w zakresie szacowania ryzyka w podmiotach realizujących zadania publiczne.

[18] Informacje na temat identyfikowania krytycznych zasobów zawarte są w NSC 199, Standardy kategoryzacji bezpieczeństwa.

[19] Aby uzyskać więcej informacji na temat ciągłego monitorowania, zobacz publikację NIST SP SP 800-137, Ciągłość monitorowania bezpieczeństwa informacji.

Security Content Automation Protocols (SCAP)[20], aby pomóc w spójnym i skutecznym zabezpieczaniu hostów.[21]

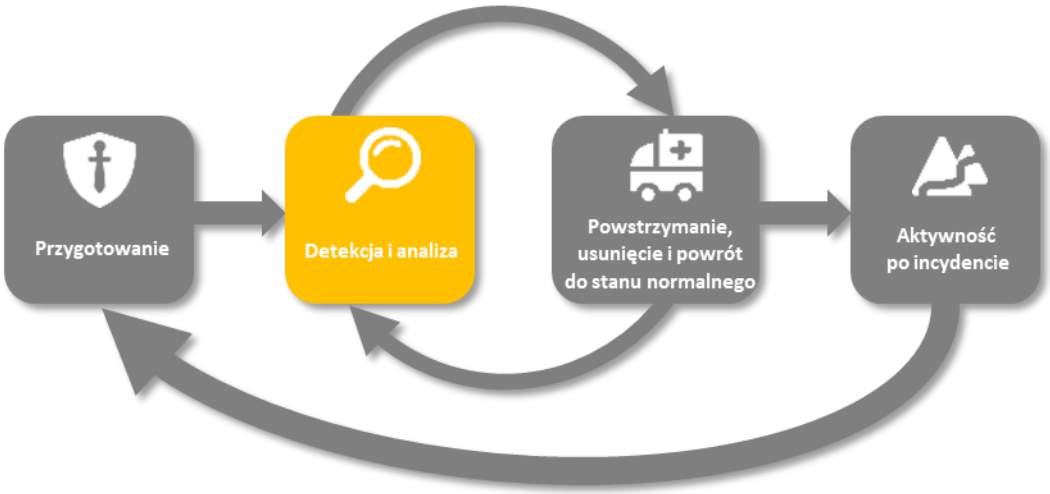
- **Bezpieczeństwo sieci.** Sieć powinna być skonfigurowana tak, aby odmawiała wszelkiej aktywności, która nie jest wyraźnie dozwolona. Obejmuje to zabezpieczenie wszystkich punktów połączeń, takich jak wirtualne sieci prywatne (VPN) i dedykowane połączenia z innymi organizacjami.
- **Zapobieganie złośliwemu oprogramowaniu.** Oprogramowanie do wykrywania i powstrzymywania złośliwego oprogramowania powinno być wdrażane w całej organizacji. Ochrona przed złośliwym oprogramowaniem powinna być wdrażana na poziomie hosta (np. systemów operacyjnych serwerów i stacji roboczych), na poziomie serwera aplikacji (np. serwera poczty elektronicznej, serwerów proxy) i na poziomie klienta aplikacji (np. klientów poczty e-mail, komunikatorów internetowych).[22]
- **Świadomość i szkolenie użytkowników.** Użytkownicy powinni być świadomi zasad i procedur dotyczących właściwego korzystania z sieci, systemów i aplikacji. Zatwierdzone wnioski z poprzednich incydentów należy również udostępnić użytkownikom, aby mogli zobaczyć, jak ich działania mogą wpłynąć na organizację. Poprawa świadomości użytkowników w zakresie incydentów powinna zmniejszyć częstotliwość incydentów. Personel IT powinien zostać przeszkolony, aby mógł utrzymywać swoje sieci, systemy i aplikacje zgodnie ze standardami bezpieczeństwa organizacji.

[20] Więcej informacji na temat SCAP można znaleźć w publikacji NIST SP 800-117 Revision 1, Guide to Adopting and Using the Security Content Automation Protocol (SCAP) w wersji 1.2, https://csrc.nist.gov/search?keywords=800-117

[21] Repozytorium list kontrolnych bezpieczeństwa można znaleźć pod przykładowym adresem http://checklists.nist.gov/

[22] Więcej informacji na temat zapobiegania złośliwemu oprogramowaniu można znaleźć w publikacji NIST SP 800-83, Przewodnik dotyczący zapobiegania i postępowania z incydentami związanymi ze złośliwym oprogramowaniem, pod adresem: https://csrc.nist.gov/search?keywords=800-83

3.2. Detekcja i analiza



Rysunek 3-2. Cykl obsługi incydentu (Detekcja i analiza).

3.2.1. Wektory ataku

Incydenty mogą wystąpić na niezliczone sposoby, więc nie jest możliwe opracowanie szczegółowych instrukcji postępowania w przypadku każdego incydentu. Organizacje powinny być ogólnie przygotowane do obsługi każdego incydentu, jednakże powinny skupić się na przygotowaniu do obsługi incydentów wykorzystujących typowe wektory ataku. Różne rodzaje incydentów wymagają różnych strategii reagowania. Wymienione poniżej wektory ataków nie mają na celu zapewnienia ostatecznej klasyfikacji incydentów. Wymieniają typowe metody ataków, które można wykorzystać jako podstawę do zdefiniowania bardziej szczegółowych procedur postępowania.

- **Nośniki zewnętrzne / wymienne:** Atak z wykorzystaniem nośnika wymiennego lub urządzenia peryferyjnego - na przykład złośliwy kod rozprzestrzeniający się na system z zainfekowanego dysku flash USB.
- **Wyniszczanie**: Atak wykorzystujący metody brutalnej siły (*ang. brute force*)w celu złamania, degradacji lub zniszczenia systemów, sieci lub usług (np. DDoS, którego celem jest utrudnienie lub odmowa dostępu do usługi lub aplikacji; atak brutalnej siły

(*brute force)* na mechanizm uwierzytelniania, taki jak jako hasła, uwierzytelnianie typu wywołanie – reakcja (*ang. CAPTCHAS*[23]) lub podpisy cyfrowe).

- **WEB:** Atak przeprowadzony z witryny internetowej lub aplikacji internetowej - na przykład atak z użyciem skryptów między witrynami (*ang. cross-site scripting)* używany do kradzieży poświadczeń lub przekierowania do witryny wykorzystującej lukę w zabezpieczeniach przeglądarki i instalującej złośliwe oprogramowanie.
- **E-mail:** Atak przeprowadzony za pośrednictwem wiadomości e-mail lub załącznika - na przykład wykorzystanie kodu zamaskowanego jako załączony dokument lub łącze do złośliwej witryny w treści wiadomości e-mail.
- **Podszywanie się:** Atak polegający na zamianie czegoś niegroźnego na coś złośliwego - na przykład podszywanie się (*spoofing*), ataki typu *man in the middle*, nieautoryzowane punkty dostępu bezprzewodowego i ataki typu *SQL injection* - wszystkie obejmują podszywanie się.
- **Niewłaściwe użytkowanie:** Wszelkie incydenty wynikające z naruszenia zasad dopuszczalnego użytkowania organizacji przez autoryzowanego użytkownika, z wyłączeniem powyższych kategorii, na przykład użytkownik instaluje oprogramowanie do udostępniania plików, co prowadzi do utraty wrazliwych danych; lub użytkownik wykonuje nielegalne działania w systemie.
- **Utrata lub kradzież sprzętu:** Utrata lub kradzież urządzenia komputerowego lub nośnika używanego przez organizację, takiego jak laptop, smartfon lub token uwierzytelniający.
- **Inne:** Atak, który nie pasuje do żadnej z pozostałych kategorii.

Ta Rozdział koncentruje się na zalecanych praktykach postępowania w przypadku każdego rodzaju incydentu. Udzielanie szczegółowych porad opartych na wektorach ataku wykracza poza zakres niniejszej publikacji. Takie wytyczne mogą być zawarte w oddzielnych publikacjach dotyczących innych zagadnień związanych z obsługą incydentów, takich jak NIST SP 800-83 dotyczący zapobieganiu i postępowaniu ze złośliwym oprogramowaniem.

[23] CAPTCHA polega na wyświetlaniu prośby o wykonanie prostego testu potwierdzającego, że jesteś człowiekiem, a nie komputerem próbującym włamać się na konto chronione hasłem. Test CAPTCHA składa się z dwóch prostych elementów: zniekształconego obrazu z losowo wygenerowaną sekwencją liter i/lub liczb oraz pola tekstowego. Aby pomyślnie przejść test i potwierdzić, że jesteś człowiekiem, należy wpisać w polu tekstowym znaki widoczne na obrazie.

3.2.2. Oznaki incydentu

Dla wielu organizacjach najtrudniejszą częścią procesu reagowania na incydenty jest precyzyjne wykrywanie i ocena ewentualnych incydentów - ustalanie czy zdarzenie miało miejsce, a jeśli tak, to jakiego rodzaju, w jakim zakres i jakiej skali. To, co sprawia, że jest to tak trudne, to połączenie trzech czynników:

- Incydenty można wykrywać na wiele różnych sposobów, z różnym poziomem szczegółowości i wierności. Funkcje automatycznego wykrywania obejmują identyfikatory IDPS oparte na sieciach i hostach, oprogramowanie antywirusowe i analizatory dzienników. Incydenty można również wykrywać ręcznie, na przykład problemy zgłaszane przez użytkowników. Niektóre incydenty mają widoczne oznaki, które można łatwo wykryć, podczas gdy inne są prawie niemożliwe do wykrycia.
- Liczba potencjalnych oznak incydentów jest zazwyczaj duża - na przykład często organizacja otrzymuje tysiące, a nawet miliony alertów czujników wykrywania włamań dziennie. (Aby uzyskać informacje na temat analizy takich ostrzeżeń, patrz Rozdział 3.2.4).
- Dogłębna, specjalistyczna wiedza techniczna i duże doświadczenie są niezbędne do prawidłowej i skutecznej analizy danych związanych ze zdarzeniami.

Oznaki incydentu należą do jednej z dwóch kategorii: zwiastunów i wskaźników. Zwiastun to sygnał, że w przyszłości może dojść do incydentu. Wskaźnik to sygnał, że incydent mógł mieć lub może mieć miejsce w tym momencie.

Większość ataków nie ma żadnych możliwych do zidentyfikowania ani wykrywalnych zwiastunów z punktu widzenia celu. W przypadku wykrycia zwiastunów, organizacja może mieć możliwość zapobieżenia incydentowi poprzez zmianę swojego stanu bezpieczeństwa, aby uchronić cel przed atakiem. Organizacja może przynajmniej dokładniej monitorować działania angażujące cel. Przykładami zwiastunów są:

- Wpisy dziennika serwera sieci web, które pokazują użycie skanera luk w zabezpieczeniach.
- Ogłoszenie o nowym programie wykorzystującym luki (exploicie), który wykorzystuje lukę w zabezpieczeniach serwera e-mail organizacji.
- Zagrożenie ze strony grupy stwierdzającej, że grupa ta zaatakuje organizację.

Chociaż zwiastuny są stosunkowo rzadkie, wskaźniki są zbyt powszechne. Istnieje zbyt wiele rodzajów wskaźników, aby je wyczerpująco wymienić, ale poniżej podano kilka przykładów:

- Detektor wykrywania włamań do sieci ostrzega, gdy na serwerze bazy danych występuje próba przepełnienia bufora.
- Oprogramowanie antywirusowe ostrzega, gdy wykryje, że host jest zainfekowany złośliwym oprogramowaniem.
- Administrator systemu widzi nazwę pliku zawierającą nietypowe znaki.
- Host rejestruje zmianę konfiguracji audytu w swoim dzienniku logów.
- Aplikacja rejestruje wiele nieudanych prób logowania z nieznanego systemu zdalnego.
- Administrator poczty e-mail widzi dużą liczbę odrzuconych wiadomości e-mail o podejrzanej zawartości.
- Administrator sieci wykrywa nietypowe odchylenie od typowego ruchu w sieci.

3.2.3. Źródła zwiastunów i wskaźników

Zwiastuny i *wskaźniki* są identyfikowane przy użyciu wielu różnych źródeł, z których najczęstsze to alerty oprogramowania zabezpieczającego komputer, dzienniki, publicznie dostępne informacje i obywatele. Tabela 3-1 zawiera listę wspólnych źródeł zwiastunów i wskaźników dla każdej kategorii.

Tabela 3-1. Główne źródła zwiastunów i wskaźników

Źródło	Opis
Alerty	
IDPS	Produkty IDPS identyfikują podejrzane zdarzenia i rejestrują dotyczące ich istotne dane, w tym datę i godzinę wykrycia ataku, typ ataku, źródłowy i docelowy adres IP oraz nazwę użytkownika (jeśli ma to zastosowanie i jest znana). Większość produktów IDPS wykorzystuje sygnatury ataków do identyfikacji złośliwej aktywności. Sygnatury muszą być aktualizowane, aby można było wykryć najnowsze ataki. Oprogramowanie IDPS często generuje fałszywe alarmy - alerty

Źródło	Opis
	wskazujące na złośliwą aktywność, podczas gdy w rzeczywistości jej nie było. Analitycy powinni ręcznie weryfikować alerty IDPS, dokładnie przeglądając zarejestrowane dane pomocnicze lub pobierając powiązane dane z innych źródeł.[24]
Zarządzanie informacją i zdarzeniami bezpieczeństwa	Produkty SIEM (*ang. Security Information and Event Management)* są podobne do produktów IDPS, ale generują alerty w oparciu o analizę danych dziennika (patrz poniżej).
Oprogramowanie antywirusowe i antyspamowe	Oprogramowanie antywirusowe wykrywa różne formy złośliwego oprogramowania, generuje alerty i zapobiega infekowaniu hostów przez złośliwe oprogramowanie. Obecne produkty antywirusowe skutecznie zatrzymują wiele przypadków złośliwego oprogramowania, jeśli ich sygnatury są aktualne. Oprogramowanie antyspamowe służy do wykrywania spamu i zapobiegania jego dotarciu do skrzynek pocztowych użytkowników. Spam może zawierać złośliwe oprogramowanie, ataki phishingowe i inną złośliwą zawartość, więc alerty oprogramowania antyspamowego mogą wskazywać na próby ataku.
Oprogramowanie sprawdzające integralność plików	Oprogramowanie do sprawdzania integralności plików może wykrywać zmiany wprowadzone w ważnych plikach podczas incydentów. Wykorzystuje algorytm haszowania, aby uzyskać kryptograficzną sumę kontrolną dla każdego wyznaczonego pliku. Jeśli plik zostanie zmieniony, a suma kontrolna zostanie ponownie obliczona, istnieje bardzo duże prawdopodobieństwo, że nowa suma kontrolna nie będzie pasować do starej sumy kontrolnej. Regularne przeliczanie sum kontrolnych i porównywanie ich z poprzednimi wartościami pozwala wykryć zmiany w plikach.

[24] Dodatkowe informacje o produktach IDPS można znaleźć w NIST SP 800-94, *Przewodnik po systemach wykrywania i zapobiegania włamaniom*

Źródło	Opis
Zewnętrzne usługi monitorowania	Firmy zewnętrzne oferują różnorodne bezpłatne usługi monitorowania oparte na subskrypcji. Przykładem są usługi wykrywania oszustw, które powiadamiają organizację, jeśli jej adresy IP, nazwy domen itp. są powiązane z bieżącą aktywnością incydentów z udziałem innych organizacji. Istnieją również bezpłatne czarne listy czasu rzeczywistego, zawierające podobne informacje. Innym przykładem zewnętrznej usługi monitorowania jest lista powiadomień CSIRC. Listy te są często dostępne tylko dla innych zespołów reagowania na incydenty.
Logi	
Logi systemu operacyjnego, usług i aplikacji	Dzienniki z systemów operacyjnych, usług i aplikacji (szczególnie dane związane z audytem) często mają dużą wartość, gdy wystąpi incydent, na przykład rejestrowanie, do których kont uzyskano dostęp i jakie działania zostały wykonane. Organizacje powinny wymagać podstawowego poziomu rejestrowania (*ang. baseline level*) we wszystkich systemach i wyższego poziomu (*ang. higher baseline level*) w systemach krytycznych. Dzienniki mogą służyć do analizy poprzez korelowanie informacji o zdarzeniach. W zależności od informacji o zdarzeniu, można wygenerować alert w celu wskazania incydentu. Rozdział 3.2.4 omawia wartość scentralizowanego rejestrowania.
Logi urządzeń sieciowych	Dzienniki z urządzeń sieciowych, takich jak zapory i routery, nie są zwykle głównym źródłem zwiastunów ani wskaźników. Chociaż te urządzenia są zwykle skonfigurowane do rejestrowania zablokowanych prób połączenia, dostarczają niewiele informacji o naturze działania. Mimo to mogą być cenne w identyfikowaniu trendów sieciowych i korelowaniu zdarzeń wykrytych przez inne urządzenia.
Ruch sieciowy	Ruch sieciowy to określona sesja komunikacyjna zachodząca między hostami. Routery i inne urządzenia sieciowe mogą dostarczać informacji o przepływie ruchu sieciowego, które można wykorzystać do wykrycia anomalnej aktywności sieciowej spowodowanej przez złośliwe oprogramowanie, eksfiltrację danych i inne złośliwe działania.

Źródło	Opis
	Istnieje wiele standardów formatów danych przepływu, w tym NetFlow, sFlow i IPFIX.
Publicznie dostępne informacje	
Informacje o nowych podatnościach i exploitach	Bieżące śledzenie informacji o nowych lukach i programach je wykorzystujących, może zapobiec występowaniu niektórych incydentów i pomóc w wykrywaniu i analizowaniu nowych ataków. zawiera informacje o lukach w zabezpieczeniach. Zespoły CSIRT poziomy krajowego dostarczają informacje o aktualizacjach zagrożeń za pośrednictwem instruktaży, publikacji internetowych i list mailingowych.
Obywatele	
Osoby z organizacji	Użytkownicy, administratorzy systemu, administratorzy sieci, pracownicy ochrony i inne osoby z organizacji mogą zgłaszać oznaki incydentów. Ważne jest, aby zweryfikować wszystkie takie raporty. Jednym ze sposobów jest zapytanie osób, które dostarczają takie informacje, na ile są pewni ich dokładności. Rejestrowanie tego oszacowania wraz z dostarczonymi informacjami może znacznie pomóc podczas analizy incydentów, szczególnie w przypadku wykrycia sprzecznych danych.
Osoby z innych organizacji	Zgłoszenia incydentów pochodzących z zewnątrz należy traktować z należytą powagą. Na przykład, z organizacją może się skontaktować strona twierdząca, że system organizacji atakuje jej systemy. Użytkownicy zewnętrzni mogą również zgłaszać inne wskaźniki, takie jak zniszczona strona internetowa lub niedostępna usługa. Inne zespoły reagowania na incydenty również mogą zgłaszać incydenty. Ważne jest, aby istniały mechanizmy umożliwiające podmiotom zewnętrznym zgłaszanie wskaźników, a przeszkolony personel uważnie monitorował te mechanizmy. Powinno to być tak proste, jak skonfigurowanie numeru telefonu i adresu e-mail do przekazywania wiadomości do działu pomocy.

3.2.4. Analiza incydentów

Wykrywanie i analiza incydentów byłyby łatwe, gdyby gwarantowano dokładność każdego zwiastuna lub wskaźnika; niestety w praktyce tak nie jest. Na przykład, wskaźniki podane przez użytkownika, takie jak zgłoszenie dotyczące niedostępności serwera, są często nieprawidłowe. Systemy wykrywania włamań mogą generować fałszywe alarmy - nieprawidłowe wskaźniki. Te przykłady pokazują, co sprawia, że wykrywanie i analiza incydentów są tak trudne: najlepiej byłoby, gdyby każdy wskaźnik został sprawdzony w celu ustalenia, czy jest on uzasadniony. Co gorsza, całkowita liczba wskaźników może wynosić tysiące lub miliony dziennie. Znalezienie rzeczywistych incydentów bezpieczeństwa, które wystąpiły na podstawie wszystkich wskaźników, może być trudnym zadaniem.

Nawet jeśli wskaźnik jest dokładny, niekoniecznie oznacza to, że wystąpił incydent. Niektóre wskaźniki, takie jak awaria serwera lub modyfikacja plików krytycznych, mogą wystąpić z kilku powodów innych niż incydent związany z bezpieczeństwem, w tym błąd ludzki. Biorąc jednak pod uwagę wystąpienie przesłanek, uzasadnione jest podejrzenie, że może wystąpić incydent, i podjęcie odpowiednich działań. Określenie, czy dane zdarzenie jest rzeczywiście incydentem, jest czasami kwestią oceny. W celu podjęcia decyzji może być konieczna współpraca z innymi pracownikami technicznymi i bezpieczeństwa informacji. W wielu przypadkach sytuacja powinna być traktowana w ten sam sposób, niezależnie od tego, czy jest ona związana z bezpieczeństwem. Na przykład, jeśli organizacja traci łączność z Internetem co 12 godzin i nikt nie zna przyczyny, pracownicy chcieliby równie szybko rozwiązać problem i wykorzystaliby te same zasoby do zdiagnozowania problemu, niezależnie od jego przyczyny.

Niektóre incydenty są łatwe do wykrycia, na przykład ewidentnie zniszczona strona internetowa. Jednak wiele incydentów nie jest związanych z tak wyraźnymi objawami. Znikome oznaki, takie jak jedna zmiana w jednym pliku konfiguracyjnym systemu, mogą być jedynymi wskazówkami, że wystąpił incydent. W obsłudze incydentów wykrywanie może być najtrudniejszym zadaniem. Osoby obsługujące incydenty są odpowiedzialne za analizę niejednoznacznych, sprzecznych i niekompletnych objawów w celu ustalenia, co się stało. Chociaż istnieją rozwiązania techniczne, które mogą ułatwić wykrywanie, najlepszym rozwiązaniem jest zbudowanie zespołu wysoce doświadczonych i biegłych pracowników, którzy potrafią skutecznie i wydajnie analizować zwiastuny i wskaźniki oraz podejmować odpowiednie działania. Bez dobrze wyszkolonego i zdolnego personelu wykrywanie i analiza incydentów będzie przebiegać nieefektywnie i będą popełniane kosztowne błędy.

Zespół reagowania na incydenty powinien działać szybko i sprawnie, aby przeanalizować i zweryfikować każdy incydent, postępując zgodnie z wcześniej zdefiniowanym procesem

i dokumentując każdy podjętą czynność. Gdy zespół uważa, że wystąpił incydent, powinien szybko przeprowadzić wstępną analizę, aby określić zakres incydentu, na przykład, których sieci, systemów lub aplikacji dotyczy problem; kto lub co spowodowało incydent; w jaki sposób dochodzi do incydentu (np. jakie narzędzia lub metody ataku są używane, jakie luki w zabezpieczeniach są wykorzystywane). Wstępna analiza powinna dostarczyć zespołowi wystarczających informacji do ustalenia priorytetów dalszych działań, takich jak powstrzymanie incydentu i głębsza analiza skutków incydentu.

Przeprowadzenie wstępnej analizy i weryfikacji jest trudnym zadaniem. Poniżej przedstawiono zalecenia dotyczące ułatwienia i zwiększenia skuteczności analizy incydentów:

- **Profile sieci i systemów.** *Profilowanie* jest pomiarem charakterystyki spodziewanej aktywności, aby jej zmiany mogły być łatwiej zidentyfikowane. Przykładem profilowania jest uruchamianie oprogramowania do sprawdzania integralności plików na hostach w celu uzyskania sum kontrolnych dla krytycznych plików oraz monitorowanie wykorzystania przepustowości sieci w celu określenia, jakie są średnie i szczytowe poziomy użycia w różnych dniach i godzinach. W praktyce trudno jest dokładnie wykryć incydenty przy użyciu większości technik profilowania. Organizacje powinny stosować profilowanie jako jedną z kilku technik wykrywania i analizy.
- **Rozpoznanie normalnych zachowań.** Członkowie zespołu reagowania na incydenty powinni badać sieci, systemy i aplikacje, aby zrozumieć, jakie jest ich normalne zachowanie i łatwiejsze było rozpoznanie nieprawidłowe zachowania. Żadna osoba zajmująca się incydentem nie posiada kompleksowej wiedzy na temat wszystkich zachowań w całym środowisku, ale osoby obsługujące incydenty powinny wiedzieć, którzy eksperci mogą uzupełnić luki. Jednym ze sposobów uzyskania tej wiedzy jest przeglądanie wpisów dziennika i alertów zabezpieczeń. Może to być uciążliwe, jeśli filtrowanie nie jest używane do ograniczania dzienników do rozsądnych rozmiarów. Gdy osoby obsługujące lepiej zaznajomią się z dziennikami i alertami, powinny móc skupić się na niewyjaśnionych wpisach, które zwykle są najważniejsze do zbadania. Prowadzenie częstych przeglądów logów powinno zapewnić aktualność wiedzy, a analityk powinien być w stanie dostrzec trendy i zmiany w czasie. Przeglądy dają również analitykowi wskazówkę co do wiarygodności każdego źródła.
- **Ustanowienie zasady retencji dzienników.** Informacje dotyczące incydentu mogą być rejestrowane w kilku miejscach, takich jak zapora sieciowa, IDPS i dzienniki aplikacji. Tworzenie i wdrażanie zasad retencji dzienników, które określają, jak długo należy

przechowywać dane dzienniki, może być niezwykle pomocne w analizie, ponieważ starsze wpisy dziennika mogą wskazywać na aktywność rozpoznania lub wcześniejsze wystąpienia podobnych ataków. Innym powodem przechowywania dzienników jest to, że incydenty mogą zostać wykryte dopiero po kilku dniach, tygodniach lub nawet miesiącach. Czas przechowywania danych dziennika zależy od kilku czynników, w tym od polityki przechowywania danych w organizacji i ilości danych. Dodatkowe zalecenia dotyczące rejestrowania można znaleźć w NSC 800-92, *Przewodnik po zarządzaniu dziennikami zabezpieczeń komputera.*

- **Przeprowadzanie korelacji zdarzeń.** Dowody z incydentu mogą być rejestrowane w kilku dziennikach, z których każdy zawiera różne typy danych - dziennik zapory może mieć źródłowy adres IP, który został użyty, podczas gdy dziennik aplikacji może zawierać nazwę użytkownika. Sieciowy IDPS może wykryć, że atak został przeprowadzony na określonego hosta, ale może nie wiedzieć, czy atak się powiódł. Analityk powinien sprawdzić dzienniki hosta, aby określić te informacje. Korelowanie zdarzeń z wielu źródeł wskaźników może być nieocenione przy sprawdzaniu, czy wystąpił konkretny incydent.
- **Utrzymywanie synchronizacji zegarów wszystkich hostów**. Protokoły synchronizacji czasu, takie jak NTP (*ang. Network Time Protocol*), synchronizują zegary między hostami.[25] Korelacja zdarzeń będzie bardziej skomplikowana, jeśli urządzenia zgłaszające zdarzenia mają niespójne ustawienia zegara. Z punktu widzenia dowodowego, lepiej jest mieć spójne sygnatury czasowe w dziennikach - na przykład trzy dzienniki pokazujące, że atak miał miejsce o godzinie 12:07:01, a nie dzienniki, które wymieniają atak jako mający miejsce o godzinie 12:07:01. 12:10:35 i 11:07:06.
- **Utrzymywanie i korzystanie z bazy wiedzy.** Baza wiedzy powinna zawierać informacje, do których osoby obsługujące muszą się szybko odwoływać podczas analizy incydentów. Chociaż możliwe jest zbudowanie bazy wiedzy o złożonej strukturze, proste podejście może być skuteczniejsze. Dokumenty tekstowe, arkusze kalkulacyjne i stosunkowo proste bazy danych zapewniają skuteczne, elastyczne i przeszukiwalne mechanizmy udostępniania danych członkom zespołu. Baza wiedzy powinna również zawierać różnorodne informacje, w tym wyjaśnienia dotyczące znaczenia i ważności zwiastunów i wskaźników, takich jak alerty IDPS, wpisy dziennika systemu operacyjnego i kody błędów aplikacji.

[25] Więcej informacji o NTP jest dostępne pod adresem http://www.ntp.org

- **Używanie wyszukiwarek internetowych do przeszukiwania.** Wyszukiwarki internetowe mogą pomóc analitykom znaleźć informacje o nietypowej aktywności. Na przykład analityk może zobaczyć nietypowe próby połączenia ukierunkowane na port TCP 22912. Wyszukiwanie terminów „TCP", „port" i „22912" może skutkować uzyskaniem wyników zawierających dzienniki podobnych działań lub nawet objasnienie znaczenia numeru portu. Należy pamiętać, że do wyszukiwania należy używać oddzielnych stacji roboczych, aby zminimalizować ryzyko dla organizacji związane z przeprowadzaniem takich wyszukiwań.
- **Uruchamianie snifferów pakietów do gromadzenia dodatkowych danych.** Czasami wskaźniki nie są szczegółowo wystarczające, aby pozwolić osobie postępującej z incydentem zrozumienie tego, co się dzieje. Jeśli zdarzenie ma miejsce w sieci, najszybszym sposobem zebrania niezbędnych danych może być przechwyceni e ruchu sieciowego przez sniffera pakietów. Skonfigurowanie sniffera do rejestrowania ruchu spełniającego określone kryteria powinno pozwolić na zarządzanie wolumenem danych i zminimalizować nieumyślne przechwytywanie innych informacji. Ze względu na obawy związane z prywatnością, niektóre organizacje mogą wymagać, aby osoby obsługujące incydenty wnioskowały o użycie snifferów i otrzymywały pozwolenie przed ich użyciem.
- **Filtrowanie danych.** Żadna organizacja nie dysponuje wystarczającym zapasem czasu, aby przejrzeć i przeanalizować wszystkie wskaźniki. Przynajmniej najbardziej podejrzane działania powinny być badane jako minimum podejmowanych dzialań. Jedną ze skutecznych strategii jest odfiltrowanie kategorii wskaźników, które zazwyczaj są nieistotne. Inną strategią filtrowania jest pokazanie tylko tych kategorii wskaźników, które mają największe znaczenie. Jednak takie podejście niesie ze sobą znaczne ryzyko, ponieważ nowa złośliwa aktywność może nie należeć do żadnej z wybranych kategorii wskaźników.

3.2.5. Uzyskiwanie pomocy z innych źródeł. Dokumentacja incydentów

Zespół reagowania na incydenty, który podejrzewa, że miał miejsce incydent, powinien natychmiast rozpocząć rejestrowanie wszystkich faktów dotyczących incydentu.[26] Dziennik

[26] Osoby zajmujące się incydentami powinny rejestrować tylko fakty dotyczące incydentu, a nie osobiste opinie lub wnioski. Materiał subiektywny powinien być przedstawiany w raportach incydentów, a nie dokumentowany jako dowód.

jest skutecznym i prostym nośnikiem[27], ale mogą do tego służyć również laptopy, dyktafony i aparaty cyfrowe.[28] Dokumentowanie zdarzeń systemowych, konwersacji i zaobserwowanych zmian w plikach może prowadzić do wydajniejszej, bardziej systematycznej i mniej podatnej na błędy obsługi problemu. Każdy krok od momentu wykrycia incydentu do jego ostatecznego rozwiązania powinien być udokumentowany i opatrzony datą. Każdy dokument dotyczący zdarzenia powinien być opatrzony datą i podpisany przez osobę zajmującą się incydentem. Informacje tego rodzaju mogą być również wykorzystane jako dowód w sądzie, jeżeli prowadzone jest postępowanie sądowe. Gdy tylko jest to możliwe, osoby postępujące z incydentami powinni pracować w co najmniej dwuosobowych zespołach: jedna osoba może zapisywać i rejestrować zdarzenia, podczas gdy druga wykonuje zadania techniczne. Rozdział 3.3.2. przedstawia więcej informacji o dowodach.[29]

Zespół reagowania na incydenty powinien przechowywać dokumentację dotyczącą statusu incydentów, wraz z innymi stosownymi informacjami.[30] Korzystanie z aplikacji lub bazy danych, takiej jak system śledzenia problemów, pomaga zapewnić obsługę i rozwiązywanie incydentów w odpowiednim czasie. System śledzenia problemów powinien zawierać następujące informacje:

- Aktualny stan incydentu (nowy, w toku, przekazany do zbadania, rozwiązany itp.).
- Podsumowanie incydentu.
- Wskaźniki związane ze incydentem.
- Inne incydenty związane z tym incydentem.
- Działania podjęte w związku z tym incydentem przez wszystkie osoby obsługujące incydent.
- Łańcuch dowodowy, jeśli dotyczy.

[27] W przypadku korzystania z dziennika zaleca się, aby dziennik był oprawiony, a osoby zajmujące się incydentami numerowały strony, pisały atramentem i pozostawiały dziennik w stanie nienaruszonym (tj. nie wyrywały żadnych stron).

[28] Należy rozważyć dopuszczalność dowodów zebranych za pomocą urządzenia przed jego użyciem. Na przykład, żadne urządzenia, które są potencjalnymi źródłami dowodów, nie powinny same być używane do rejestrowania innych dowodów.

[29] Publikacja NIST SP 800-86, *Przewodnik po integracji technik śledczych do reagowania na incydent*, zawiera szczegółowe informacje na temat ustanawiania zdolności śledczych, w tym opracowywania zasad i procedur. Patrz: https://csrc.nist.gov/publications/detail/sp/800-86/final

[30] Załącznik B zawiera sugerowaną listę danych, które należy gromadzić w przypadku zgłaszania incydentów.

- Oceny skutków związanych z incydentem.
- Dane kontaktowe innych zaangażowanych stron (np. właścicieli systemu, administratorów systemu).
- Lista dowodów zebranych podczas badania incydentu.
- Komentarze osób obsługujących incydent.
- Kolejne kroki, które należy podjąć (np. przebudowa hosta, aktualizacja aplikacji).[31]

Zespół reagowania na incydenty powinien chronić dane na temat incydentów i ograniczać do nich dostęp, ponieważ często zawierają wrażliwe informacje - na przykład dane dotyczące wykorzystanych luk w zabezpieczeniach, najnowszych naruszeń bezpieczeństwa oraz użytkowników, którzy mogli wykonać niewłaściwe działania. Na przykład, tylko upoważniony personel powinien mieć dostęp do bazy danych incydentów. Komunikacja dotycząca incydentu (np. e-maile) i dokumenty powinny być zaszyfrowane lub w inny sposób zabezpieczone, aby tylko autoryzowany personel mógł je odczytywać.

3.2.6. Priorytetyzacja incydentu

Nadanie priorytetu obsłudze incydentu jest prawdopodobnie najbardziej krytycznym punktem decyzyjnym w procesie obsługi incydentu. Ze względu na ograniczenia zasobów nie należy obsługiwać incydentów według kolejności zgłoszeń. Zamiast tego, postępowanie powinno być traktowane priorytetowo w oparciu o istotne czynniki, takie jak:

- **Wpływ incydentu na funkcjonowanie organizacji.** Incydenty dotyczące systemów IT zwykle wpływają na funkcjonalność biznesową, którą zapewniają te systemy, powodując pewien rodzaj negatywnego wpływu na użytkowników tych systemów. Osoby zajmujące się obsługą incydentów powinny rozważyć, jak incydent wpłynie na istniejącą funkcjonalność systemów, których dotyczy luka. Osoby zajmujące się incydentami powinny wziąć pod uwagę nie tylko bieżący wpływ funkcjonalny incydentu, ale także prawdopodobny przyszły wpływ funkcjonalny incydentu, jeśli nie zostanie natychmiast powstrzymany.

[31] Transeuropejskie Stowarzyszenie Sieci Badań i Edukacji (TERENA) opracowało RFC 3067, wymagania dotyczące opisu obiektu incydentu i formatu wymiany TERENA (http://www.ietf.org/rfc/rfc3067.txt). Dokument zawiera zalecenia dotyczące tego, jakie informacje należy gromadzić dla każdego zdarzenia. Grupa robocza IETF Extended Incident Handling (inch) Working Group (http://www.cert.org/ietf/inch/inch.html) utworzyła dokument RFC, który rozszerza prace TERENA - RFC 5070, format wymiany opisu obiektu incydentów (http://www.ietf.org/rfc/rfc5070.txt).

- **Wpływ incydentu na informacje.** Incydenty mogą wpływać na poufność, integralność i dostępność informacji organizacji. Na przykład podstępny czynnik może wydobyć wrażliwe informacje. Osoby zajmujące się incydentami powinny rozważyć, w jaki sposób ujawnienie tych informacji wpłynie na ogólną misję organizacji. Incydent, który powoduje eksfiltrację wrażliwych informacji, może również wpłynąć na inne organizacje, jeśli którekolwiek z danych dotyczą organizacji partnerskiej.
- **Możliwość odtworzenia po incydencie**. Rozmiar incydentu i rodzaj zasobów, na które ma on wpływ, określają ilość czasu i zasobów, które należy poświęcić na powrót do stanu normalnego po tym incydencie. W niektórych przypadkach nie jest możliwe odzyskanie sprawności po incydencie (np. jeśli poufność wrażliwych informacji została naruszona) i nie ma sensu wydawanie ograniczonych zasobów na wydłużony cykl obsługi incydentu, chyba, że wysiłek ten został skierowany na zapewnienie, żeby podobny incydent nie miał miejsca w przyszłości. W innych przypadkach incydent może wymagać znacznie większych zasobów do obsługi niż to, co organizacja ma do dyspozycji. Osoby zajmujące się obsługą incydentów powinny wziąć pod uwagę wysiłek niezbędny do rzeczywistego przywrócenia stanu normalnego po zdarzeniu i dokładnie rozważyć, jakie korzyści może przynieść przywrócenie stanu normalnego w stosunku do wielkości wysiłków poniesionych na rzecz przywrócenia stanu normalnego.

Połączenie wpływu na funkcjonowanie systemów organizacji i wpływu na informacje organizacji określa wpływ incydentu na biznes - na przykład rozproszony atak typu „odmowa usługi" na publiczny serwer WWW może tymczasowo zmniejszyć funkcjonalność dla użytkowników próbujących uzyskać dostęp do serwera, natomiast nieautoryzowany dostęp na poziomie administratora do publicznego serwera internetowego może skutkować eksfiltracją danych osobowych, co może mieć długotrwały wpływ na reputację organizacji.

Możliwość odtworzenia danych po incydencie określa możliwe reakcje, które zespół może podjąć podczas obsługi incydentu. Incydent o dużym wpływie na funkcjonalność i niewielkim wysiłku koniecznym, aby powrócić do stanu normalnego, jest idealnym materiałem do natychmiastowego działania zespołu. Jednak niektóre incydenty mogą nie mieć płynnych ścieżek odtwarzania i mogą wymagać kolejkowania w celu uzyskania odpowiedzi na bardziej strategicznym poziomie - na przykład incydent, w wyniku którego atakujący wyprowadza i publikuje gigabajty wrażliwych danych, nie ma łatwej ścieżki odzyskiwania, ponieważ dane już zostały narażone. W takim przypadku zespół może przenieść część odpowiedzialności za obsługę incydentu związanego z eksfiltracją danych na zespół o bardziej strategicznym poziomie, który opracuje strategię zapobiegania przyszłym naruszeniom i stworzy plan

zasięgu powiadamiania, w celu zaalarmowania osób lub organizacji, których dane zostały eksfiltrowane. Zespół powinien ustalić priorytety reakcji na każde incydent na podstawie oszacowania wpływu na biznes spowodowanego incydentem oraz szacowanych wysiłków niezbędnych do przywrócenia sprawności po incydencie.

Organizacja może najlepiej określić ilościowo skutki swoich własnych incydentów ze względu na swoją świadomość sytuacyjną. Tabela 3-2 zawiera przykłady kategorii wpływu funkcjonalnego, których organizacja może używać do oceny własnych incydentów. Ocenianie incydentów może być pomocne w określaniu priorytetów ograniczonych zasobów.

Tabela 3-2. Kategorie wpływu na funkcjonowanie

Kategoria	Definicja
Brak	Brak wpływu na zdolność organizacji do świadczenia wszystkich usług wszystkim użytkownikom.
Niska	Efekt minimalny; organizacja może nadal świadczyć wszystkie krytyczne usługi wszystkim użytkownikom, ale straciła wydajność.
Średnia	Organizacja utraciła możliwość świadczenia krytycznych usług części użytkownikom systemu.
Wysoka	Organizacja nie jest już w stanie świadczyć wybranych krytycznych usług żadnym użytkownikom.

Tabela 3-3 zawiera przykłady możliwych kategorii wpływu informacji, które opisują zakres naruszenia informacji występujących podczas incydentu. W tej tabeli, z wyjątkiem wartości „Brak", kategorie nie wykluczają się wzajemnie i organizacja może wybrać więcej niż jedną.

Tabela 3-3. Kategorie wpływu na informacje

Kategoria	Definicja

Brak	Żadne informacje nie zostały wyodrębnione, zmienione, usunięte ani w inny sposób naruszone.
Naruszenie prywatności	Uzyskano dostęp lub wyprowadzono wrażliwe dane osobowe podatników, pracowników, beneficjentów itp.
Naruszenie własności	Uzyskano dostęp lub wyprowadzono niesklasyfikowane informacje, takie jak chronione informacje o infrastrukturze krytycznej.
Utrata integralności	Informacje wrażliwe lub zastrzeżone zostały zmienione lub usunięte.

Tabela 3-4 przedstawia przykłady kategorii nakładów związanych z odzyskiwaniem, które odzwierciedlają poziom i rodzaj zasobów wymaganych do odtworzenia funkcjonowania po incydencie.

Tabela 3-4. Kategorie wysiłku odtwarzania

Kategoria	Definicja
Standardowy	Czas powrotu do stanu normalnego jest przewidywalny z użyciem istniejących zasobów.
Rozszerzony	Czas odtworzenia jest przewidywalny z użyciem dodatkowych zasobów.
Wymagający wsparcia	Czas odtworzenia jest nieprzewidywalny. potrzebne są dodatkowe zasoby i pomoc z zewnątrz.
Niemożliwy do odtworzenia	Odtworzenie po incydencie nie jest możliwe (np. dane wrażliwe wyprowadzone i udostępnione publicznie); należy uruchomić postępowanie dochodzeniowe.

Organizacje powinny również ustanowić proces eskalacji dla tych przypadków, kiedy zespół nie reaguje na incydent w wyznaczonym czasie. Może się to zdarzyć z wielu powodów, na przykład brak /utrudniona łączność, osobiste nagłe problemy członków zespołu. Proces eskalacji powinien określać, jak długo dana osoba powinna czekać na odpowiedź i co zrobić, jeśli nie ma odpowiedzi. Generalnie pierwszym krokiem jest powtórzenie pierwszego

kontaktu. Po odczekaniu krótkiego czasu, np. 15 minut, dzwoniący powinien eskalować incydent na wyższy poziom, na przykład do kierownika zespołu reagowania na incydenty. Jeśli ta osoba nie zareaguje w określonym czasie, incydent powinien zostać ponownie przekazany do kierownictwa wyższego szczebla. Ten proces należy powtarzać do czasu reakcji na zgłaszany problem.

3.2.7. Powiadamianie o incydencie

Kiedy incydent jest analizowany i uszeregowany pod względem ważności (ustalone są priorytety), zespół reagowania na incydent musi powiadomić odpowiednie osoby, tak aby wszyscy, którzy muszą być zaangażowani, odegrali swoje role. Zasady reagowania na incydenty powinny zawierać postanowienia dotyczące zgłaszania incydentów - co najmniej, co należy zgłaszać, komu i w jakim czasie (np. wstępne powiadomienie, regularne aktualizacje statusu). Dokładne wymagania dotyczące zgłaszania różnią się w zależności od organizacji, ale strony, które są zwykle powiadamiane, obejmują[32]:

- CIO
- SAISO
- Lokalnego inspektora bezpieczeństwa informacji.
- Inne zespoły reagowania na incydenty w organizacji.
- Zewnętrzne zespoły reagowania na incydenty (jeśli dotyczy).
- Właściciela systemu.
- Dział zasobów ludzkich (w sprawach dotyczących pracowników, takich jak nękanie za pośrednictwem poczty elektronicznej).
- Dział spraw publicznych (w przypadku incydentów, które mogą generować rozgłos).
- Dział prawny (w przypadku incydentów z potencjalnymi konsekwencjami prawnymi).
- Zespół reagowania na incydenty bezpieczeństwa komputerowego (CSIRT) - patrz rozdział 2.3.4.3).
- Organy ścigania (w stosownych przypadkach).

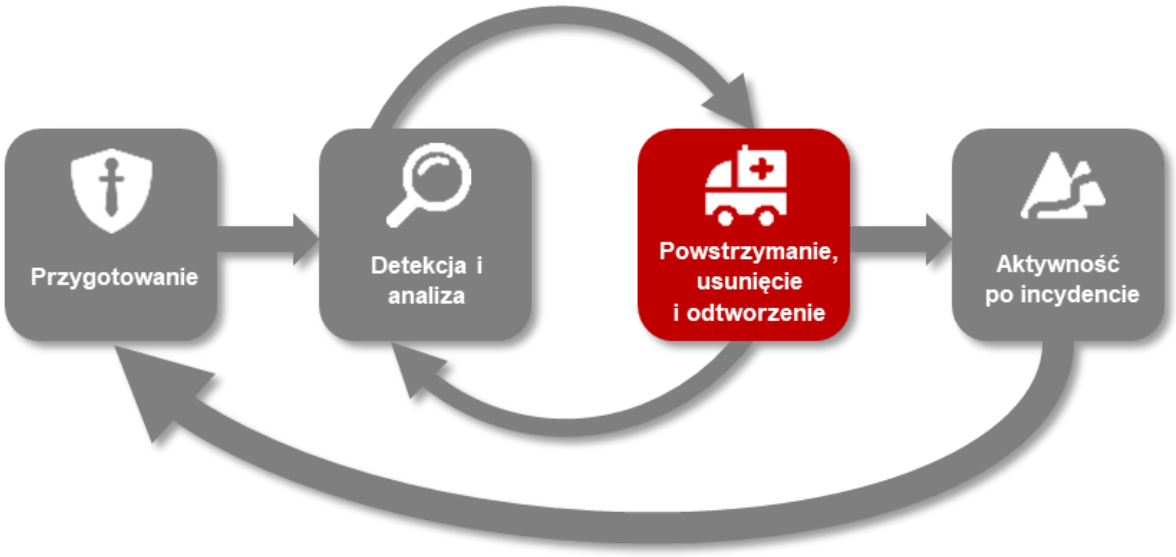
Podczas obsługi incydentu może istnieć konieczność, aby zespół dostarczał aktualizacje statusu określonym stronom, a w niektórych przypadkach nawet całej organizacji. Zespół

[32] patrz Słownik kluczowych pojęć z zakresu cyberbezpieczeństwa https://www.gov.pl/attachment/48226cb6-29d4-49f9-860f-acd703072e60

powinien zaplanować i przygotować kilka metod komunikacji, w tym metody nienormatywne (np. osobiście, na papierze) i wybrać metody, które są odpowiednie dla konkretnego zdarzenia. Możliwe metody komunikacji obejmują:

- e-mail.
- Witryna internetowa (wewnętrzna, zewnętrzna lub portal).
- Rozmowy telefoniczne.
- Osobiście (np. codzienne odprawy).
- Powitanie w poczcie głosowej (np. skonfigurowanie oddzielnej skrzynki głosowej do aktualizacji zdarzeń i wiadomości powitalnej, aby odzwierciedlała aktualny stan zdarzenia; użycie powitania w poczcie głosowej działu pomocy).
- Na papierze (np. zawiadomienia na tablicach ogłoszeń i drzwiach, wręczanie ogłoszeń we wszystkich wejściach).

3.3. Powstrzymanie, usunięcie i odtworzenie



Rysunek 3-3. Cykl obsługi incydentu (Powstrzymanie, usunięcie i odtworzenie).

3.3.1. Wybór strategii powstrzymania

Powstrzymanie jest ważnym elementem, zanim incydent pochłonie zasoby lub zwiększy szkodę. Większość incydentów wymaga powstrzymania, więc jest to ważna kwestia na

wczesnym etapie obsługi każdego incydentu. Powstrzymywanie zapewnia czas na opracowanie dostosowanej strategii naprawczej. Istotną częścią powstrzymania jest podejmowanie decyzji (np. zamknięcie systemu, odłączenie go od sieci, wyłączenie niektórych funkcji). Takie decyzje są znacznie łatwiejsze do podjęcia, jeśli istnieją z góry określone strategie i procedury powstrzymania incydentu. Organizacje powinny zdefiniować akceptowalne ryzyko w postępowaniu z incydentami i odpowiednio opracować strategie.

Strategie powstrzymywania różnią się w zależności od rodzaju incydentu. Na przykład strategia powstrzymywania infekcji złośliwym oprogramowaniem przenoszonym przez pocztę e-mail różni się znacznie od strategii sieciowego ataku DDoS. Organizacje powinny stworzyć oddzielne strategie powstrzymywania dla każdego poważnego typu incydentu, z jasno udokumentowanymi kryteriami, aby ułatwić podejmowanie decyzji.

Kryteria określania właściwej strategii obejmują:

- Potencjalne uszkodzenie i kradzież zasobów.
- Potrzebę zabezpieczenia dowodów.
- Dostępność usług (np. połączenia sieciowe, usługi świadczone na rzecz podmiotów zewnętrznych).
- Czas i zasoby potrzebne do wdrożenia strategii.
- Skuteczność strategii (np. częściowe zabezpieczenie, pełne zabezpieczenie).
- Czas rozwiązania (np. awaryjne obejście do usunięcia w ciągu czterech godzin, tymczasowe rozwiązanie do usunięcia za dwa tygodnie, trwałe rozwiązanie).

W niektórych przypadkach niektóre organizacje przekierowują atakującego do środowiska izolowanego (*ang. sandboxing*), jako formę powstrzymywania, w celu monitorowania aktywność atakującego, oraz zebrania dodatkowych dowodów. Zespół reagowania na incydenty powinien omówić tę strategię ze swoim działem prawnym, aby określić, czy jest ona prawnie wykonalna. Nie należy stosować innych sposobów monitorowania aktywności atakującego niż środowisko izolowane. Jeśli organizacja posiada wiedzę, że system został naruszony i zezwala na kontynuowanie naruszenia, może pozostać pociągnięta do odpowiedzialności, jeśli osoba atakująca wykorzysta zaatakowany system, którego zabezpieczenia zostały naruszone, do zaatakowania innych systemów. Strategia opóźnionego powstrzymywania jest niebezpieczna, ponieważ osoba atakująca może poszerzyć nieautoryzowany dostęp lub złamać zabezpieczenia innych systemów.

Innym potencjalnym problemem związanym z powstrzymywaniem jest to, że niektóre ataki mogą powodować dodatkowe szkody, gdy zostaną powstrzymane. Na przykład,

zaatakowany host może uruchomić złośliwy proces, który okresowo wysyła pingi do innego hosta. Gdy program obsługi incydentów próbuje powstrzymać incydent poprzez odłączenie od sieci hosta, którego dotyczy luka, kolejne pingi zakończą się niepowodzeniem. W wyniku awarii złośliwy proces może nadpisać lub zaszyfrować wszystkie dane na dysku twardym hosta. Osoby obsługujące incydent nie powinny zakładać, że tylko dlatego, że host został odłączony od sieci, można zapobiec dalszym uszkodzeniom hosta.

3.3.2. Gromadzenie i postępowanie z dowodami

Chociaż głównym powodem gromadzenia dowodów podczas incydentu jest rozwiązanie incydentu, może to być również potrzebne w postępowaniu sądowym.[33] W takich przypadkach ważne jest, aby jasno udokumentować, jak wszystkie dowody, w tym naruszone systemy, zostały zachowane.[34] Dowody należy gromadzić zgodnie z procedurami, które są zgodne ze wszystkimi obowiązującymi przepisami prawa i regulacjami, które zostały opracowane w uzgodnieniu z działem prawnym i odpowiednimi organami ścigania, tak, aby wszelkie dowody mogły zostać dopuszczone w sądzie.

Ponadto zawsze należy prowadzić ewidencję dowodów. Za każdym razem, gdy dowody są przekazywane pomiędzy osobami, formularze kontroli dowodowej powinny określać szczegóły przekazania i zawierać podpis każdej ze stron. Należy prowadzić szczegółowy dziennik wszystkich dowodów, w tym:

- Informacje identyfikacyjne (np. lokalizacja, numer seryjny, numer modelu, nazwa hosta, adresy sprzętowe MAC i adresy IP komputera).
- Nazwisko, stanowisko i numer kontaktowy każdej osoby, która zebrała lub zajmowała się materiałami dowodowymi podczas prowadzonego dochodzenia.
- Godzina i data (w tym strefa czasowa) każdego przypadku postępowania dowodowego.
- Lokalizacje, w których przechowywano dowody.

[33] Patrz NIST SP 800-86, *Przewodnik po integracji technik śledczych do reagowania na incydent*, zawierający szczegółowe informacje na temat ustanawiania zdolności kryminalistycznych. Skupia się on na informatyce śledczej odnoszącej się do komputerów osobistych, ale większość materiału ma zastosowanie w innych systemach.

[34] Gromadzenie i przetwarzanie dowodów nie jest zwykle wykonywane dla każdego zdarzenia, które ma miejsce - na przykład, większość incydentów związanych ze złośliwym oprogramowaniem nie wymaga gromadzenia dowodów. W wielu organizacjach, informatyka śledcza nie jest potrzebna w przypadku większości incydentów.

Gromadzenie dowodów z zasobów komputerowych stwarza pewne wyzwania. Zasadniczo pożądane jest uzyskanie dowodów z właściwego systemu, gdy tylko podejrzewa się, że incydent mógł mieć miejsce. Wiele incydentów powoduje dynamiczny łańcuch wydarzeń. Wstępne zrzuty z systemu mogą przynieść więcej korzyści w identyfikacji problemu i jego źródła niż większość innych działań, które można podjąć na tym etapie. Z punktu widzenia dowodowego znacznie lepiej jest uzyskać zrzut stanu systemu, zamiast robić to po tym, jak osoby obsługujące incydenty, administratorzy systemu i inne osoby nieumyślnie zmienili stan urządzeń podczas przeprowadzanego dochodzenia. Użytkownicy i administratorzy systemu powinni być świadomi kroków, które powinni podjąć, aby zachować dowody. Wskazanym jest zapoznanie się z publikacja NIST SP 800-86, *Przewodnik po integracji technik śledczych do reagowania na incydent*, aby uzyskać dodatkowe informacje na temat zabezpieczania dowodów.

3.3.3. Zidentyfikowanie atakujących hostów

Podczas obsługi incydentów właściciele systemów i inne osoby czasami chcą lub muszą zidentyfikować atakującego hosta lub hosty. Chociaż te informacje mogą być ważne, osoby zajmujące się incydentami powinny zasadniczo skupiać się na powstrzymywaniu, eliminowaniu i odzyskiwaniu. Identyfikacja atakującego hosta może być czasochłonnym i daremnym procesem, który może uniemożliwić zespołowi osiągnięcie głównego celu - zminimalizowania wpływu na biznes. Poniższe pozycje opisują najczęściej wykonywane działania w celu identyfikacji atakującego hosta:

- **Sprawdzanie adresu IP atakującego hosta.** Nowe programy obsługi incydentów często koncentrują się na adresie IP atakującego hosta. Program obsługi może próbować sprawdzić, czy adres nie został sfałszowany, weryfikując komunikację z nim. Jednakże oznacza to po prostu, że host pod tym adresem odpowiada lub nie odpowiada na żądania. Brak odpowiedzi nie oznacza, że adres nie jest rzeczywisty - na przykład host może być skonfigurowany tak, aby ignorował pingi i trasy śledzenia (*ang. traceroute*). Ponadto osoba atakująca mogła otrzymać adres dynamiczny, który został już przypisany komuś innemu.
- **Badanie atakującego hosta za pomocą wyszukiwarek.** Przeprowadzenie wyszukiwania w Internecie przy użyciu pozornego adresu IP źródła ataku, może doprowadzić do uzyskania dodatkowych informacji o ataku - na przykład wiadomości z listy mailingowej dotyczącej podobnego ataku.
- **Korzystanie z baz danych incydentów.** Kilka grup zbiera i konsoliduje dane incydentów z różnych organizacji w bazach danych incydentów. Takie udostępnianie

informacji może mieć różne formy, takie jak urządzenia śledzące w i czarne listy czasu rzeczywistego. Organizacja może również sprawdzić swoją własną bazę wiedzy lub system śledzenia problemów pod kątem powiązanych działań.

- **Monitorowanie prawdopodobnych kanałów komunikacyjnych atakującego.** Programy obsługi incydentów mogą monitorować kanały komunikacyjne, które mogą być używane przez atakującego hosta. Na przykład wiele botów używa czatów internetowych (*ang. Internet Relay Chat IRCt*)[35] jako podstawowego środka komunikacji. Atakujący mogą również gromadzić się na niektórych kanałach IRC, aby chwalić się swoimi włamaniami i dzielić się informacjami. Jednak osoby zajmujące się incydentami powinny traktować wszelkie takie informacje, które uzyskają, jedynie jako potencjalny trop, a nie jako fakty.

3.3.4. Usunięcie i odtworzenie

Po powstrzymaniu incydentu może być konieczne jego wyeliminowanie, aby wyeliminować elementy incydentu, takie jak usunięcie złośliwego oprogramowania i wyłączenie kont użytkowników, których podatności zostało naruszone, a także zidentyfikowanie i usuwanie wszystkich wykorzystanych luk (podatności). Podczas eliminacji ważne jest, aby zidentyfikować wszystkie zarażone hosty w organizacji, aby można było je wyczyścić. W przypadku niektórych incydentów eliminacja nie jest konieczna lub jest wykonywana podczas odtwarzania.

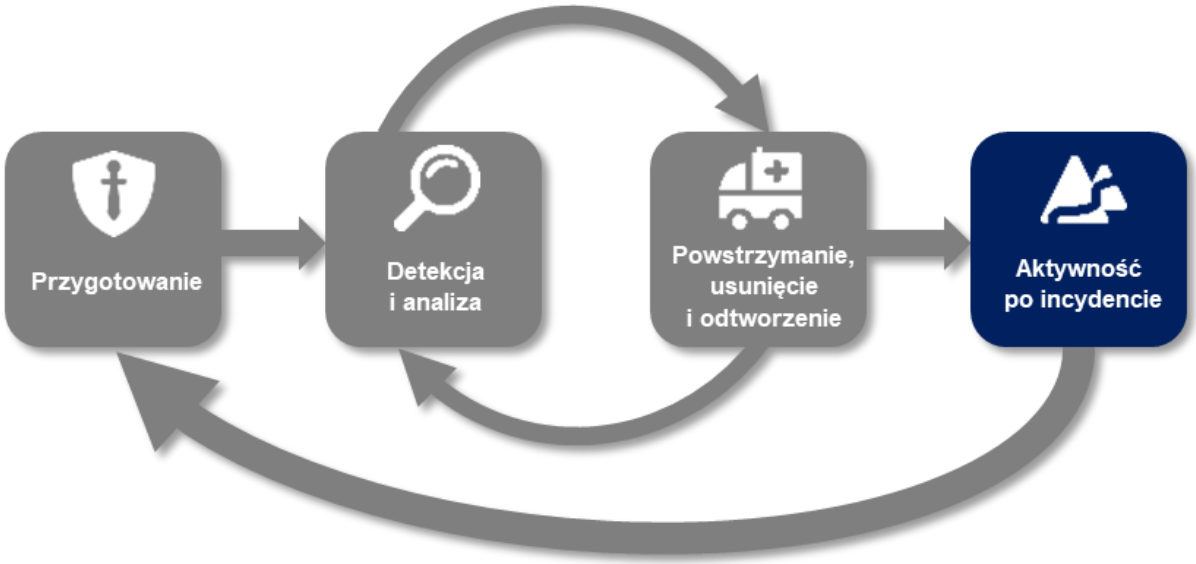
Podczas odtwarzania administratorzy przywracają systemy do normalnego działania, potwierdzają, że systemy działają normalnie i (jeśli dotyczy) usuwają luki w zabezpieczeniach, aby zapobiec podobnym incydentom. Odtwarzanie może obejmować takie działania, jak przywracanie systemów z czystych kopii zapasowych, odbudowywanie systemów od podstaw, zastępowanie zainfekowanych plików czystymi wersjami, instalowanie poprawek, zmiana haseł i zwiększanie bezpieczeństwa granic sieci (np. reguły firewalli, listy kontroli dostępu routera brzegowego). Wyższe poziomy logowania w systemie lub monitorowania sieci są często częścią procesu odtwarzania. Raz pomyślnie zaatakowany zasób jest często atakowany ponownie lub w podobny sposób są atakowane inne zasoby w organizacji.

[35] IRC bot – zbiór skryptów lub niezależny program, który działa w sieci IRC. Jest to program, który wykonuje automatycznie pewne akcje np.: dodawanie operatorów, wyrzucanie użytkowników z kanału, automatyczne odpowiadanie na rozmaite pytania a nawet prowadzenie gier i konkursów przeprowadzanych na kanałach IRC.

Usuwanie i odtwarzanie powinno odbywać się etapami, tak, aby nadać priorytet krokom naprawczym. W przypadku incydentów na dużą skalę odzyskiwanie może zająć miesiące. Zamierzeniem wczesnych faz powinno być zwiększenie ogólnego bezpieczeństwa poprzez stosunkowo szybkie (w ciągu kilku dni lub tygodni) zmiany o dużym znaczeniu, aby zapobiec przyszłym incydentom. Późniejsze fazy powinny koncentrować się na długoterminowych zmianach (np. zmianach infrastruktury) i bieżących pracach nad zapewnieniem maksymalnego bezpieczeństwa organizacji.

Ponieważ działania związane z usuwaniem i odtwarzaniem są zwykle specyficzne dla systemu operacyjnego lub aplikacji, szczegółowe zalecenia i porady dotyczące ich nie są objęte zakresem tego dokumentu.

3.4. Aktywność po incydencie



Rysunek 3-4. Cykl obsługi incydentu (Aktywność po incydencie).

3.4.1. Wyciągnięte wnioski

Jedna z najważniejszych części reagowania na incydenty jest również najczęściej pomijana: uczenie się i doskonalenie. Każdy zespół reagowania na incydenty powinien ewoluować, aby odzwierciedlać nowe zagrożenia, ulepszoną technologię i wyciągnięte wnioski. Organizowanie spotkań na temat zdobytego doświadczenia z wszystkimi zaangażowanymi

stronami po poważnym incydencie i opcjonalnie okresowo po mniejszych incydentach, na ile pozwalają na to zasoby, może być niezwykle pomocne w ulepszaniu środków bezpieczeństwa i samego procesu obsługi incydentu. Podczas jednego spotkania można omówić wiele incydentów. Spotkanie to daje szansę na zamknięcie incydentu poprzez przegląd tego, co się wydarzyło, co zostało zrobione podczas interwencji i jak sprawnie przebiegała odpowiedź na incydent. Spotkanie powinno odbyć się w ciągu kilku dni od zakończenia incydentu. Pytania, na które należy odpowiedzieć podczas spotkania, to:

- Dokładnie określić, co się stało i w jakim czasie?
- Jak dobrze personel i kierownictwo poradzili sobie z incydentem? Czy przestrzegano udokumentowanych procedur? Czy były one odpowiednie?
- Jakie informacje były potrzebne wcześniej, przed wystąpieniem incydentu?
- Czy wykonano jakieś kroki lub działania, które mogły utrudnić odtworzenie?
- Co personel i kierownictwo zrobiliby inaczej, gdyby następnym razem wystąpił podobny incydent?
- W jaki sposób można ulepszyć wymianę informacji z innymi organizacjami?
- Jakie działania naprawcze mogą zapobiec podobnym incydentom w przyszłości?
- Na jakie zwiastuny lub wskaźniki należy zwrócić uwagę w przyszłości, aby wykryć podobne incydenty?
- Jakie dodatkowe narzędzia lub zasoby są potrzebne do wykrywania, analizowania i łagodzenia skutków przyszłych incydentów?

Incydenty o potencjalnym małym wpływie na bezpieczeństwo wymagają ograniczonej analizy po incydencie, z wyjątkiem incydentów przeprowadzonych za pomocą nowych metod ataków, które budzą powszechne obawy i zainteresowanie. Po wystąpieniu poważnych ataków zwykle warto zorganizować spotkania *post factum*, które wykraczają poza możliwości zespołu reagowania i organizacji, aby zapewnić mechanizm wymiany informacji. Podstawową kwestią podczas organizowania takich spotkań jest zapewnienie zaangażowania właściwych osób. Nie tylko ważne jest, aby zaprosić osoby, które brały udział w analizowanym incydencie, ale warto również rozważyć, kogo należy zaprosić w celu ułatwienia przyszłej współpracy.

Sukces takich spotkań zależy również od agendy. Zbieranie informacji na temat oczekiwań i potrzeb (w tym sugerowanych tematów do omówienia) od uczestników przed spotkaniem zwiększa prawdopodobieństwo, że potrzeby uczestników zostaną zaspokojone. Ponadto

ustalenie zasad porządku przed lub w trakcie spotkania może zminimalizować zamieszanie i niezgodę. Posiadanie jednego lub więcej moderatorów, którzy są biegli w prowadzeniu grup, może przynieść duże korzyści. Na koniec ważne jest również udokumentowanie głównych punktów porozumienia i działań, a także przekazanie ich stronom, które nie mogły uczestniczyć w spotkaniu.

Spotkania na temat zdobytego doświadczenia dają inne korzyści. Raporty z tych spotkań są dobrym materiałem do szkolenia nowych członków zespołu, pokazując im, jak bardziej doświadczeni członkowie zespołu reagują na incydenty. Aktualizacja zasad i procedur reagowania na incydenty to kolejna ważna część procesu wyciągania wniosków. Analiza *post factum* sposobu, w jaki obsłużono incydent, często ujawnia brakujący krok lub niedokładność procedury, dając impuls do zmiany. Ze względu na zmieniający się charakter technologii informacyjnej i zmiany personalne, zespół reagowania na incydenty powinien przeglądać całą powiązaną dokumentację i procedury obsługi incydentów w wyznaczonych odstępach czasu.

Innym ważnym działaniem po incydencie jest stworzenie raportu uzupełniającego do każdego incydentu, który może być bardzo cenny do wykorzystania w przyszłości. Raport zawiera odniesienie, które może pomóc w obsłudze podobnych incydentów. Stworzenie formalnej chronologii zdarzeń (w tym informacji z sygnaturami czasowymi, takimi jak dane dziennika z systemów) jest ważne ze względów prawnych, podobnie jak oszacowanie kwoty szkód spowodowanych przez incydent. Szacunek ten może stać się podstawą dalszych działań dochodzeniowych. Raporty z działań następczych należy przechowywać przez okres określony w zasadach przechowywania dokumentacji.

3.4.2. Wykorzystanie zebranych danych o incydencie

Wyciągnięte wnioski powinny zapewnić zestaw obiektywnych i subiektywnych danych dotyczących każdego incydentu. Z biegiem czasu zebrane dane o incydentach powinny być przydatne na kilka sposobów. Dane, w szczególności łączna liczba godzin zaangażowania i koszt, mogą posłużyć do uzasadnienia dodatkowego finansowania zespołu reagowania na incydenty. Badanie charakterystyk incydentów może wskazywać na systemowe słabości i zagrożenia bezpieczeństwa informacji, a także zmiany trendów. Dane te można włączyć do procesu oceny ryzyka, ostatecznie prowadząc do wyboru i wdrożenia dodatkowych zabezpieczeń. Innym zastosowaniem danych jest mierzenie sukcesu zespołu reagowania na incydenty. Jeśli dane o incydentach są prawidłowo gromadzone i przechowywane, powinny zapewnić kilka miar sukcesu (lub przynajmniej działań) zespołu reagowania na incydenty. Dane o incydentach mogą być również gromadzone w celu ustalenia, czy zmiana możliwości

reagowania na incydenty powoduje odpowiednią zmianę w wydajności zespołu (np. poprawa wydajności, redukcja kosztów). Ponadto organizacje, które są zobowiązane do zgłaszania informacji o incydentach, będą musiały zebrać niezbędne dane, aby wypełnić swoje obowiązki. Dodatkowe informacje na temat udostępniania danych o incydentach innym organizacjom można znaleźć w rozdziale 4.

Organizacje powinny skupić się na gromadzeniu danych, które są przydatne, a nie tylko dlatego, że są dostępne. Na przykład, policzenie liczby zwiastunów skanowań portów, które mają miejsce w każdym tygodniu i utworzenie wykresu na koniec roku pokazującego wzrost liczby skanowań portów o osiem procent nie jest zbyt pomocne i może być dość czasochłonne. Liczby bezwzględne nie mają charakteru informacyjnego - ważne jest zrozumienie, w jaki sposób reprezentują one zagrożenia dla procesów biznesowych organizacji. Organizacje powinny zdecydować, jakie dane o incydentach należy gromadzić w oparciu o wymogi sprawozdawcze i oczekiwany zwrot z inwestycji z tych danych (np. identyfikacja nowego zagrożenia i łagodzenie powiązanych luk w zabezpieczeniach, zanim będzie można je wykorzystać). Możliwe wskaźniki danych związanych z incydentami obejmują:

- **Liczbę obsłużonych incydentów.**[36] Liczba obsługiwanych incydentów może spaść z powodu stosowania lepszych środków bezpieczeństwa sieci i hosta, a nie z powodu zaniedbania zespołu reagowania na incydenty. Liczbę obsłużonych incydentów najlepiej jest traktować jako miarę względnej ilości pracy, jaką zespół reagowania na incydenty musiał wykonać, a nie jako miarę jakości zespołu, chyba że jest rozważana w kontekście innych miar, które łącznie dają wskazanie jakości pracy. Bardziej efektywne jest tworzenie oddzielnych liczb incydentów dla każdej kategorii incydentów. Aby uzyskać więcej informacji, można również użyć podkategorii. Na przykład rosnąca liczba incydentów dokonywanych przez osoby mające dostęp do informacji wrażliwych może skutkować zaostrzeniem zasad dotyczących badania informacji o członkach personelu i niewłaściwego wykorzystania zasobów komputerowych oraz zastosowania silniejszych zabezpieczeń w sieciach

[36] Wskaźniki, takie jak liczba obsłużonych incydentów, generalnie nie mają wartości przy porównywaniu dla wielu organizacji, ponieważ każda organizacja prawdopodobnie inaczej definiuje kluczowe terminy. Na przykład, większość organizacji definiuje „incydent" w kategoriach swoich własnych zasad i praktyk, a to, co jedna organizacja uważa za pojedynczy incydent, może być przez inne uznane za wielokrotne incydenty. Bardziej szczegółowe wskaźniki, takie jak liczba skanów portów, również mają niewielką wartość w porównaniach prowadzonych przez organizacje. Na przykład, jest bardzo mało prawdopodobne, aby różne systemy bezpieczeństwa, takie jak czujniki wykrywania włamań do sieci, używały tych samych kryteriów przy oznaczaniu aktywności, jak przy skanowaniu portów.

wewnętrznych (np. wdrażanie oprogramowania do wykrywania włamań w większej liczbie sieci wewnętrznych i hostów).

- **Czas wykorzystany na obsługę incydentu**. W przypadku każdego zdarzenia, czas można mierzyć na kilka sposobów:
  - Całkowita ilość pracy poświęconej na incydent;
  - Czas, który upłynął od początku incydentu do jego wykrycia, do wstępnej oceny skutków oraz do każdego etapu procesu obsługi incydentu (np. powstrzymanie, odtworzenie);
  - Ile czasu zajęło zespołowi reagowania na incydenty udzielenie odpowiedzi na wstępne zgłoszenie incydentu;
  - Ile czasu zajęło zgłoszenie incydentu kierownictwu oraz w razie potrzeby odpowiednim podmiotom zewnętrznym (np. CSIRT poziomu krajowego).
- **Obiektywna ocena każdego incydentu.** Reakcję na incydent, który został rozwiązany, powinna zostać przeanalizowana w celu określenia, jaki był stopień jej skuteczności. Przykłady wykonania obiektywnej oceny incydentu:
  - Przeglądanie dzienników, formularzy, raportów i innej dokumentacji incydentów pod kątem przestrzegania ustalonych zasad i procedur reagowania na incydenty;
  - Określenie, które zwiastuny i wskaźniki incydentu zostały zarejestrowane, aby określić, jak skutecznie incydent został zarejestrowany i zidentyfikowany;
  - Ustalenie, czy incydent spowodował szkody, zanim został wykryty;
  - Ustalenie, czy zidentyfikowano rzeczywistą przyczynę incydentu, oraz określenie wektora ataku, wykorzystanych luk w zabezpieczeniach oraz charakterystyki docelowych lub dedykowanych systemów, sieci i aplikacji;
  - Ustalenie, czy incydent jest powtórzeniem poprzedniego incydentu;
  - Oszacowanie wstępnych szkód finansowych wynikających z incydentu (np. informacje i krytyczne procesy biznesowe, na które incydent miał negatywny wpływ);
  - Pomiar różnicy między wstępną oceną skutków, a ostateczną oceną skutków (zob. Rozdział 3.2.6);
  - Określenie, jakie środki, jeśli w ogóle istnieją, mogłyby zapobiec incydentowi.

- **Subiektywna ocena każdego incydentu.** Członkowie zespołu reagowania na incydenty mogą zostać poproszeni o ocenę wyników własnych, a także innych członków zespołu i całego zespołu. Innym cennym źródłem informacji jest właściciel zasobu, który został zaatakowany, w celu ustalenia, czy sądzi, że zdarzenie zostało obsłużone skutecznie i czy wynik był zadowalający.

Oprócz wykorzystywania tych wskaźników do mierzenia sukcesu zespołu, organizacje mogą również uznać za przydatne okresowe audytowanie programów reagowania na incydenty. Audyty zidentyfikują problemy i niedociągnięcia, które można następnie poprawić. Audyt reagowania na incydenty powinien co najmniej oceniać następujące elementy pod kątem obowiązujących przepisów, reguł i ogólnie przyjętych praktyk:

- Zasady, plany i procedury reagowania na incydenty.
- Narzędzia i zasoby.
- Model i struktura zespołu.
- Szkolenia i edukacja osób zajmujących się incydentami.
- Dokumentacja i raporty dotyczące incydentów.
- Mierniki sukcesu omówione wcześniej w tym rozdziale.

3.4.3. Retencja dowodów

Organizacje powinny ustalić zasady dotyczące tego, jak długo należy przechowywać dowody z incydentu. Większość organizacji decyduje się na przechowywanie wszystkich dowodów przez okres zgodny z obowiązującymi przepisami prawnymi. Podczas opracowywania zasad należy wziąć pod uwagę następujące czynniki:

- **Ściganie.** Jeśli jest prawdopodobne, że atakujący zostanie postawiony przed sądem, może być konieczne przechowywanie dowodów do czasu zakończenia wszystkich czynności prawnych. W niektórych przypadkach może to zająć kilka lat. Ponadto dowody, które wydają się teraz nieistotne, mogą stać się kluczowe w przyszłości. Na przykład, jeśli atakujący jest w stanie wykorzystać wiedzę zebraną podczas jednego ataku, aby później przeprowadzić poważniejszy atak, dowody z pierwszego ataku mogą być kluczowe dla wyjaśnienia, w jaki sposób drugi atak został dokonany.
- **Retencja danych.** Większość organizacji ma ustalone zasady retencji danych, które określają, jak długo można przechowywać określone typy danych. Na przykład organizacja może określić, że wiadomości e-mail powinny być przechowywane tylko przez 180 dni. Jeśli obraz dysku zawiera tysiące wiadomości e-mail, organizacja może

nie chcieć, aby był przechowywany dłużej niż 180 dni, chyba że jest to absolutnie konieczne. Jak omówiono w rozdziale 3.4.2, W podmiotach realizujących zadania publiczne czas retencji określają przepisy.

- **Koszty.** Oryginalny sprzęt (np. dyski twarde, systemy, których zabezpieczenia zostały naruszone), który jest przechowywany jako dowód, a także dyski twarde i nośniki wymienne używane do przechowywania obrazów dysków są na ogół niedrogie. Jeśli jednak organizacja przechowuje wiele takich komponentów przez lata, koszt może być znaczny. Organizacja musi również zachować funkcjonujące komputery, które mogą korzystać z magazynowanego sprzętu i nośników.

3.5. Lista kontrolna obsługi incydentu

Lista kontrolna w Tabeli 3-5 przedstawia główne kroki, które należy wykonać podczas postępowania z incydentem. Należy pamiętać, że faktycznie wykonywane czynności mogą się różnić w zależności od rodzaju zdarzenia i charakteru poszczególnych incydentów. Na przykład, jeśli osoba postępująca z incydentami dokładnie wie, na podstawie analizy wskaźników (krok 1.1), co się wydarzyło, może nie być potrzeby wykonywania kroków 1.2 lub 1.3 w celu dalszego zbadania działania. Lista kontrolna zawiera wytyczne dla osób postępujących z incydentami w zakresie głównych kroków, które należy wykonać. Nie narzuca dokładnej kolejności kroków, które należy bezwzględnie wykonywać.

Tabela 3-5. Lista kontrolna obsługi incydentu.

L.p.	Czynność	Ukończenie
Detekcja i analiza		
1.	Ustalenie, czy wystąpił incydent.	
1.1	Analiza zwiastunów i wskaźników.	
1.2	Analiza korelacji informacji.	
1.3	Przeprowadzenie badań (np. wyszukiwarki, bazy wiedzy)	
1.4	Z chwilą uznania przez obsługującego incydent uzna, że doszło do incydentu, rozpoczęcie dokumentowania dochodzenia i gromadzenia dowodów.	

2.	Ustalenie priorytetów obsługi incydentu w oparciu o istotne czynniki (wpływ na funkcjonowanie, wpływ na informacje, wysiłek związany z odtworzeniem itd.)	
3.	Zgłoszenie incydentu do właściwego CSIRT poziomu krajowego.	
Powstrzymanie, usunięcie i odtworzenie		
4.	Uzyskanie, zachowanie, zabezpieczenie i udokumentowanie dowodów.	
5.	Powstrzymanie incydentu.	
6.	Usunięcie incydentu.	
6.1	Identyfikacja i ograniczenie wykorzystanych podatności.	
6.2	Usunięcie złośliwego oprogramowania, nieodpowiednich materiałów i innych komponentów.	
6.3	Jeśli wykryto więcej zainfekowanych hostów (np. nowe infekcje złośliwym oprogramowaniem), powtórz kroki z Detekcji i analizy (pkt. 1.1, 1.2) żeby zidentyfikować wszystkie pozostałe zainfekowane hosty, następnie powstrzymaj (pkt. 5) i usuń incydent (pkt. 6).	
7.	Odtworzenie po incydencie.	
7.1	Przywrócenie dotkniętych systemów do stanu gotowości operacyjnej.	
7.2	Sprawdzenie, czy zainfekowane systemy funkcjonują normalnie.	
7.3	W razie potrzeby, implementacja dodatkowego monitoringu w celu poszukiwania powiązanych przyszłych aktywności.	
Aktywność po incydencie		
8.	Utworzenie raportu uzupełniającego.	

9.	Organizacja spotkania, na którym są wyciągane wnioski (obowiązkowo dla znacznych incydentów, opcjonalne dla innych przypadków).	

3.6. Rekomendacje

Najważniejsze zalecenia przedstawione w tej rozdziale dotyczące obsługi incydentów podsumowane zostały poniżej.

- **Zdobycie narzędzi i zasobów, które mogą być przydatne podczas obsługi incydentów.** Zespół będzie skuteczniejszy w obsłudze incydentów, jeśli będzie w posiadaniu dostępnych różnorodnych narzędzi i zasobów. Przykłady obejmują listy kontaktów, oprogramowanie szyfrujące, diagramy sieciowe, urządzenia do tworzenia kopii zapasowych, listy portów, oprogramowanie do kryminalistyki cyfrowej.
- **Zapobieganie występowaniu incydentów poprzez upewnienie się, że sieci, systemy i aplikacje są odpowiednio zabezpieczone.** Zapobieganie incydentom jest korzystne dla organizacji, a także zmniejsza obciążenie zespołu reagowania na incydenty. Dokonywanie okresowych ocen ryzyka i ograniczanie zidentyfikowanych zagrożeń do akceptowalnego poziomu, skutecznie ogranicza liczbę incydentów. Również bardzo ważna jest świadomość zasad i procedur bezpieczeństwa przez użytkowników, personel IT i kierownictwo.
- **Identyfikacja zwiastunów i wskaźników za pomocą alertów generowanych przez kilka rodzajów oprogramowania zabezpieczającego.** Systemy wykrywania włamań i zapobiegania im, oprogramowanie antywirusowe i oprogramowanie do sprawdzania integralności plików są przydatne w wykrywaniu oznak incydentów. Każdy rodzaj oprogramowania może wykrywać incydenty, których inne rodzaje oprogramowania nie są w stanie wykryć, dlatego zdecydowanie zaleca się korzystanie z kilku rodzajów oprogramowania zabezpieczającego komputery. Pomocne mogą być również usługi monitorowania zlecane firmom zewnętrznym.
- **Ustanowienie mechanizmów umożliwiających stronom zewnętrznym zgłaszanie incydentów.** Podmioty zewnętrzne mogą chcieć zgłaszać organizacji zidentyfikowane incydenty - na przykład mogą sądzić, że jeden z użytkowników organizacji, której zgłaszają incydent, atakuje ich zasoby. Organizacje powinny opublikować numer telefonu i adres e-mail kontaktowego, których strony zewnętrzne mogą używać do zgłaszania takich incydentów.

- **Wymaganie podstawowego poziomu rejestrowania i audytowania we wszystkich systemach oraz wyższego poziomu dla wszystkich systemów krytycznych.** Dzienniki z systemów operacyjnych, usług i aplikacji często dostarczają wartości podczas analizy incydentów, zwłaszcza jeśli włączono funkcję audytu. Dzienniki mogą zawierać informacje, takie jak konta, do których uzyskano dostęp i wykaz czynności, które zostały wykonane.
- **Utrzymywanie profili sieci i systemów.** Profilowanie mierzy cechy oczekiwanych poziomów aktywności, dzięki czemu można łatwiej zidentyfikować zmiany we wzorcach. Jeśli proces profilowania jest zautomatyzowany, odchylenia od oczekiwanych poziomów aktywności można szybko wykryć i zgłosić administratorom, co prowadzi do szybszego wykrywania incydentów i problemów operacyjnych.
- **Ustalenie normalnego zachowanie sieci, systemów i aplikacji.** Członkowie zespołu, którzy rozumieją normalne zachowanie, powinni łatwiej rozpoznawać nienormalne zachowanie. Tę wiedzę najlepiej można uzyskać, przeglądając wpisy dziennika i alerty zabezpieczeń. Osoby postępujące z incydentami powinny zapoznać się z typowymi danymi i mogą zbadać nietypowe wpisy, celem zdobycia większej wiedzy.
- **Utworzenie zasad retencji dzienników**. Informacje o zdarzeniu mogą być zapisane w kilku miejscach. Tworzenie i wdrażanie zasad przechowywania dziennika, które określają, jak długo należy przechowywać dane dziennika, może być niezwykle pomocne w analizie, ponieważ starsze wpisy dziennika mogą wskazywać na aktywność mającą na celu rozpoznanie lub wcześniejsze wystąpienia podobnych ataków.
- **Skorelowanie zdarzeń.** Dowody zdarzenia mogą być rejestrowane w kilku dziennikach. Korelowanie zdarzeń z wielu źródeł może być nieocenione w zbieraniu wszystkich dostępnych informacji na temat incydentu i sprawdzaniu, czy incydent miał miejsce.
- **Synchronizacja wszystkich zegarów hosta.** Jeśli urządzenia zgłaszające zdarzenia mają niespójne ustawienia zegara, korelacja zdarzeń będzie bardziej skomplikowana. Rozbieżności w zegarze mogą również powodować problemy z dowodowego punktu widzenia.
- **Utrzymywanie i korzystanie z bazy wiedzy.** Osoby zajmujące się obsługą muszą szybko odwoływać się do informacji podczas analizy incydentów. Scentralizowana baza wiedzy stanowi spójne, możliwe do utrzymania źródło informacji. Baza wiedzy

powinna zawierać ogólne informacje, takie jak dane o zwiastunach i wskaźniki poprzednich incydentów.

- **Rozpoczęcie rejestrowania wszystkich informacji, gdy tylko zespół zacznie podejrzewać, że doszło do incydentu.** Każdy podjęty krok, od momentu wykrycia incydentu do ostatecznego rozwiązania, powinien być udokumentowany i oznaczony datą i czasem. Informacje tego rodzaju mogą służyć jako dowód w sądzie, jeśli prowadzone jest postępowanie sądowe. Rejestrowanie wykonanych czynności może również prowadzić do bardziej wydajnej, systematycznej i mniej podatnej na błędy obsługi problemu.
- **Zabezpieczenie danych z incydentów.** Te dane zawierają wrażliwe informacje dotyczące takich kwestii jak luki w zabezpieczeniach, naruszenia bezpieczeństwa i użytkownicy, którzy mogli wykonywać niewłaściwe działania. Zespół powinien zapewnić, że dostęp do danych o incydentach jest odpowiednio ograniczony, zarówno logicznie, jak i fizycznie.
- **Ustalenie priorytetów obsługi incydentów na podstawie istotnych czynników.** Ze względu na ograniczone zasoby, incydenty nie powinny być obsługiwane na zasadzie „kto pierwszy, ten lepszy". Zamiast tego, organizacje powinny ustanowić pisemne wytyczne, które określają, jak szybko zespół musi zareagować na incydent i jakie działania należy wykonać w oparciu o istotne czynniki, takie jak funkcjonalny i informacyjny wpływ incydentu oraz prawdopodobna możliwość odzyskania po incydencie. Oszczędza to czas osób obsługujących incydenty i zapewnia kierownictwu i właścicielom systemu uzasadnienie ich działań. Organizacje powinny również ustanowić proces eskalacji dla tych przypadków, gdy zespół nie reaguje na incydent w wyznaczonym czasie.
- **Uwzględnienie w zasadach reagowania na incydenty organizacji postanowień dotyczących zgłaszania incydentów.** Organizacje powinny określić, które incydenty należy zgłaszać, kiedy i komu. Najczęściej powiadamianymi stronami są: członek kierownictwa ds. bezpieczeństwa informacji, dyrektor ds. bezpieczeństwa informacji, specjalista ds. bezpieczeństwa informacji, inne zespoły reagowania na incydenty w organizacji oraz właściciele systemów. Należy przy tym pamiętać, że niektóre kategorie incydentów muszą być zgłaszane zgodnie z obowiązującymi przepisami
- **Ustanowienie strategii i procedur powstrzymywania incydentów.** Ważne jest, aby szybko i skutecznie ograniczać incydenty, zmniejszając ich wpływ na działalność. Organizacje powinny zdefiniować dopuszczalne ryzyko związane

z powstrzymywaniem incydentów i opracować odpowiednie strategie i procedury. Strategie powstrzymywania powinny różnić się w zależności od rodzaju incydentu.

- **Przestrzeganie ustalonych procedur gromadzenia i postępowania z dowodami.** Zespół powinien zrozumiale udokumentować sposób zachowania wszystkich dowodów. Dowody powinny być zawsze rozliczane. Zespół powinien spotkać się z personelem prawnym i organami ścigania w celu omówienia postępowania z dowodami, a następnie, na podstawie tych dyskusji, opracować procedury.
- **Retencja ulotnych danych z systemów jako dowodów.** Obejmuje to listy połączeń sieciowych, procesów, sesji logowania, otwartych plików, konfiguracji interfejsów sieciowych i zawartości pamięci. Wykonywanie starannie dobranych poleceń z zaufanych nośników, może dostarczyć niezbędnych informacji bez uszkadzania dowodów systemu.
- **Uzyskiwanie z systemu wstępnych zrzutów pełnych obrazów dysków do badań sądowych, a nie z kopii zapasowych systemu plików.** Obrazy dysków powinny być wykonane na oczyszczonych nośnikach zabezpieczonych przed zapisem lub nośników jednokrotnego zapisu. Proces ten, dla celów śledczych i dowodowych, jest bardziej wiarygodny niż wykonywany z kopi zapasowej systemu plików. Obrazowanie jest również cenne, ponieważ znacznie bezpieczniej jest analizować obraz niż przeprowadzać analizę na oryginalnym systemie, ponieważ analiza może nieumyślnie zmienić oryginał.

  Organizowanie spotkań na temat zdobytego doświadczenia po poważniejszych incydentach. Spotkania, na których wyciągane są wnioski, są niezwykle pomocne w doskonaleniu środków bezpieczeństwa i samego procesu obsługi incydentów.

4. KOORDYNACJA I WYMIANA INFORMACJI

Charakter współczesnych zagrożeń i ataków sprawia, że współpraca organizacji podczas reagowania na incydenty jest ważniejsza niż kiedykolwiek. Organizacje powinny zapewnić, że skutecznie koordynują część swoich działań w zakresie reagowania na incydenty z odpowiednimi partnerami. Najważniejszym aspektem koordynacji reagowania na incydenty jest wymiana informacji, podczas której różne organizacje przekazują informacje o zagrożeniach, atakach i słabych punktach, po to, aby każda z organizacji czerpała wiedzę z doświadczenia pozostałych organizacji. Udostępnianie informacji o incydentach jest często korzystne dla obu stron, ponieważ te same zagrożenia i ataki często wpływają na wiele organizacji jednocześnie.

Jak wspomniano w rozdziale 2, koordynacja i udostępnianie informacji organizacjom partnerskim może wzmocnić zdolność organizacji do skutecznego reagowania na incydenty. Na przykład, jeśli organizacja zidentyfikuje zachowanie w swojej sieci, które wydaje się podejrzane i wyśle informacje o zdarzeniu do grupy zaufanych partnerów, ktoś inny z adresatów informacji mógł już zauważyć podobne zachowanie i być w stanie odpowiedzieć, podając dodatkowe szczegóły dotyczące podejrzanego działania, w tym sygnatury, inne wskaźniki, których należy szukać, lub sugerowane działania naprawcze. Współpraca z zaufanym partnerem może umożliwić organizacji szybszą i skuteczniejszą reakcję na incydent niż organizacja działająca w izolacji.

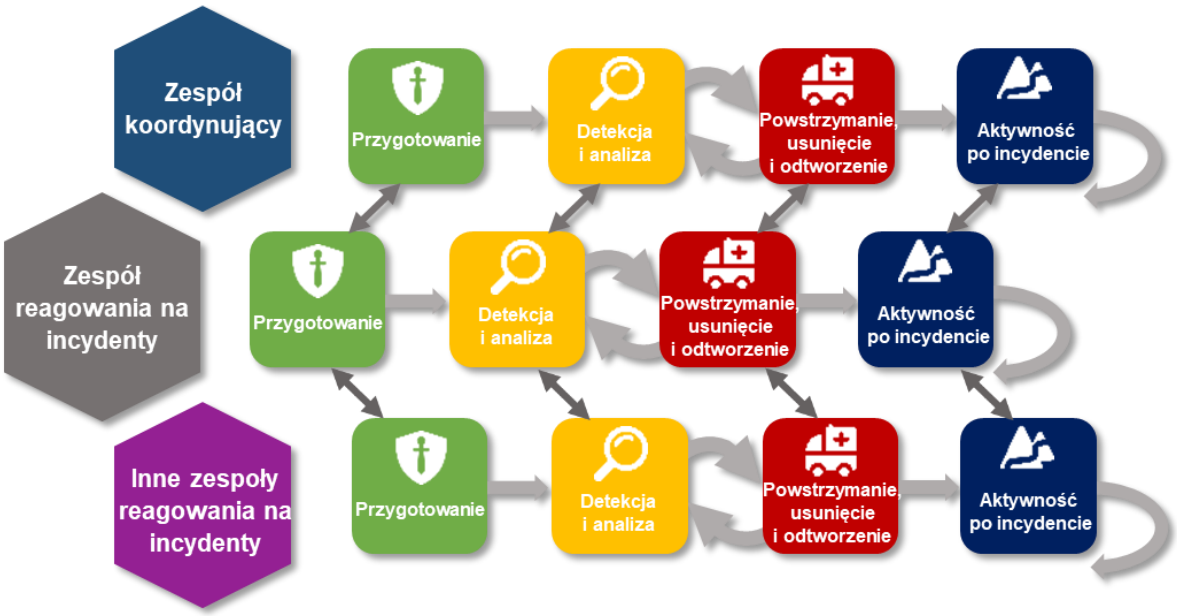
Ten wzrost wydajności standardowych technik reagowania na incydenty nie jest jedyną motywacją do koordynacji między organizacjami i wymiany informacji. Inną zachętą do wymiany informacji jest możliwość reagowania na incydenty przy użyciu technik, które mogą nie być dostępne dla pojedynczej organizacji, zwłaszcza jeśli jest to organizacja małej lub średniej wielkości. Na przykład mała organizacja, która zidentyfikuje szczególnie złożone wystąpienie złośliwego oprogramowania w swojej sieci, może nie mieć własnych zasobów, aby w pełni przeanalizować złośliwe oprogramowanie i określić jego wpływ na system. W tym przypadku organizacja może być wykorzystać zaufaną sieć wymiany informacji, aby skutecznie zlecić analizę tego złośliwego oprogramowania zasobom stron trzecich, które mają odpowiednie możliwości techniczne do przeprowadzenia analizy złośliwego oprogramowania.

W tej części dokumentu zwraca się uwagę na koordynację i wymianę informacji. Rozdział 4.1 przedstawia przegląd koordynacji reagowania na incydenty i koncentruje się na potrzebie koordynacji między organizacjami w celu uzupełnienia procesów reagowania na incydenty w organizacji. Rozdział 4.2 omawia techniki udostępniania informacji między organizacjami,

natomiast rozdział 4.3 analizuje, jak ograniczyć do niezbędnych informacje udostępniane innym organizacjom.

4.1. Koordynacja

Jak omówiono w rozdziale 2.3.4, organizacja, w trakcie prowadzenia działań reagowania na incydenty, może posiadać potrzebę współdziałania z kilkoma rodzajami organizacji zewnętrznych. Przykładami takich organizacji są zespoły CSIRT poziomu krajowego i inne zespoły reagowania na incydenty, organy ścigania, dostawcy usług internetowych oraz zleceniodawcy i klienci. Zespół reagowania na incydenty organizacji powinien zaplanować koordynację incydentów z tymi stronami przed wystąpieniem incydentów, aby zapewnić, że wszystkie strony znają swoje role, i że ustanowiono skuteczne linie komunikacji. Rysunek 4-1 przedstawia przykładowy sposób przeprowadzania przez organizację koordynacji obsługi incydentu w każdym etapie cyklu życia reakcji na incydent, podkreślając, że koordynacja jest wartością w całym cyklu życia.



Rysunek 4-1. Koordynacja obsługi incydentu.

4.1.1. Relacje koordynacyjne

Zespół reagowania na incydenty w organizacji może uczestniczyć w różnego rodzaju uzgodnieniach dotyczących koordynacji, w zależności od rodzaju organizacji, z którymi współpracuje. Na przykład, członkowie zespołu odpowiedzialni za techniczne szczegóły reagowania na incydenty mogą koordynować współpracę ze współpracownikami

operacyjnymi w organizacjach partnerskich, aby dzielić się strategiami łagodzenia ataku obejmującego wiele organizacji. Alternatywnie, podczas tego samego incydentu, kierownik zespołu reagowania na incydent może współpracować z ISAC, o ile został powołany, w celu spełnienia niezbędnych wymogów sprawozdawczych oraz uzyskiwać porady i dodatkowe zasoby, aby skutecznie zareagować na incydent. Tabela 4-1 zawiera kilka przykładów relacji koordynacyjnych, które mogą istnieć podczas współpracy z organizacjami zewnętrznymi.

Kategoria	Definicja	Wymieniane informacje
Zespół-do-zespołu	Relacje między zespołami występują zawsze, gdy personel techniczny reagujący na incydenty w różnych organizacjach, współpracuje ze swoimi odpowiednikami w każdym etapie cyklu obsługi incydentu. Organizacje uczestniczące w tego typu relacjach są zazwyczaj równorzędnie, bez żadnej władzy nad sobą i decydują się na dzielenie się informacjami, łączenie zasobów i ponowne wykorzystywanie wiedzy do rozwiązywania problemów wspólnych dla obu zespołów.	Informacje najczęściej wymieniane w relacjach między zespołami mają charakter taktyczny i techniczny (np. techniczne wskaźniki naruszenia, sugerowane działania naprawcze), ale mogą również obejmować inne rodzaje informacji (plany, procedury, wyciągnięte wnioski), jeśli są prowadzone w ramach fazy przygotowawczej.
Zespół-do-koordynatora	Relacje między zespołem i zespołem koordynującym istnieją między organizacyjnym zespołem reagowania na incydenty, a odrębną organizacją, która	Zespoły reagowania i zespoły koordynujące często udostępniają informacje taktyczne, techniczne, a także informacje dotyczące zagrożeń, słabych punktów

Kategoria	Definicja	Wymieniane informacje
	funkcjonuje jako centralny punkt skoordynowanej reakcji na incydenty i zarządzania, taką CSIRT NASK. Ten rodzaj relacji może obejmować obowiązek wykonywania sprawozdawczości, wymagany od organizacji członkowskich przez organ koordynujący, a także oczekiwanie, że zespół koordynujący, w odpowiednim czasie, rozpowszechni wśród uczestniczących organizacji członkowskich użyteczne informacje.	i zagrożeń dla społeczności obsługiwanej przez zespół koordynujący. Zespół koordynujący może również wymagać szczegółowych informacji o wpływie na incydenty, aby pomóc w podejmowaniu decyzji, gdzie należy skoncentrować swoje zasoby i uwagę.
Zespół koordynujący -do-zespół koordynujący	Relacje między wieloma zespołami koordynującymi tworzone są w celu wymiany informacji dotyczących incydentów przekrojowych, które mogą mieć wpływ na wiele społeczności. Zespoły koordynujące, w celu wsparcia reakcji między społecznościami, działają w imieniu swoich organizacji członkowskich w celu wymiany informacji na temat charakteru i zakresu incydentów przekrojowych	Typ informacji wymienianych przez zespoły koordynujące z ich odpowiednikami często składa się z okresowych podsumowań podczas operacji w stanie ustalonym, dokonywanych podczas wymiany szczegółów taktycznych, technicznych, planów reagowania oraz informacji o ocenie wpływu lub ryzyka podczas skoordynowanych działań reagowania na incydenty.

Kategoria	Definicja	Wymieniane informacje
	oraz strategii łagodzenia skutków ponownego ich użycia.	

Zbudowanie relacji potrzebnych do koordynacji może okazać się dla organizacji trudnym zadaniem. Dobre miejsca na rozpoczęcie budowania wspólnoty obejmują sektor przemysłu, do którego należy organizacja, oraz region geograficzny, w którym działa organizacja. Zespół reagowania na incydenty organizacji może próbować nawiązać relacje z innymi zespołami (na poziomie między zespołami) w ramach własnego sektora i regionu lub dołączyć do ugruntowanych organów w branży, które już ułatwiają wymianę informacji. Inną kwestią przy budowaniu relacji jest to, że niektóre relacje są obowiązkowe, a inne dobrowolne . Na przykład, relacje między zespołem, a koordynatorem są często obowiązkowe, podczas gdy relacje między zespołami są zwykle dobrowolne. Organizacje dążą do dobrowolnych relacji, ponieważ realizują wspólne interesy. Obowiązkowe relacje są zwykle definiowane przez organ regulacyjny w branży lub przez inny podmiot.

4.1.2. Uzgodnienia dotyczące wymiany informacji i wymogi sprawozdawcze

Organizacje próbujące udostępniać informacje organizacjom zewnętrznym, powinny skonsultować się ze swoim działem prawnym przed podjęciem jakichkolwiek działań koordynacyjnych. Przykładem jest umowa o zachowaniu poufności (NDA) mająca na celu ochronę poufności najbardziej wrażliwych informacji organizacji. `Techniki wymiany informacji`

Udostępnianie informacji jest kluczowym elementem umożliwiającym koordynację między organizacjami. Nawet najmniejsze organizacje muszą mieć możliwość udostępniania informacji o incydentach współpracownikom i partnerom, aby skutecznie radzić sobie z wieloma incydentami. Organizacje powinny udostępniać takie informacje przez cały cykl reagowania na incydent, nie czekając, aż incydent zostanie w pełni rozwiązany przed

udostępnieniem jego szczegółów innym. W rozdziale 4.3 omówiono rodzaje informacji o incydentach, które organizacje mogą, ale nie muszą udostępniać innym. Rozdział ten koncentruje się na technikach wymiany informacji. Sekcja 4.2.1 dotyczy metod doraźnych (*ang. ad hoc*), podczas gdy sekcja 4.2.2 analizuje metody częściowo zautomatyzowane. Podrozdział 4.2.3 omawia kwestie bezpieczeństwa związane z udostępnianiem informacji.

4.1.3. Metody doraźne (ad hoc)

Większość informacji o incydentach jest udostępniana tradycyjnie metodami *ad hoc*, takimi jak poczta e-mail, komunikatory internetowe i telefon. Mechanizmy udostępniania informacji *ad hoc* zwykle opierają się na powiązaniach poszczególnych pracowników z pracownikami zespołów reagowania na incydenty organizacji partnerskich. Pracownik wykorzystuje te kontakty, aby ręcznie udostępniać informacje współpracownikom i koordynować z nimi tworzenie strategii reagowania na incydenty. W zależności od wielkości organizacji, techniki *ad hoc* mogą być najbardziej efektywnym sposobem wymiany informacji z organizacjami partnerskimi. Jednak ze względu na nieformalny charakter wymiany informacji *ad hoc,* nie można zagwarantować, że procesy udostępniania informacji będą zawsze działały. Na przykład, jeśli szczególnie dobrze skomunikowany pracownik zrezygnuje z zespołu reagowania na incydenty, zespół ten może chwilowo stracić większość kanałów wymiany informacji, na których opiera się efektywna koordynacja z organizacjami zewnętrznymi.

Metody wymiany informacji *ad hoc* są również w dużej mierze nie znormalizowane pod względem tego, jakie informacje są przekazywane i jak odbywa się ta komunikacja. Ze względu na brak standaryzacji wymagają one ręcznej obsługi i wymagają większej ilości zasobów w przetwarzaniu niż alternatywne, częściowo zautomatyzowane metody. Gdy tylko jest to możliwe, organizacja powinna próbować sformalizować swoje strategie wymiany informacji poprzez formalne umowy z organizacjami partnerskimi i mechanizmy techniczne, które pomogą częściowo zautomatyzować wymianę informacji.

4.1.4. Metody częściowo zautomatyzowane

Projektując zautomatyzowane rozwiązania do udostępniania informacji, organizacje powinny najpierw rozważyć, jakie rodzaje informacji będą wymieniane z partnerami. Organizacja może chcieć skonstruować formalny słownik danych wymieniający wszystkie jednostki i relacje między jednostkami, które będą chciały udostępniać. Gdy organizacja pozna typy informacji, które będą udostępniane, konieczne jest skonstruowanie formalnych modeli przetwarzalnych maszynowo, aby pozyskiwać te informacje. W miarę możliwości organizacja powinna wykorzystywać istniejące standardy wymiany danych do przedstawiania informacji,

które muszą udostępniać. Organizacja powinna współpracować ze swoimi organizacjami partnerskimi przy podejmowaniu decyzji dotyczących modeli wymiany danych, aby zapewnić zgodność wybranych standardów z systemami reagowania na incydenty organizacji partnerskiej. Wybierając istniejące modele wymiany danych, organizacje mogą preferować wybór wielu modeli, które formują różne aspekty dziedziny reagowania na incydenty, a następnie wykorzystują te modele w sposób modułowy, przekazując tylko informacje potrzebne w określonym momencie podejmowania decyzji w cyklu życia. Załącznik E zawiera otwartą listę istniejących standardów definiujących modele wymiany danych, które mają zastosowanie w dziedzinie reagowania na incydenty.

Oprócz wyboru modeli wymiany danych w celu udostępniania informacji o incydentach, organizacja musi również współpracować ze swoimi organizacjami partnerskimi w celu uzgodnienia technicznych mechanizmów komunikacyjnych umożliwiających wymianę informacji w sposób zautomatyzowany. Te mechanizmy komunikacji obejmują co najmniej protokół transportowy do wymiany informacji, model architektoniczny komunikacji z zasobem informacyjnym oraz odpowiednie porty i nazwy domen umożliwiające dostęp do zasobu informacyjnego w określonej organizacji. Na przykład grupa organizacji partnerskich może zdecydować o wymianie informacji o zdarzeniach przy użyciu architektury REST (*ang. Representational State Transfer*) w celu wymiany danych IODEF / Real-Time Inter-Network Defense (RID) za pośrednictwem protokołu HTTPS (ang. *Hypertext Transfer Protocol Secure*) na porcie 4590 danej nazwy domeny w strefie DMZ każdej organizacji.

4.1.5. Względy bezpieczeństwa

Istnieje kilka kwestii dotyczących bezpieczeństwa, które zespoły reagowania na incydenty powinny wziąć pod uwagę podczas planowania udostępniania informacji. Jednym z nich jest zdolność określania, kto i jakie elementy informacji o zdarzeniu może zobaczyć (np. ochrona informacji wrażliwych). Może być również konieczne wykonanie sanityzacji lub czyszczenia danych w celu usunięcia wrażliwych fragmentów danych z informacji o incydencie, bez naruszania informacji o zwiastunach, wskaźnikach i innych informacjach technicznych. Więcej informacji na temat szczegółowego udostępniania informacji zawiera rozdział 4.3. Zespół reagowania na incydenty powinien również zapewnić podjęcie niezbędnych środków w celu ochrony informacji udostępnianych zespołowi przez inne organizacje.

Istnieje również wiele kwestii prawnych do rozważenia dotyczących udostępniania danych. Dodatkowe informacje znajdują się w sekcji 4.1.2.

4.2. Szczątkowa wymiana informacji

Organizacje muszą zrównoważyć korzyści płynące z wymiany informacji z wadami udostępniania informacji wrażliwych, udostępniając odpowiednim stronom tylko i wyłącznie niezbędne informacje. Organizacje mogą myśleć o swoich informacjach o incydentach jak o dwóch rodzajach informacji: wpływach biznesowych i technicznych. Informacje o wpływie na biznes są często udostępniane w kontekście relacji między zespołem, a zespołem koordynującym, jak określono w sekcji 4.1.1, podczas gdy informacje techniczne są często udostępniane w ramach wszystkich trzech rodzajów relacji koordynacyjnych. W tym rozdziale omówiono oba typy informacji i przedstawiono zalecenia dotyczące szczegółowego udostępniania informacji.

4.2.1. Informacje o wpływie na biznes

Informacje o wpływie na biznes dotyczą tego, jak incydent wpływa na organizację pod względem kategorii misji, wpływu finansowego itp. Takie informacje, przynajmniej na poziomie podsumowania, są często zgłaszane zespołom koordynującym reagowanie na incydenty wyższego szczebla, w celu przekazania oszacowania szkód. spowodowanych przez incydent. Koordynacja zespołów reagowania może potrzebować informacji o wpływie do podejmowania decyzji dotyczących stopnia pomocy, jakiej należy udzielić organizacji zgłaszającej. Zespół koordynujący może również wykorzystać te informacje do podejmowania decyzji dotyczących tego, jak określone zdarzenie wpłynie na inne organizacje w społeczności, którą reprezentują.

Zespoły koordynujące mogą wymagać od organizacji członkowskich przedstawienia określonego rodzaju informacji o wpływie na biznes. Na przykład, zespół koordynujący może wymagać, aby organizacja członkowska zgłaszała informacje o wpływie używając kategorii określonych w sekcji 3.2.6. W takim przypadku, dla hipotetycznego incydentu, organizacja zgłosiłaby, że ma on *średni* wpływ funkcjonalny, *brak* wpływu informacyjnego i będzie wymagał *wydłużonego* czasu odzyskiwania. Te informacje wysokiego poziomu ostrzegają zespół koordynujący, że organizacja członkowska wymaga pewnego poziomu dodatkowych zasobów, aby odzyskać sprawność po incydencie. Zespół koordynujący mógłby następnie przeprowadzić dodatkową komunikację z organizacją członkowską, aby określić, na podstawie dostarczonych informacji technicznych o incydencie, ile i jaki rodzaj zasobów jest wymagany.

Informacje o wpływie na biznes są przydatne tylko do zgłaszania organizacjom, które są zainteresowane zapewnieniem misji organizacji, która doświadcza incydentu. W wielu przypadkach zespoły reagowania na incydenty powinny unikać udostępniania informacji o

wpływie na działalność organizacjom zewnętrznym, chyba że istnieje jasna propozycja wartości lub formalne wymogi dotyczące raportowania. Dzieląc się informacjami z organizacjami rówieśniczymi i partnerskimi, zespoły reagowania na incydenty powinny skupić się na wymianie informacji technicznych, jak opisano w rozdziale 4.3.2.

4.2.2. Informacje techniczne

Istnieje wiele różnych typów wskaźników technicznych wskazujących na wystąpienie incydentu w organizacji. Wskaźniki te pochodzą z różnorodnych informacji technicznych związanych z incydentami, takich jak nazwy hostów i adresy IP atakujących hostów, próbki złośliwego oprogramowania, zwiastuny i wskaźniki podobnych incydentów oraz rodzaje luk w zabezpieczeniach wykorzystanych w incydencie. Rozdział 3.2.2 zawiera przegląd tego, w jaki sposób organizacje powinny gromadzić i wykorzystywać te wskaźniki, aby móc zidentyfikować trwający incydent. Ponadto zawiera listę typowych źródeł danych dotyczących wskaźników incydentów.

Chociaż organizacje czerpią korzyści ze zbierania własnych wewnętrznych wskaźników, mogą zyskać dodatkową wartość, analizując wskaźniki otrzymane od organizacji partnerskich i udostępniając wewnętrzne wskaźniki do zewnętrznej analizy i wykorzystania. Jeśli organizacja otrzyma zewnętrzne dane wskaźnikowe odnoszące się do incydentu, którego nie zdiagnozowała, może wykorzystać te dane wskaźnikowe do zidentyfikowania incydentu, który zaczyna się pojawiać. Podobnie organizacja może wykorzystać zewnętrzne dane wskaźnikowe do wykrycia trwającego incydentu, o którym nie była świadoma z powodu braku wewnętrznych zasobów do przechwytywania określonych danych wskaźnikowych. Organizacje mogą również skorzystać na udostępnianiu swoich wewnętrznych danych wskaźnikowych organizacjom zewnętrznym. Na przykład, jeśli dzielą się informacjami technicznymi dotyczącymi incydentu, którego doświadczają, organizacja partnerska może zareagować sugerowaną strategią naprawczą w celu obsługi tego incydentu.

Organizacje powinny udostępniać jak najwięcej tych informacji. Jednak mogą istnieć przyczyny związane z bezpieczeństwem i odpowiedzialnością, z powodu których organizacja nie może ujawniać szczegółów wykorzystanej luki. Wskaźniki zewnętrzne, takie jak ogólna charakterystyka ataków i tożsamość atakujących hostów, można zwykle bezpiecznie udostępniać innym. Organizacje powinny rozważyć, które rodzaje informacji technicznych powinny lub nie powinny być udostępniane różnym stronom, a następnie starać się udostępniać jak najwięcej odpowiednich informacji innym organizacjom.

Dane wskaźników technicznych są przydatne, gdy pozwalają organizacji zidentyfikować rzeczywisty incydent. Jednak nie wszystkie dane wskaźnikowe otrzymane ze źródeł

zewnętrznych będą dotyczyły organizacji je otrzymującej. W niektórych przypadkach te dane zewnętrzne będą generować fałszywe alarmy w sieci organizacji przyjmującej i mogą powodować zaangażowanie zasobów na nieistniejące problemy.

Organizacje uczestniczące w wymianie informacji o incydentach powinny posiadać personel wykwalifikowany w pozyskiwaniu informacji ze wskaźników technicznych od społeczności udostępniających i rozpowszechnianiu tych informacji w całym przedsiębiorstwie, najlepiej w sposób zautomatyzowany. Organizacje powinny również starać się zapewnić, aby dzielić się tylko wskaźnikiem, co do którego mają stosunkowo wysoki poziom pewności, że oznacza on rzeczywisty incydent.

4.3. Rekomendacje

Najważniejsze zalecenia przedstawione w tej części rozdziału dotyczące obsługi incydentów podsumowano poniżej.

- **Zaplanowanie koordynacji incydentów ze stronami zewnętrznymi przed wystąpieniem incydentów.** Przykładami stron zewnętrznych są inne zespoły reagowania na incydenty, organy ścigania, dostawcy usług internetowych oraz zleceniodawcy i klienci. Takie planowanie pomaga zapewnić, że wszystkie strony znają swoje role i ustanowione są skuteczne linie komunikacji.
- **Konsultowanie z działem prawnym przed podjęciem jakichkolwiek działań.** Przed rozpoczęciem rozmów konieczne może być wprowadzenie umów lub innych porozumień z innymi podmiotami.
- **Udostępnianie informacji o incydencie przez cały cykl reakcji na incydent.** Udostępnianie informacji jest kluczowym elementem umożliwiającym koordynację między organizacjami. Organizacje nie powinny czekać, aż incydent zostanie w pełni rozwiązany, przed udostępnieniem jego szczegółów innym podmiotom.
- **Automatyzacja jak największej części procesu wymiany informacji**. Dzięki temu koordynacja między organizacjami jest wydajna i opłacalna. Organizacje powinny próbować osiągnąć równowagę zautomatyzowanej wymiany informacji i procesów zarządzania przepływem informacji przez personel.
- **Zrównoważenie korzyści wynikające z udostępniania informacji z wadami udostępniania informacji wrażliwych.** Idealnie byłoby, gdyby organizacje dzieliły się z odpowiednimi stronami tylko i wyłącznie informacjami niezbędnymi. Informacje o wpływie na biznes są często udostępniane w ramach relacji między zespołem, a zespołem koordynującym, podczas gdy informacje techniczne są często

udostępniane w ramach wszystkich rodzajów relacji koordynacyjnych. Dzieląc się informacjami z organizacjami równorzędnymi i partnerskimi, zespoły reagowania na incydenty powinny skupić się na wymianie informacji technicznych.

- **Udostępnianie innym organizacjom jak najwięcej odpowiednich informacji o zdarzeniach**. Organizacje powinny rozważyć, jakie rodzaje informacji technicznych powinny lub nie powinny być udostępniane innym stronom. Na przykład, wskaźniki zewnętrzne, takie jak ogólna charakterystyka ataków i tożsamość atakujących hostów, są zwykle bezpieczne do udostępnienia innym, ale mogą istnieć zarówno powody związane z bezpieczeństwem, jak i odpowiedzialnością, dla których organizacja nie chciałaby ujawniać szczegółów wykorzystanej słabości.

ZAŁĄCZNIK A: SCENARIUSZE OBSŁUGI INCYDENTÓW

Scenariusze obsługi incydentów zapewniają niedrogi i skuteczny sposób budowania umiejętności reagowania na incydenty i identyfikowania potencjalnych problemów z procesami reagowania na incydenty. Zespołowi reagowania na incydenty lub członkom zespołu przedstawia się scenariusz i listę powiązanych pytań. Następnie zespół omawia każde pytanie i określa najbardziej prawdopodobną odpowiedź. Celem jest ustalenie, co naprawdę zrobiłby zespół i porównanie tego z zasadami, procedurami i ogólnie zalecanymi praktykami w celu zidentyfikowania rozbieżności lub braków. Na przykład, brak odpowiedzi na wszystkie pytania może wskazywać, że reakcja byłaby opóźniona, ponieważ zespołowi brakuje oprogramowania lub z powodu braku wsparcia przez inny zespół poza godzinami pracy.

Poniższe pytania mają zastosowanie do prawie każdego scenariusza. Po każdym pytaniu następuje odniesienie do odpowiedniego rozdziału publikacji. Po pytaniach znajdują się scenariusze, z których każdy jest poprzedzony dodatkowymi pytaniami dotyczącymi konkretnego zdarzenia. Zachęca się organizacje do dostosowania tych pytań i scenariuszy do wykorzystania we własnych ćwiczeniach reagowania na incydenty[37].

A.1 Pytania do scenariusza

Przygotowanie:

1. Czy organizacja uznałaby to działanie za incydent? Jeśli tak, którą z zasad organizacji narusza to działanie? *(Rozdział 2.1)*
2. Jakie środki podjęto, aby zapobiec wystąpieniu tego typu incydentu lub ograniczyć jego skutki? *(Rozdział 3.1.2)*

Detekcja i analiza:

1. Jakie zwiastuny incydentu, jeśli w ogóle, organizacja może wykryć? Czy jakiekolwiek zwiastuny skłoniłyby organizację do podjęcia działań przed wystąpieniem incydentu? *(Rozdziały 3.2.2; 3.2.3)*
2. Jakie wskaźniki incydentu może wykryć organizacja? Jakie wskaźniki sprawiłyby, że pojawiłyby się podejrzenia, że mogło dojść do jakiegoś incydentu? ? *(Rozdziały 3.2.2; 3.2.3)*

[37] Aby uzyskać dodatkowe informacje na temat ćwiczeń, zobacz NIST SP 800-84, Przewodnik po programach testów, szkoleń i ćwiczeń na potrzeby planów i zastosowań IT.

3. Jakie dodatkowe narzędzia mogą być potrzebne do wykrycia tego konkretnego incydentu? *(Rozdział 3.2.3)*
4. W jaki sposób zespół reagowania na incydent przeanalizowałby i zweryfikował ten incydent? Jaki personel brałby udział w procesie analizy i weryfikacji? *(Rozdział 3.2.4)*
5. Jakim osób i grupom w organizacji zespół zgłosiłby incydent? *(Rozdział 3.2.7)*
6. Jak zespół określiłby priorytety w postępowaniu z tym incydentem? *(Rozdział 3.2.6)*

Powstrzymanie, usuwanie i odtwarzanie:

1. Jaką strategię powinna obrać organizacja, aby powstrzymać incydent? Dlaczego ta strategia jest lepsza od innych? (Rozdział 3.3.1)
2. Co mogłoby się stać, gdyby incydent nie został powstrzymany? *(Rozdział 3.3.1)*
3. Jakie dodatkowe narzędzia mogą być potrzebne, aby zareagować na ten konkretny incydent? *(Rozdziały 3.3.1; 3.3.4)*
4. Jaki personel byłby zaangażowany w procesy powstrzymywania, usuwania i / lub odtwarzania? *(Rozdziały 3.3.1, 3.3.4)*
5. Jakie źródła dowodów, jeśli w ogóle, organizacja powinna zdobyć? Jak można uzyskać dowody? Gdzie byłyby przechowywane? Jak długo powinny być przechowywane? *(Rozdziały 3.2.5, 3.3.2, 3.4.3)*

Aktywność po incydencie:

1. Kto wziąłby udział w spotkaniu dotyczącym tego incydentu? *(Rozdział 3.4.1)*
2. Co można zrobić, aby zapobiec podobnym incydentom w przyszłości? *(Rozdział 3.1.2)*
3. Co można zrobić, aby poprawić wykrywanie podobnych incydentów? *(Rozdział 3.1.2)*

Ogólne pytania:

1. Ilu członków zespołu reagowania na incydenty uczestniczyłoby w obsłudze tego incydentu? *(Rozdział 2.4.3)*
2. Oprócz zespołu reagowania na incydenty, jakie grupy w organizacji byłyby zaangażowane w obsługę tego incydentu? *(Rozdział 2.4.4)*
3. Jakim podmiotom zewnętrznym, zespół zgłosiłby incydent? Kiedy miałoby się pojawić zgłoszenie? Jak wyglądałby raport? Jakie informacje zgłosiłby lub nie i dlaczego? *(Rozdział 2.3.2)*

4. Jakie inne komunikaty mogą być wymieniane ze stronami zewnętrznymi? *(Rozdział 2.3.2)*
5. Jakich narzędzi i zasobów użyłby zespół do obsługi tego incydentu? (*Rozdział 3.1.1)*
6. Jakie aspekty obsługi byłyby inne, gdyby incydent miał miejsce w innym dniu i o innej godzinie (w godzinach pracy i poza nimi)? *(Rozdział 2.4.2)*
7. Jakie aspekty obsługi byłyby inne, gdyby incydent miał miejsce w innej fizycznej lokalizacji (w siedzibie firmy lub poza nią)? *(Rozdział 2.4.2)*

A.2 Scenariusze

Scenariusz 1: Odmowa usługi (DoS) serwera DNS

W sobotnie popołudnie użytkownicy zewnętrzni mają problemy z dostępem do publicznych witryn internetowych organizacji. W ciągu następnej godziny problem pogarsza się do tego stopnia, że prawie każda próba uzyskania dostępu kończy się niepowodzeniem.
W międzyczasie członek personelu sieciowego organizacji reaguje na alerty z routera brzegowego i stwierdza, że przepustowość dostępu do Internetu w organizacji jest zużywana przez niezwykle dużą ilość pakietów protokołu UDP (*ang. User Datagram Protocol)* do i z obu publicznych serwerów DNS organizacji. Analiza ruchu pokazuje, że serwery DNS otrzymują duże ilości żądań z jednego zewnętrznego adresu IP. Ponadto wszystkie żądania DNS z tego adresu pochodzą z tego samego portu źródłowego.

Poniżej znajdują się dodatkowe pytania dotyczące tego scenariusza:

1. Z kim organizacja powinna się skontaktować w sprawie zewnętrznego adresu IP?
2. Załóżmy, że po wprowadzeniu wstępnych środków bezpieczeństwa administratorzy sieci wykryli, że dziewięć hostów wewnętrznych również próbowało wykonać te same nietypowe żądania do serwera DNS. Jak to wpłynie na obsługę tego incydentu?
3. Załóżmy, że dwa z dziewięciu hostów wewnętrznych odłączyły się od sieci, zanim zidentyfikowano właścicieli ich systemów. W jaki sposób zostaliby zidentyfikowani właściciele systemu?

Scenariusz 2: Atak „agenta-robaka” i DDoS

We wtorek rano wypuszczany jest nowy „robak”. Rozprzestrzenia się za pomocą nośników wymiennych i może kopiować się, aby uruchomić udostępnianie systemu Window. Gdy „robak” infekuje hosta, instaluje agenta DDoS. Organizacja została już narażona na

powszechne infekcje, zanim sygnatury antywirusowe staną się dostępne kilka godzin po rozpoczęciu rozprzestrzeniania się robaka.

Poniżej znajdują się dodatkowe pytania dotyczące tego scenariusza:

1. W jaki sposób zespół reagowania na incydenty zidentyfikowałby wszystkie zainfekowane hosty?
2. W jaki sposób organizacja próbowałaby zapobiec przedostawaniu się „robaka" do organizacji przed udostępnieniem sygnatur antywirusowych?
3. W jaki sposób organizacja podjęłaby próbę zapobieżenia rozprzestrzenianiu się „robaka" przez zainfekowane hosty, przed udostępnieniem sygnatur antywirusowych?
4. Czy organizacja próbowałaby zainstalować poprawki na wszystkich podatnych komputerach? Jeśli tak, to w jaki sposób?
5. Jak zmieniłaby się obsługa tego incydentu, gdyby zainfekowane hosty, które otrzymały agenta DDoS, zostały skonfigurowane do ataku na witrynę innej organizacji następnego dnia?
6. Jak zmieniłaby się obsługa tego incydentu, gdyby co najmniej jeden z zainfekowanych hostów zawierał wrażliwe dane osobowe pracowników organizacji?
7. W jaki sposób zespół reagowania na incydenty informowałby użytkowników w organizacji o statusie incydentu?
8. Jakie dodatkowe środki zastosowałby zespół w przypadku hostów, które nie są obecnie podłączone do sieci (np. pracownicy na wakacjach, pracownicy spoza firmy, którzy łączą się sporadycznie z zasobami organizacji)?

Scenariusz 3: Skradzione dokumenty

W poniedziałek rano dział prawny organizacji odbiera telefon z organu ścigania w sprawie podejrzanej działalności związanej z systemami organizacji. Później tego samego dnia funkcjonariusz organu ścigania spotyka się z członkami zarządu i działem prawnym, aby omówić tę działalność. Organ ścigania prowadzi dochodzenie w sprawie publicznego opublikowania poufnych dokumentów rządowych, a niektóre dokumenty podobno należą do organizacji. Funkcjonariusz prosi organizację o wsparcie, a kierownictwo prosi o pomoc zespołu reagowania na incydenty w uzyskaniu niezbędnych dowodów w celu ustalenia, czy te dokumenty są legalne, czy nie, oraz w jaki sposób mogły zostać ujawnione.

Poniżej znajdują się dodatkowe pytania dotyczące tego scenariusza:

1. Z jakich źródeł zespół reagowania na incydenty może zbierać dowody?
2. Co zrobiłby zespół, aby zachować poufność dochodzenia?
3. Jak zmieniłaby się obsługa tego incydentu, gdyby zespół zidentyfikował wewnętrznego hosta odpowiedzialnego za wycieki?
4. Jak zmieniłaby się obsługa tego incydentu, gdyby zespół znalazł rootkita zainstalowanego na hoście wewnętrznym odpowiedzialnym za wycieki?

Scenariusz 4: Przejęty serwer bazy danych

We wtorek wieczorem administrator bazy danych przeprowadza konserwację poza godzinami pracy na kilku produkcyjnych serwerach baz danych. Administrator zauważa nieznane i nietypowe nazwy katalogów na jednym z serwerów. Po przejrzeniu list katalogów i przejrzeniu niektórych plików administrator stwierdza, że serwer został zaatakowany i wzywa zespół reagowania na incydenty o pomoc. Dochodzenie zespołu ustaliło, że osoba atakująca z powodzeniem uzyskała uprawnienia roota do serwera sześć tygodni temu.

Poniżej znajdują się dodatkowe pytania dotyczące tego scenariusza:

1. Z jakich źródeł może skorzystać zespół, aby ustalić, kiedy nastąpiło naruszenie?
2. Jak zmieniłaby się obsługa tego incydentu, gdyby zespół odkrył, że serwer bazy danych uruchamiał sniffer pakietów i przechwytywał hasła z sieci?
3. Jak zmieniłaby się obsługa tego incydentu, gdyby zespół stwierdził, że serwer uruchamia proces, który każdego wieczoru kopiuje bazę danych zawierającą wrażliwe informacje o klientach (w tym dane osobowe) i przesyła ją na adres zewnętrzny?
4. Jak zmieniłaby się obsługa tego incydentu, gdyby zespół odkrył rootkita na serwerze?

Scenariusz 5: Nieznana eksfiltracja

W niedzielny wieczór jeden z czujników wykrywania włamań sieciowych w organizacji ostrzega o anomalnej wychodzącej aktywności sieciowej, która obejmuje transfery dużych plików. Analityk włamań przegląda alerty. Wygląda na to, że tysiące plików z rozszerzeniem .RAR są kopiowane z hosta wewnętrznego do hosta zewnętrznego, a host zewnętrzny znajduje się w innym kraju. Analityk kontaktuje się z zespołem reagowania na incydenty, w celu dokładniejszego zbadania działanie. Zespół nie może stwierdzić, co przechowują pliki

.RAR, ponieważ ich zawartość jest zaszyfrowana. Analiza wewnętrznego hosta zawierającego pliki .RAR wykazuje oznaki instalacji bota.

Poniżej znajdują się dodatkowe pytania dotyczące tego scenariusza:

1. W jaki sposób zespół ustaliłby, co najbardziej prawdopodobnie znajduje się w plikach .RAR? Jakie inne zespoły mogą pomóc zespołowi reagowania na incydenty?
2. Gdyby zespół reagowania na incydenty ustalił, że początkowe naruszenie bezpieczeństwa nastąpiło za pośrednictwem karty sieci bezprzewodowej w hoście wewnętrznym, w jaki sposób zespół powinien dalej badać tę czynność?
3. Jeśli zespół reagowania na incydenty ustali, że host wewnętrzny był używany do umieszczania wrażliwych plików z innych hostów z przedsiębiorstwa, w jaki sposób zespół miałby dalej badać to działanie?

Scenariusz 6: Nieautoryzowany dostęp do list płac

W środę wieczorem zespół ochrony fizycznej organizacji odbiera informację od administratora listy płac, który widział, jak nieznana osoba opuszcza jej biuro, biegnie korytarzem i wychodzi z budynku. Administrator zostawił jej stację roboczą odblokowaną i bez nadzoru tylko na kilka minut. Program płacowy jest nadal zalogowany i znajduje się w menu głównym, tak jak wtedy, gdy go pozostawił, ale administrator zauważa, że mysz wydaje się być przesunięta. Zespół reagowania na incydenty został poproszony o zebranie dowodów związanych z incydentem i określenie, jakie czynności zostały wykonane.

Poniżej znajdują się dodatkowe pytania dotyczące tego scenariusza:

1. W jaki sposób zespół określiłby, jakie działania zostały wykonane?
2. Czym różniłaby się obsługa tego incydentu, gdyby administrator listy płac rozpoznał osobę wychodzącą z biura jako byłego pracownika działu kadr?
3. Czym różniłaby się obsługa tego incydentu, gdyby zespół miał podstawy sądzić, że dana osoba była obecnym pracownikiem?
4. Czym różniłaby się obsługa tego incydentu, gdyby zespół ochrony fizycznej ustalił, że dana osoba użyła technik inżynierii społecznej, aby uzyskać fizyczny dostęp do budynku?
5. Czym różniłaby się obsługa tego incydentu, gdyby dzienniki z poprzedniego tygodnia wykazywały niezwykle dużą liczbę nieudanych prób zdalnego logowania przy użyciu identyfikatora użytkownika administratora listy płac?

6. Czym różniłaby się obsługa tego incydentu, gdyby zespół reagowania na incydenty odkrył, że program rejestrujący naciśnięcia klawiszy został zainstalowany na komputerze dwa tygodnie wcześniej?

Scenariusz 7: Znikający Host

W czwartkowe popołudnie czujnik wykrywania włamań sieciowych rejestruje aktywność skanowania luk w zabezpieczeniach skierowaną do hostów wewnętrznych, która jest generowana przez wewnętrzny adres IP. Ponieważ analityk ds. wykrywania włamań nie posiada wiedzy o żadnej autoryzowanej, zaplanowanej czynności skanowania podatności, zgłasza ją zespołowi reagowania na incydenty. Kiedy zespół rozpoczyna analizę, odkrywa, że działanie zostało zatrzymane i nie istnieje już host używający tego adresu IP.

Poniżej znajdują się dodatkowe pytania dotyczące tego scenariusza:

1. Jakie źródła danych mogą zawierać informacje dotyczące tożsamości hosta skanującego luki w zabezpieczeniach?
2. W jaki sposób zespół miałby określić, kto wykonywał skanowanie luk w zabezpieczeniach?
3. Czym różniłaby się obsługa tego incydentu, gdyby skanowanie pod kątem luk w zabezpieczeniach było skierowane na najbardziej krytyczne hosty organizacji?
4. Czym różniłaby się obsługa tego incydentu, gdyby skanowanie luk w zabezpieczeniach było skierowane na zewnętrzne hosty?
5. Czym różniłaby się obsługa tego incydentu, gdyby wewnętrzny adres IP był powiązany z bezprzewodową siecią gości organizacji?
6. Czym różniłaby się obsługa tego incydentu, gdyby pracownicy ochrony fizycznej odkryli, że ktoś włamał się do obiektu na pół godziny przed dokonaniem skanowania luk w zabezpieczeniach?

Scenariusz 8: Naruszenie zabezpieczeń podczas pracy zdalnej

W sobotę wieczorem oprogramowanie do wykrywania włamań sieciowych rejestruje połączenie przychodzące pochodzące z listy obserwowanych adresów IP. Analityk ds. wykrywania włamań ustala, że połączenie jest nawiązywane z serwerem VPN organizacji i następnie kontaktuje się z zespołem reagowania na incydenty. Zespół przegląda dzienniki wykrywania włamań, zapory oraz serwera VPN i ustala identyfikator użytkownika, który został uwierzytelniony w sesji, oraz nazwę użytkownika powiązanego z identyfikatorem użytkownika.

Poniżej znajdują się dodatkowe pytania dotyczące tego scenariusza:

1. Jaki powinien być następny krok zespołu (np. zadzwonienie do użytkownika w domu, wyłączenie identyfikatora użytkownika, rozłączenie sesji VPN)? Dlaczego ten krok należy wykonać jako pierwszy? Jaki krok należy wykonać jako drugi?
2. Czym różniłaby się obsługa tego incydentu, gdyby zewnętrzny adres IP należał do otwartego serwera proxy?
3. Czym różniłaby się obsługa tego incydentu, gdyby identyfikator został użyty do zainicjowania połączeń VPN z kilku zewnętrznych adresów IP bez wiedzy użytkownika?
4. Załóżmy, że komputer zidentyfikowanego użytkownika został naruszony przez grę zawierającą konia trojańskiego pobranego przez członka rodziny. Jak wpłynęłoby to na analizę incydentu przez zespół? Jak wpłynęłoby to na gromadzenie i przetwarzanie dowodów? Co powinien zrobić zespół, aby usunąć incydent z komputera użytkownika?
5. Załóżmy, że użytkownik zainstalował oprogramowanie antywirusowe i stwierdził, że koń trojański zawiera rejestrator naciśnięć klawiszy. Jak wpłynęłoby to na obsługę incydentu? Jak wpłynęłoby to na obsługę incydentu, gdyby użytkownik był administratorem systemu? Jak wpłynęłoby to na obsługę incydentu, gdyby użytkownik należał do kierownictwa wysokiego szczebla w organizacji?

Scenariusz 9: Anonimowe zagrożenie

W czwartkowe popołudnie zespół ds. bezpieczeństwa fizycznego w organizacji odbiera informację od menedżera IT, który informuje, że dwaj pracownicy organizacji właśnie otrzymali anonimowe groźby skierowane przeciwko systemom organizacji. Na podstawie przeprowadzonego postepowania sprawdzającego, zespół ochrony fizycznej uważa, że zagrożenia należy traktować poważnie i powiadamia o zagrożeniach odpowiednie zespoły wewnętrzne, w tym zespół reagowania na incydenty.

Poniżej znajdują się dodatkowe pytania dotyczące tego scenariusza:

1. Co, jeśli w ogóle, powinien zrobić zespół reagowania na incydenty w odpowiedzi na powiadomienie o zagrożeniu?
2. Jaki wpływ może mieć zaostrzona kontrola bezpieczeństwa fizycznego na reakcje zespołu na incydenty?

Scenariusz 10: Współdzielenie plików w sieci peer-to-peer

Organizacja zabrania korzystania z usług udostępniania plików w trybie peer-to-peer. Sensory wykrywania włamań do sieci organizacji mają włączone sygnatury, które mogą wykryć użycie kilku popularnych usług udostępniania plików w trybie peer-to-peer. W poniedziałkowy wieczór analityk ds. wykrywania włamań zauważa, że w ciągu ostatnich trzech godzin wystąpiło kilka alertów dotyczących udostępniania plików, z których wszystkie dotyczą tego samego wewnętrznego adresu IP.

1. Jakie kryteria należy zastosować, aby ustalić priorytety postępowania w przypadku tego incydentu (np. widoczna zawartość udostępnianych plików)?
2. Jakie względy prywatności mogą mieć wpływ na obsługę tego incydentu?
3. Czym różniłaby się obsługa tego incydentu, gdyby komputer udostępniający pliki w trybie peer-to-peer zawierał również wrażliwe dane osobowe?

Scenariusz 11: Nieznany bezprzewodowy punkt dostępowy

W poniedziałek rano do działu pomocy w organizacji dzwoni trzech użytkowników z tego samego piętra budynku, zgłaszając, że mają problemy z dostępem bezprzewodowym. Administrator sieci poproszony o pomoc w rozwiązaniu problemu udaje się z laptopem z dostępem bezprzewodowym na piętro, gdzie przebywają użytkownicy zgłaszający problem. Kiedy przegląda konfigurację sieci bezprzewodowej, zauważa, że na liście znajduje się nowy aktywny punkt dostępu. Konsultuje sie z kolegami z zespołu i stwierdza, że ten punkt dostępu nie został wdrożony przez jego zespół, więc najprawdopodobniej jest to fałszywy punkt dostępu, który został ustanowiony bez pozwolenia.

1. Jaki powinien być pierwszy krok w obsłudze tego incydentu (np. fizyczne znalezienie fałszywego punktu dostępu, logiczne połączenie z punktem dostępu)?
2. Jaki jest najszybszy sposób zlokalizowania punktu dostępu? Jaki jest najbardziej dyskretny sposób zlokalizowania punktu dostępu?
3. Czym różniłaby się obsługa tego incydentu, gdyby punkt dostępu został wdrożony przez stronę zewnętrzną (np. wykonawcę) pracującą tymczasowo w biurze organizacji?
4. Czym różniłaby się obsługa tego incydentu, gdyby analityk ds. wykrywania włamań zgłosił oznaki podejrzanej aktywności obejmującej niektóre stacje robocze na tym samym piętrze budynku?
5. Czym różniłaby się obsługa tego incydentu, gdyby punkt dostępu został usunięty, podczas gdy zespół nadal próbował go fizycznie zlokalizować?

ZAŁĄCZNIK B: ELEMENTY DANYCH ZWIĄZANYCH Z INCYDENTAMI

Organizacje powinny określić standardowy zestaw elementów danych dotyczących incydentów, które mają być gromadzone dla każdego incydentu. Wysiłki te nie tylko ułatwią skuteczniejszą i spójniejszą obsługę incydentów, ale także pomogą organizacji w spełnieniu odpowiednich wymagań dotyczących zgłaszania incydentów. Organizacja powinna wyznaczyć zestaw podstawowych elementów (np. imię i nazwisko zgłaszającego incydent, numer telefonu i lokalizację, adres e-mail), które mają być gromadzone podczas zgłaszania incydentu, oraz dodatkowy zestaw elementów, które mają być zbierane przez osoby zajmujące się incydentem podczas udzielania odpowiedzi. Te dwa zestawy elementów stanowiłyby podstawę bazy danych zgłaszania incydentów, omówionej wcześniej w rozdziale 3.2.5. Poniższe listy zawierają sugestie dotyczące tego, jakie informacje należy gromadzić na wypadek incydentów i nie są wyczerpujące. Każda organizacja powinna stworzyć własną listę elementów w oparciu o kilka czynników, w tym model i strukturę zespołu reagowania na incydenty oraz definicję terminu „incydent".

B.1 Podstawowe dane

- Dane kontaktowe osoby zgłaszającej incydenty i osoby obsługującej
  - Imię i nazwisko.
  - Rola / stanowisko.
  - Jednostka organizacyjna (np. agencja, departament, dział, zespół) i przynależność
  - Adres e-mail; numer telefonu kontaktowego.
  - Lokalizacja (np. adres do korespondencji, numer biura).
- Szczegół y incydentu
  - Data / znaczniki czasu zmiany statusu (w tym strefa czasowa): kiedy incydent się rozpoczął, kiedy incydent został odkryty / wykryty, kiedy incydent został zgłoszony, kiedy incydent został rozwiązany / zakończony itp.;
  - Fizyczna lokalizacja zdarzenia (np. miejscowość);
  - Aktualny stan incydentu (np. trwający atak);
  - Źródło / przyczyna incydentu (jeśli jest znana), w tym nazwy hostów i adresy IP;
  - Opis zdarzenia (np. w jaki sposób zostało wykryte, co się stało);

  - Opis zasobów, których dotyczy problem (np. sieci, hosty, aplikacje, dane), w tym nazwy hostów systemów, adresy IP i funkcje;
  - Jeśli są znane, kategoria incydentu, wektory ataku związane z incydentem oraz wskaźniki związane ze zdarzeniem (wzorce ruchu, klucze rejestru itp.) ;
  - Czynniki priorytetyzacji (wpływ funkcjonalny, wpływ informacji, możliwość odzyskania itp.);
  - Czynniki łagodzące (np. skradziony laptop zawierający wrażliwe dane korzystał z szyfrowania całego dysku) ;
  - Wykonane działania w odpowiedzi na incydent (np. wyłączenie hosta, odłączenie hosta od sieci);
  - Inne organizacje, z którymi się skontaktowano (np. dostawca oprogramowania).
- Uwagi ogólne.

B.2 Elementy danych dotyczące obsługi incydentów

- Bieżący stan reakcji na incydent.
- Podsumowanie incydentu.
- Działania związane z obsługą incydentów:
  - Dziennik działań podjętych przez wszystkie osoby postępujące z incydentem;
  - Dane kontaktowe wszystkich zaangażowanych stron;
  - Lista zebranych dowodów.
- Komentarze osoby obsługującej incydent;
- Przyczyna incydentu (np. niewłaściwie skonfigurowana aplikacja, host bez zainstalowanych poprawek);
- Koszt zdarzenia;
- Wpływ incydentu na biznes[38]

[38] Skutkiem biznesowym incydentu może być opis skutków incydentu (np. dział księgowości nie może wykonywać zadań przez dwa dni) lub kategoria wpływu oparta na kosztach (np. „poważny" incydent ma koszt ponad 100 000 PLN).

ZAŁĄCZNIK C: SŁOWNIK

Patrz: NSC 7298, Słownik kluczowych pojęć z zakresu cyberbezpieczeństwa.

ZAŁĄCZNIK D: AKRONIMY

Patrz: NSC 7298, Słownik kluczowych pojęć z zakresu cyberbezpieczeństwa.

ZAŁĄCZNIK E: ŹRÓDŁA

Poniższe listy zawierają przykłady zasobów, które mogą być pomocne w ustanawianiu i utrzymywaniu zdolności reagowania na incydenty.

Organizacje reagowania na incydenty

Organizacja	Odnośnik
Anti-Phishing Working Group (APWG)	http://www.antiphishing.org/
Computer Crime and Intellectual Property Section (CCIPS), U.S. Department of Justice	http://www.cybercrime.gov/
CERT Coordination Center, Carnegie Mellon University (CERT®/CC)	http://www.cert.org/
CSIRT GOV	https://csirt.gov.pl/
CSIRT NASK	https://www.nask.pl/pl/dzialalnosc/csirt-nask/3424,CSIRT-NASK.html
CSIRT MON	https://csirt-mon.wp.mil.pl/
European Union Agency for Cybersecurity (ENISA)	http://www.enisa.europa.eu/activities/cert
Forum of Incident Response and Security Teams (FIRST)	http://www.first.org/

Powiązane Publikacje

Nazwa	Odnośnik
NSC 800-53, Zasady stosowania zabezpieczeń w systemach informatycznych podmiotów publicznych	https://www.gov.pl/attachment/459869e4-cbbf-4829-8ecd-02993e00c765

NIST SP 800-84, *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities*	https://csrc.nist.gov/search?keywords=800-84
NIST SP 800-86, *Guide to Integrating Forensic Techniques into Incident Response*	https://csrc.nist.gov/publications/detail/sp/800-86/final
NIST SP 800-92, *Guide to Computer Security Log Management*	https://csrc.nist.gov/search?keywords=800-92
NIST SP 800-94, *Guide to Intrusion Detection and Prevention Systems (IDPS)*	https://csrc.nist.gov/search?keywords=800-94
NIST SP 800-115, *Technical Guide to Information Security Testing and Assessment*	https://csrc.nist.gov/search?keywords=800-115
NIST SP 800-128, *Guide for Security-Focused Configuration Management of Information Systems*	https://csrc.nist.gov/search?keywords=800-128

ZAŁĄCZNIK F: CZYNNOŚCI POSTĘPOWANIA W SYTUACJI KRYZYSOWEJ

Poniżej zamieszczona jest lista głównych kroków, które należy wykonać, gdy pracownik techniczny uważa, że wystąpił poważny incydent, a organizacja nie ma dostępnej zdolności reagowania na incydenty. Służy jako podstawowe odniesienie do tego, jak należy postępować w sytuacji kryzysowej i nie ma czasu na zapoznanie się z całym dokumentem.

1. **Dokumentować wszystko.** Ten wysiłek obejmuje każde wykonywane działanie, każdy dowód i każdą rozmowę z użytkownikami, właścicielami systemu i innymi w sprawie incydentu.
2. **Znaleźć współpracownika, który może udzielić pomocy.** Obsługa incydentu będzie znacznie łatwiejsza, jeśli dwie lub więcej osób będzie współpracować. Na przykład jedna osoba może wykonywać czynności, a druga je dokumentować.
3. **Przeanalizować dowody, aby potwierdzić, że incydent miał miejsce.** W razie potrzeby przeprowadź dodatkowe badania (np. wyszukiwarki internetowe, dokumentację oprogramowania), aby lepiej zrozumieć dowody. Skontaktuj się z innymi specjalistami technicznymi w organizacji, aby uzyskać dodatkową pomoc.
4. **Powiadomić odpowiednie osoby w organizacji.** Powinno to obejmować członka kierownictwa ds. Informacji (CIO), dyrektora ds. bezpieczeństwa informacji (CISO) oraz lokalnego menadżera ds. bezpieczeństwa. Zachowaj ostrożność podczas omawiania szczegółów zdarzenia z innymi osobami. Powiadom tylko te osoby, które powinny znać i wykorzystywać mechanizmy komunikacji, które są w miarę bezpieczne. Jeśli osoba atakująca przejęła usługi poczty e-mail, nie wysyłaj wiadomości e-mail o zdarzeniu.
5. **Powiadomić CSIRT i / lub inne organizacje zewnętrzne** w celu uzyskania pomocy w postępowaniu z incydentem.
6. **Powstrzymać incydent, jeśli nadal trwa.** Najczęstszym sposobem jest odłączenie od sieci systemów, których dotyczy luka. W niektórych przypadkach może być konieczne zmodyfikowanie konfiguracji zapory i routera w celu zatrzymania ruchu sieciowego będącego częścią zdarzenia, takiego jak atak typu DoS (odmowa usługi).
7. **Zachować dowody z incydentu.** Twórz kopie zapasowe systemów (najlepiej kopie zapasowe obrazu dysku, a nie kopie zapasowe systemu plików), których dotyczy luka. Zrób kopie plików dziennika, które zawierają dowody związane z incydentem.
8. **Usunąć wszystkie skutki incydentu.** Działania te obejmują infekcje złośliwym oprogramowaniem, nieodpowiednie materiały (np. pirackie oprogramowanie), pliki koni

trojańskich i wszelkie inne zmiany wprowadzone w systemach przez incydenty. Jeśli system został w pełni naruszony, odbuduj go od podstaw lub przywróć ze znanej zaufanej kopii zapasowej.

9. **Zidentyfikować i ograniczyć wszystkie podatności, które zostały wykorzystane.** Incydent mógł mieć miejsce w wyniku wykorzystania luk w zabezpieczeniach systemów operacyjnych lub aplikacji. Niezwykle ważne jest, aby zidentyfikować takie luki i wyeliminować je lub w inny sposób złagodzić, aby incydent się nie powtórzył.
10. **Potwierdzić, że operacje zostały przywrócone do normalnego stanu.** Upewnij się, że dane, aplikacje i inne usługi, na które miał wpływ incydent, zostały przywrócone do normalnego działania.
11. **Utworzyć raport końcowy.** Raport ten powinien szczegółowo opisywać proces obsługi incydentu. Powinien również zawierać podsumowanie tego, co się stało i jak formalna zdolność reagowania na incydenty pomogłaby poradzić sobie z sytuacją, złagodzić ryzyko i szybciej ograniczyć szkody.