KATALOG ZABEZPIECZEŃ

Niniejszy katalog zawiera wykaz zabezpieczeń organizacyjnych i technicznych niezbędnych do zapewnienia wysokiego poziomu bezpieczeństwa informacji. Katalog opracowany został na podstawie standardu NIST 800-53 rev. 4.

Katalog zawiera zestawienie podstawowych środków bezpieczeństwa (zabezpieczeń), które stanowią punkt wyjścia przy ustalaniu potencjalnego wpływu (niski, umiarkowany i wysoki) na ustanowione atrybuty bezpieczeństwa systemów informatycznych i przetwarzanych informacji. Trzy podstawowe priorytety wdrożenia zabezpieczeń mają charakter hierarchiczny w odniesieniu do zastosowanych środków bezpieczeństwa. Dla jednej rodziny zabezpieczeń wybrany jest środek bezpieczeństwa, do którego przypisany jest identyfikator i numer zabezpieczenia wymieniony w odpowiedniej kolumnie Tabeli 5-2. Jeśli stosowanie danego zabezpieczenia nie jest obligatoryjne, wpis jest oznaczony jako opcjonalny. Zabezpieczenia rozszerzone stosowane są jako uzupełnienia podstawowych środków bezpieczeństwa i są oznaczane numerem tego rozszerzenia.
Organizacje mogą zastosować zalecany priorytet wdrożenia zabezpieczeń, który jest powiązany z każdym zabezpieczeniem, aby pomóc w podejmowaniu decyzji dotyczących sekwencjonowania kolejności wdrożenia zabezpieczenia [np. zabezpieczenie z kodem priorytetu P1 ma wyższy priorytet wdrożenia niż zabezpieczenie z kodem priorytetu P2; zabezpieczenie z kodem priorytetu P2 ma wyższy priorytet implementacji niż zabezpieczenie z kodem priorytetu P3, a kod priorytetu P0 wskazuje, że dany środek bezpieczeństwa stosowany jest opcjonalnie (stosowanie jego jest szacowane przez organizację)]. Zastosowanie zalecanego priorytetu ustalania kolejności wdrażania zabezpieczenia pomaga zapewnić, że środki bezpieczeństwa, od których zależą inne zabezpieczenia, są wdrażane jako pierwsze, umożliwiając tym samym organizacjom wdrożenie zabezpieczeń w bardziej uporządkowany i terminowy sposób, zgodnie z dostępnymi zasobami. Wdrożenie środków bezpieczeństwa według priorytetu wdrożenia nie oznacza żadnego określonego poziomu ograniczenia ryzyka, dopóki wszystkie zabezpieczenia, określone w planie bezpieczeństwa, nie zostaną wdrożone. Kody priorytetów są używane tylko do sekwencjonowania implementacji, a nie do podejmowania decyzji co do wyboru środków bezpieczeństwa. Tabela 5-1 opisuje priorytety wdrożenia dla podstawowych środków bezpieczeństwa zawartych w Tabeli 5-2.

TABELA 5-1 Kody priorytetów wdrożenia zabezpieczeń

Priorytet wdrożenia	Sekwencja wdrożenia	Implementacja
Kod Priorytetu **P1**	W pierwszej kolejności	Zabezpieczenie z kodem priorytetu P1 implementowane jest jako pierwsze
Kod Priorytetu **P2**	W drugiej kolejności	Zabezpieczenie z kodem priorytetu P2 implementowane jest po wdrożeniu P1
Kod Priorytetu **P3**	W trzeciej kolejności	Zabezpieczenie z kodem priorytetu P3 implementowane jest po wdrożeniu P1 i P2
Kod Priorytetu **P0**	Opcjonalnie	Zabezpieczenie z kodem priorytetu P0 implementowane jest opcjonalnie

Tabela 5-2 zawiera podsumowanie podstawowych i rozszerzonych środków bezpieczeństwa opisanych w Załączniku 5, które zostały przypisane do podstawowych zabezpieczeń dla poszczególnych poziomów wpływu informacji (tj. niski, umiarkowany i wysoki). Zabezpieczenia oraz kody priorytetów wdrożenia , które zostały wycofane z Załącznika 5, są wskazane w Tabeli 5-2 jako niewykorzystywane (oznaczone symbolem ---).

AC – Kontrola dostępu
AT – Uświadamianie i szkolenia
AU– Audyt i rozliczalność
CA – Ocena bezpieczeństwa i autoryzacja
CM – Zarządzanie konfiguracją
CP – Planowanie awaryjne/ciągłość działania
IA – Identyfikacja i uwierzytelnianie
IR – Reagowanie na incydenty
MA – Utrzymanie i wsparcie
MP – Ochrona nośników danych
PE – Ochrona fizyczna i środowiskowa
PL – Planowanie
PM – Programy bezpieczeństwa informacji
PS – Bezpieczeństwo osobowe
RA – Ocena ryzyka
SA – Nabywanie systemu i usług
SC – Ochrona systemów i sieci telekomunikacyjnych
SI – Integralność systemu i informacji

TABELA 5-2 Katalog podstawowych zabezpieczeń na poszczególnych poziomach potencjalnego wpływu na atrybuty bezpieczeństwa informacji (niski, umiarkowany, wysoki)

Numer Zabezpieczenia	NAZWA ZABEZPIECZENIA	PRIORYTET	POZIOMY WPŁYWU NA ATRYBUTY BEZPIECZEŃSTWA INFORMACJI		
			NISKI	UMIARKOWANY	WYSOKI
Kontrola dostępu					
AC-1	Polityka i procedury kontroli dostępu	P1	AC-1	AC-1	AC-1
AC-2	Zarządzanie kontem	P1	AC-2	AC-2 (1) (2) (3) (4)	AC-2 (1) (2) (3) (4) (5) (11) (12) (13)
AC-3	Egzekwowanie uprawnień dostępu	P1	AC-3	AC-3	AC-3
AC-4	Egzekwowanie zasad przepływu informacji	P1	AC-4 (opcjonalnie)	AC-4	AC-4
AC-5	Rozdział obowiązków	P1	–	AC-5	AC-5
AC-6	Zasada wiedzy koniecznej	P1	–	AC-6 (1) (2) (5) (9) (10)	AC-6 (1) (2) (3) (5) (9) (10)
AC-7	Nieudane próby logowania	P2	AC-7	AC-7	AC-7
AC-8	Powiadomianie o zasadach użycia systemu	P1	AC-8	AC-8	AC-8
AC-9	Powiadomianie o zalogowaniu	P0	–	–	–
AC-10	Kontrola ilości równoczesnych sesji	P3	–	–	AC-10
AC-11	Zamknięcie / Blokada sesji	P3	–	AC-11 (1)	AC-11 (1)
AC-12	Zakończenie sesji	P2	–	AC-12	AC-12
AC-13	Nadzór i przegląd – kontrola dostepu	---	---	---	---
AC-14	Działania dozwolone bez identyfikacji lub uwierzytelnienia	P3	AC-14	AC-14	AC-14
AC-15	Zautomatyzowane znakowanie	---	---	---	---
AC-16	Atrybuty bezpieczeństwa	P0	–	–	–
AC-17	Zdalny dostęp	P1	AC-17	AC-17 (1) (2) (3) (4)	AC-17 (1) (2) (3) (4)
AC-18	Dostęp bezprzewodowy	P1	AC-18	AC-18 (1)	AC-18 (1) (4) (5)
AC-19	Kontrola dostępu realizowanewgo z	P1	AC-19	AC-19 (5)	AC-19 (5)

Numer Zabezpieczenia	NAZWA ZABEZPIECZENIA	PRIORYTET	POZIOMY WPŁYWU NA ATRYBUTY BEZPIECZEŃSTWA INFORMACJI		
			NISKI	UMIARKOWANY	WYSOKI
	urządzeń przenośnych (mobilnych)				
AC-20	Wykorzystanie zewnętrznych systemów teleinformatycznych	P1	AC-20	AC-20 (1) (2)	AC-20 (1) (2)
AC-21	Udostępnianie informacji	P2	–	AC-21	AC-21
AC-22	Treści publicznie dostępne	P3	AC-22	AC-22	AC-22
AC-23	Ochrona przed przeszukiwaniem danych	P0	–	–	–
AC-24	Przyznawanie praw dostępu	P0	–	–	–
AC-25	Monitorowanie referencyjne	P0	–	–	–
Uświadamianie i szkolenia					
AT-1	Świadomość bezpieczeństwa, polityka i procedury szkoleniowe	P1	AT-1	AT-1	AT-1
AT-2	Szkolenie w zakresie uświadamiania bezpieczeństwa	P1	AT-2	AT-2 (2)	AT-2 (2)
AT-3	Szkolenie w zakresie bezpieczeństwa opartego na rolach	P1	AT-3	AT-3	AT-3
AT-4	Rejestrowanie szkoleń z zakresu bezpieczeństwa	P3	AT-4	AT-4	AT-4
AT-5	Utrzymywanie kontaktów z zespołami i stowarzyszeniami specjalizującymi się w cyberbezpieczeństwie	---	---	---	---
Audyt i rozliczalność					
AU-1	Polityka oraz procedury w zakresie audytu i rozliczalności	P1	AU-1	AU-1	AU-1
AU-2	Audyt zdarzeń	P1	AU-2	AU-2 (3)	AU-2 (3)
AU-3	Zawartość rejestrów audytu	P1	AU-3	AU-3 (1)	AU-3 (1) (2)
AU-4	Pojemność pamięci zapisów audytu	P1	AU-4	AU-4	AU-4
AU-5	Reakcja na błędy procesów audytu	P1	AU-5	AU-5	AU-5 (1) (2)
AU-6	Przegląd audytu, analiza i raportowanie	P1	AU-6	AU-6 (1) (3)	AU-6 (1) (3) (5) (6)
AU-7	Redukcja treści zapisów audytu i generowanie raportów	P2	–	AU-7 (1)	AU-7 (1)
AU-8	Znaczniki czasu	P1	AU-8	AU-8 (1)	AU-8 (1)

Numer Zabezpieczenia	NAZWA ZABEZPIECZENIA	PRIORYTET	POZIOMY WPŁYWU NA ATRYBUTY BEZPIECZEŃSTWA INFORMACJI		
			NISKI	UMIARKOWANY	WYSOKI
AU-9	Ochrona informacji audytowych	P1	AU-9	AU-9 (4)	AU-9 (2) (3) (4)
AU-10	Niezaprzeczalność	P2	–	–	AU-10
AU-11	Retencja zapisów audytu	P3	AU-11	AU-11	AU-11
AU-12	Tworzenie zapisów audytu	P1	AU-12	AU-12	AU-12 (1) (3)
AU-13	Monitorowanie ujawniania informacji	P0	–	–	–
AU-14	Audyt sesji	P0	–	–	–
AU-15	Zdolność do alternatywnego audytu	P0	–	–	–
AU-16	Audyt międzyorganizacyjny	P0	–	–	–
Ocena bezpieczeństwa i autoryzacja					
CA-1	Ocena bezpieczeństwa i autoryzacja - polityka i procedury	P1	CA-1	CA-1	CA-1
CA-2	Ocena bezpieczeństwa	P2	CA-2	CA-2 (1)	CA-2 (1) (2)
CA-3	Połączenia międzysystemowe	P1	CA-3	CA-3 (5)	CA-3 (5)
CA-4	Certyfikacja bezpieczeństwa	---	---	---	---
CA-5	Plan i etapy działania	P3	CA-5	CA-5	CA-5
CA-6	Autoryzacja bezpieczeństwa	P2	CA-6	CA-6	CA-6
CA-7	Ciągłość monitorowania	P2	CA-7	CA-7 (1)	CA-7 (1)
CA-8	Testy penetracyjne	P2	–	–	CA-8
CA-9	Połączenia wewnętrzsystemowe	P2	CA-9	CA-9	CA-9
Zarządzanie konfiguracją					
CM-1	Zarządzanie konfiguracją – polityka i procedury	P1	CM-1	CM-1	CM-1
CM-2	Konfiguracja podstawowa	P1	CM-2	CM-2 (1) (3) (7)	CM-2 (1) (2) (3) (7)
CM-3	Zabezpieczanie zmian konfiguracji	P1	–	CM-3 (2)	CM-3 (1) (2)
CM-4	Analiza zmian wpływających na bezpieczeństwo	P2	CM-4	CM-4	CM-4 (1)
CM-5	Ograniczenia możliwości wykonywania zmian	P1	–	CM-5	CM-5 (1) (2) (3)

Numer Zabezpieczenia	NAZWA ZABEZPIECZENIA	PRIORYTET	POZIOMY WPŁYWU NA ATRYBUTY BEZPIECZEŃSTWA INFORMACJI		
			NISKI	UMIARKOWANY	WYSOKI
CM-6	Ustawienia konfiguracji	P1	CM-6	CM-6	CM-6 (1) (2)
CM-7	Zasada minimalnej funkcjonalności	P1	CM-7	CM-7 (1) (2) (4)	CM-7 (1) (2) (5)
CM-8	Inwentaryzacja komponentów systemu teleinformatycznego	P1	CM-8	CM-8 (1) (3) (5)	CM-8 (1) (2) (3) (4) (5)
CM-9	Plan zarządzania konfiguracją	P1	–	CM-9	CM-9
CM-10	Ograniczenia w użyciu oprogramowania	P2	CM-10	CM-10	CM-10
CM-11	Oprogramowanie instalowane przez użytkownika	P1	CM-11	CM-11	CM-11
Planowanie awaryjne / Ciągłość działania					
CP-1	Polityka i procedury planowania ciągłości działania	P1	CP-1	CP-1	CP-1
CP-2	Plan ciągłości działania	P1	CP-2	CP-2 (1) (3) (8)	CP-2 (1) (2) (3) (4) (5) (8)
CP-3	Szkolenie z zakresie planowania ciągłości działania	P2	CP-3	CP-3	CP-3 (1)
CP-4	Testowanie planu ciągłości dzałania	P2	CP-4	CP-4 (1)	CP-4 (1) (2)
CP-5	Aktualizacja planu ciągłości dzałania	---	---	---	---
CP-6	Zapasowe miejsce przechowywania kopii	P1	–	CP-6 (1) (3)	CP-6 (1) (2) (3)
CP-7	Zapasowe miejsce przetwarzania	P1	–	CP-7 (1) (2) (3)	CP-7 (1) (2) (3) (4)
CP-8	Usługi telekomunikacyjne	P1	–	CP-8 (1) (2)	CP-8 (1) (2) (3) (4)
CP-9	Kopia zapasowa	P1	CP-9	CP-9 (1)	CP-9 (1) (2) (3) (5)
CP-10	Odzyskiwanie i odtwarzanie systemu	P1	CP-10	CP-10 (2)	CP-10 (2) (4)
CP-11	Alternatywne protokoły komunikacyjne	P0	–	–	–
CP-12	Tryb bezpieczny	P0	–	–	–
CP-13	Alternatywne mechanizmy bezpieczeństwa	P0	–	–	–
Identyfikacja i uwierzytelnianie					
IA-1	Identyfikacja i uwierzytelnianie – polityka i procedury	P1	IA-1	IA-1	IA-1

Numer Zabezpieczenia	NAZWA ZABEZPIECZENIA	PRIORYTET	POZIOMY WPŁYWU NA ATRYBUTY BEZPIECZEŃSTWA INFORMACJI		
			NISKI	UMIARKOWANY	WYSOKI
IA-2	Identyfikacja i uwierzytelnianie (użytkownicy organizacyjni)	P1	IA-2 (1) (12)	IA-2 (1) (2) (3) (8) (11) (12)	IA-2 (1) (2) (3) (4) (8) (9) (11) (12)
IA-3	Identyfikacja i uwierzytelnianie urządzenia	P1	–	IA-3	IA-3
IA-4	Zarządzanie identyfikatorem	P1	IA-4	IA-4	IA-4
IA-5	Zarządzanie metodami uwierzytelniania	P1	IA-5 (1) (11)	IA-5 (1) (2) (3) (11)	IA-5 (1) (2) (3) (11)
IA-6	Ochrona procesu uwierzytelniania	P2	IA-6	IA-6	IA-6
IA-7	Uwierzytelnianie modułu kryptograficznego	P1	IA-7	IA-7	IA-7
IA-8	Identyfikacja i uwierzytelnianie (użytkownicy spoza organizacji)	P1	IA-8 (1) (2) (3) (4)	IA-8 (1) (2) (3) (4)	IA-8 (1) (2) (3) (4)
IA-9	Identyfikacja i uwierzytelnianie usługi	P0	–	–	–
IA-10	Identyfikacja i uwierzytelnianie adaptacyjne	P0	–	–	–
IA-11	Ponowne uwierzytelnianie	P0	–	–	–
Reagowanie na incydenty					
IR-1	Polityka i procedury reagowania na incydenty	P1	IR-1	IR-1	IR-1
IR-2	Szkolenie w zakresie reagowania na incydenty	P2	IR-2	IR-2	IR-2 (1) (2)
IR-3	Testowanie reagowania na incydenty	P2	–	IR-3 (2)	IR-3 (2)
IR-4	Obsługa incydentów	P1	IR-4	IR-4 (1)	IR-4 (1) (4)
IR-5	Monitorowanie incydentów	P1	IR-5	IR-5	IR-5 (1)
IR-6	Raportowanie incydentu	P1	IR-6	IR-6 (1)	IR-6 (1)
IR-7	Wsparcie reagowania na incydenty	P2	IR-7	IR-7 (1)	IR-7 (1)
IR-8	Plan reagowania na incydenty	P1	IR-8	IR-8	IR-8
IR-9	Informacja o wyciek / ujawnienie informacji	P0	–	–	–
IR-10	Zintegrowany zespół reagowania na incydenty	P0	–	–	–
Utrzymanie i wsparcie					
MA-1	Polityka i procedury utrzymania systemu	P1	MA-1	MA-1	MA-1

Numer Zabezpieczenia	NAZWA ZABEZPIECZENIA	PRIORYTET	POZIOMY WPŁYWU NA ATRYBUTY BEZPIECZEŃSTWA INFORMACJI		
			NISKI	UMIARKOWANY	WYSOKI
MA-2	Nadzór nad utrzymaniem	P2	MA-2	MA-2	MA-2 (2)
MA-3	Narzędzia utrzymaniowe	P2	–	MA-3 (1) (2)	MA-3 (1) (2) (3)
MA-4	Utrzymanie zdalne	P2	MA-4	MA-4 (2)	MA-4 (2) (3)
MA-5	Personel utrzymaniowy	P2	MA-5	MA-5	MA-5 (1)
MA-6	Terminowość przeprowadzania konserwacji	P2	–	MA-6	MA-6
Ochrona nośników danych					
MP-1	Polityka i procedury ochrony nośników danych	P1	MP-1	MP-1	MP-1
MP-2	Dostęp do nosników	P1	MP-2	MP-2	MP-2
MP-3	Oznakowanie nosników	P2	–	MP-3	MP-3
MP-4	Przechowywanie nośników	P1	–	MP-4	MP-4
MP-5	Transport nośników	P1	–	MP-5 (4)	MP-5 (4)
MP-6	Sanityzacja nośników	P1	MP-6	MP-6	MP-6 (1) (2) (3)
MP-7	Używanie nośników	P1	MP-7	MP-7 (1)	MP-7 (1)
MP-8	Deklasyfikacja nośników	P0	–	–	–
Ochrona fizyczna i środowiskowa					
PE-1	Polityka i procedury ochrony fizycznej i środowiskowej	P1	PE-1	PE-1	PE-1
PE-2	Zezwolenie na dostęp fizyczny	P1	PE-2	PE-2	PE-2
PE-3	Kontrola dostępu fizycznego	P1	PE-3	PE-3	PE-3 (1)
PE-4	Kontrola dostępu do medium transmisyjnego	P1	–	PE-4	PE-4
PE-5	Kontrola dostępu do urządzeń wejścia - wyjścia	P2	–	PE-5	PE-5
PE-6	Monitorowanie dostępu fizycznego	P1	PE-6	PE-6 (1)	PE-6 (1) (4)
PE-7	Kontrola gości	---	---	---	---
PE-8	Rejestracja dostępu gości	P3	PE-8	PE-8	PE-8 (1)
PE-9	Wyposażenie energetyczne i	P1	–	PE-9	PE-9

Numer Zabezpieczenia	NAZWA ZABEZPIECZENIA	PRIORYTET	POZIOMY WPŁYWU NA ATRYBUTY BEZPIECZEŃSTWA INFORMACJI		
			NISKI	UMIARKOWANY	WYSOKI
	okablowanie				
PE-10	Wyłączenia awaryjne	P1	–	PE-10	PE-10
PE-11	Zasilanie awaryjne	P1	–	PE-11	PE-11 (1)
PE-12	Oświetlenie awaryjne	P1	PE-12	PE-12	PE-12
PE-13	Ochrona przeciwpożarowa	P1	PE-13	PE-13 (3)	PE-13 (1) (2) (3)
PE-14	Kontrola temperatury i wilgotności	P1	PE-14	PE-14	PE-14
PE-15	Ochrona przed zalaniem	P1	PE-15	PE-15	PE-15 (1)
PE-16	Dostawa i usuwanie	P2	PE-16	PE-16	PE-16
PE-17	Zapasowe miejsca pracy	P2	–	PE-17	PE-17
PE-18	Lokalizacja elementów systemu teleinformatycznego	P3	–	–	PE-18
PE-19	Ulot informacji / elektromagnetyczna emisja ujawniająca	P0	–	–	–
PE-20	Monitorowanie i śledzenie zasobów	P0	–	–	–
Planowanie					
PL-1	Polityka i procedury planowania bezpieczeństwa	P1	PL-1	PL-1	PL-1
PL-2	Plan bezpieczeństwa systemu	P1	PL-2	PL-2 (3)	PL-2 (3)
PL-3	Aktualizacja planu bezpieczeństwa systemu	---	---	---	---
PL-4	Zasady postępowania	P2	PL-4	PL-4 (1)	PL-4 (1)
PL-5	Ocena wpływu na prywatność	---	---	---	---
PL-6	Planowanie działalności związanej z bezpieczeństwem	---	---	---	---
PL-7	Koncepcja bezpieczeństwa działań operacyjnych	P0	–	–	–
PL-8	Architektura bezpieczeństwa informacji	P1	–	PL-8	PL-8
PL-9	Zarządzanie centralne	P0	–	–	–
Programy bezpieczeństwa informacji					
PM-1	Plan programu bezpieczeństwa informacji	P1	PM-1	PM-1	PM-1

Numer Zabezpieczenia	NAZWA ZABEZPIECZENIA	PRIORYTET	POZIOMY WPŁYWU NA ATRYBUTY BEZPIECZEŃSTWA INFORMACJI		
			NISKI	UMIARKOWANY	WYSOKI
PM-2	Osoba odpowiedzialna za bezpieczeństwo informacji	P1	PM-2	PM-2	PM-2
PM-3	Środki bezpieczeństwa informacji	P1	PM-3	PM-3	PM-3
PM-4	Plan działania i etapy wprowadzania zabezpieczeń	P1	PM-4	PM-4	PM-4
PM-5	Inwentaryzacja systemu informacyjnego	P1	PM-5	PM-5	PM-5
PM-6	Skuteczność środków bezpieczeństwa informacji	P1	PM-6	PM-6	PM-6
PM-7	Struktura organizacyjna	P1	PM-7	PM-7	PM-7
PM-8	Plan infrastruktury krytycznej	P1	PM-8	PM-8	PM-8
PM-9	Strategia zarządzania ryzykiem	P1	PM-9	PM-9	PM-9
PM-10	Proces autoryzacji zabezpieczeń	P1	PM-10	PM-10	PM-10
PM-11	Definicja misji / procesu biznesowego	P1	PM-11	PM-11	PM-11
PM-12	Zagrożenia wewnętrzne	P1	PM-12	PM-12	PM-12
PM-13	Personel bezpieczeństwa informacji	P1	PM-13	PM-13	PM-13
PM-14	Testowanie, szkolenia i monitorowanie	P1	PM-14	PM-14	PM-14
PM-15	Kontakty z grupami i stowarzyszeniami zajmującymi się bezpieczeństwem informacji	P3	PM-15	PM-15	PM-15
PM-16	Ostrzeganie o zagrożeniach	P1	PM-16	PM-16	PM-16
Bezpieczeństwo osobowe					
PS-1	Bezpieczeństwo osobowe – polityka i procedury	P1	PS-1	PS-1	PS-1
PS-2	Określanie ryzyka dla stanowiska pracy	P1	PS-2	PS-2	PS-2
PS-3	Dobór personelu	P1	PS-3	PS-3	PS-3
PS-4	Zakończenie zatrudnienia	P1	PS-4	PS-4	PS-4 (2)
PS-5	Obsadzenie lub przeniesienie stanowiska	P2	PS-5	PS-5	PS-5
PS-6	Umowy dostępu / współpracy	P3	PS-6	PS-6	PS-6
PS-7	Bezpieczeństwo osobowe stron trzecich	P1	PS-7	PS-7	PS-7

Numer Zabezpieczenia	NAZWA ZABEZPIECZENIA	PRIORYTET	POZIOMY WPŁYWU NA ATRYBUTY BEZPIECZEŃSTWA INFORMACJI		
			NISKI	UMIARKOWANY	WYSOKI
PS-8	Sankcje personalne	P3	PS-8	PS-8	PS-8
Ocena ryzyka					
RA-1	Polityka i procedury szacowania ryzyka	P1	RA-1	RA-1	RA-1
RA-2	Kategoryzacja bezpieczeństwa	P1	RA-2	RA-2	RA-2
RA-3	Szacowanie ryzyka	P1	RA-3	RA-3	RA-3
RA-4	Aktualizacja szacowania ryzyka	---	---	---	---
RA-5	Skanowanie podatności	P1	RA-5	RA-5 (1) (2) (5)	RA-5 (1) (2) (4) (5)
RA-6	Techniczne zabezpieczenie przed podglądem i podsłuchem	P0	–	–	–
Nabycie systemu i usług					
SA-1	Polityka i procedury nabywania systemu i usług	P1	SA-1	SA-1	SA-1
SA-2	Przydział zasobów	P1	SA-2	SA-2	SA-2
SA-3	Cykl życia systemu	P1	SA-3	SA-3	SA-3
SA-4	Proces nabycia	P1	SA-4 (10)	SA-4 (1) (2) (9) (10)	SA-4 (1) (2) (9) (10)
SA-5	Dokumentacja systemu teleinformatycznego	P2	SA-5	SA-5	SA-5
SA-6	Ograniczenia w użyciu oprogramowania	---	---	---	---
SA-7	Oprogramowanie instalowane przez użytkownika	---	---	---	---
SA-8	Zarządzanie bezpieczeństwem informacji	P1	–	SA-8	SA-8
SA-9	Usługi zewnętrznego systemu informatycznego	P1	SA-9	SA-9 (2)	SA-9 (2)
SA-10	Zarządzanie konfiguracją dewelopera	P1	–	SA-10	SA-10
SA-11	Testowanie i ocena bezpieczeństwa przez dewelopera	P1	–	SA-11	SA-11
SA-12	Bezpieczeństwo łańcucha dostaw	P1	–	–	SA-12
SA-13	Wiarygodność	P0	–	–	–

Numer Zabezpieczenia	NAZWA ZABEZPIECZENIA	PRIORYTET	POZIOMY WPŁYWU NA ATRYBUTY BEZPIECZEŃSTWA INFORMACJI		
			NISKI	UMIARKOWANY	WYSOKI
SA-14	Analiza krytyczności	P0	–	–	–
SA-15	Proces rozwoju, standardy i narzędzia	P2	–	–	SA-15
SA-16	Szkolenie dostarczone przez dewelopera	P2	–	–	SA-16
SA-17	Architektura i projekt bezpieczeństwa dewelopera	P1	–	–	SA-17
SA-18	Odporność na sabotaż i i wykrywanie manipulacji	P0	–	–	–
SA-19	Autentyczność komponentów	P0	–	–	–
SA-20	Niestandardowa (na zamówienie) rozbudowa komponentów krytycznych	P0	–	–	–
SA-21	Dobór deweloperów	P0	–	–	–
SA-22	Komponenty systemu bez wsparcia	P0	–	–	–
Ochrona systemów i sieci telekomunikacyjnych					
SC-1	Polityka i procedury ochrony systemów i sieci telekomunikacyjnych	P1	SC-1	SC-1	SC-1
SC-2	Separacja	P1	–	SC-2	SC-2
SC-3	Izolacja funkcji bezpieczeństwa	P1	–	–	SC-3
SC-4	Informacje we współdzielonych zasobach	P1	–	SC-4	SC-4
SC-5	Ochrona przed blokadą usług (DoS)	P1	SC-5	SC-5	SC-5
SC-6	Dostępność zasobów	P0	–	–	–
SC-7	Ochrona połączeń brzegowych	P1	SC-7	SC-7 (3) (4) (5) (7)	SC-7 (3) (4) (5) (7) (8) (18) (21)
SC-8	Poufność i integralność transmisji	P1	–	SC-8 (1)	SC-8 (1)
SC-9	Poufność transmisji	---	---	---	---
SC-10	Zakończenie połączenia sieciowego	P2	–	SC-10	SC-10
SC-11	Zaufana ścieżka komunikacyjna	P0	–	–	–
SC-12	Generowanie i zarządzanie kluczami kryptograficznymi	P1	SC-12	SC-12	SC-12 (1)
SC-13	Ochrona kryptograficzna	P1	SC-13	SC-13	SC-13

Numer Zabezpieczenia	NAZWA ZABEZPIECZENIA	PRIORYTET	POZIOMY WPŁYWU NA ATRYBUTY BEZPIECZEŃSTWA INFORMACJI		
			NISKI	UMIARKOWANY	WYSOKI
SC-14	Ochrona dostępu publicznego	---	---	---	---
SC-15	Współpracujące urządzenia komputerowe	P1	SC-15	SC-15	SC-15
SC-16	Transmisja atrybutów bezpieczeństwa	P0	–	–	–
SC-17	Certyfikaty infrastruktury klucza publicznego	P1	–	SC-17	SC-17
SC-18	Kod mobilny	P2	–	SC-18	SC-18
SC-19	Protokół transmisji pakietowej (VoIP)	P1	–	SC-19	SC-19
SC-20	Bezpieczeństwo nazw domen / adresów IP (autentyczność pochodzenia)	P1	SC-20	SC-20	SC-20
SC-21	Bezpieczeństwo nazw domen / usługa ustalania adresu IP	P1	SC-21	SC-21	SC-21
SC-22	Architektura nazw domen / adresów IP / zamawianie usług DNS	P1	SC-22	SC-22	SC-22
SC-23	Autentyczność sesji	P1	–	SC-23	SC-23
SC-24	Przejście do określonego stanu systemu po błędzie	P1	–	–	SC-24
SC-25	Think nodes / terminalowe stacje robocze	P0	–	–	–
SC-26	Honeypots	P0	–	–	–
SC-27	Wieloplatformowość aplikacji	P0	–	–	–
SC-28	Ochrona danych w składowaniu / kopie konfiguracji systemu	P1	–	SC-28	SC-28
SC-29	Heterogoniczność systemu	P0	–	–	–
SC-30	Maskowanie i dezinformacja	P0	–	–	–
SC-31	Analiza ukrytego kanału komunikacji	P0	–	–	–
SC-32	Dzielenie systemu teleinformatycznego na partycje	P0	–	–	–
SC-33	Integralność transmisji	---	---	---	---
SC-34	Niemodyfikowalne programy wykonywalne	P0	–	–	–
SC-35	Honeyclients	P0	–	–	–

Numer Zabezpieczenia	NAZWA ZABEZPIECZENIA	PRIORYTET	POZIOMY WPŁYWU NA ATRYBUTY BEZPIECZEŃSTWA INFORMACJI		
			NISKI	UMIARKOWANY	WYSOKI
SC-36	Przetwarzanie i przechowywanie rozproszone	P0	–	–	–
SC-37	Kanały pozapasmowe	P0	–	–	–
SC-38	Bezpieczeństwo operacji	P0	–	–	–
SC-39	Izolacja procesów	P1	SC-39	SC-39	SC-39
SC-40	Ochrona łącza bezprzewodowego	P0	–	–	–
SC-41	Dostęp do portów i urządzeń wejścia / wyjścia	P0	–	–	–
SC-42	Czujniki	P0	–	–	–
SC-43	Ograniczenia użycia	P0	–	–	–
SC-44	Komory detonacyjne	P0	–	–	–
Integralność systemu i informacji					
SI-1	Polityka i procedury integralności systemu i informacji	P1	SI-1	SI-1	SI-1
SI-2	Usuwanie usterek	P1	SI-2	SI-2 (2)	SI-2 (1) (2)
SI-3	Zabezoieczenie przed złośliwym kodem	P1	SI-3	SI-3 (1) (2)	SI-3 (1) (2)
SI-4	Monitorowanie systemu teleinformatycznego	P1	SI-4	SI-4 (2) (4) (5)	SI-4 (2) (4) (5)
SI-5	Alerty bezpieczeństwa, porady i dyrektywy	P1	SI-5	SI-5	SI-5 (1)
SI-6	Weryfikacja funkcji bezpieczeństwa	P1	–	–	SI-6
SI-7	Aplikacje, oprogramowanie układowe i integralność informacji	P1	–	SI-7 (1) (7)	SI-7 (1) (2) (5) (7) (14)
SI-8	Ochrona przed spamem	P2	–	SI-8 (1) (2)	SI-8 (1) (2)
SI-9	Ograniczenia wprowadzania informacji	---	---	---	---
SI-10	Weryfikacja wprowadzanych informacji	P1	–	SI-10	SI-10
SI-11	Obsługa błędów	P2	–	SI-11	SI-11
SI-12	Przechowywaniei retencja informacji	P2	SI-12	SI-12	SI-12
SI-13	Przewidywanie awarii	P0	–	–	–

Numer Zabezpieczenia	NAZWA ZABEZPIECZENIA	PRIORYTET	POZIOMY WPŁYWU NA ATRYBUTY BEZPIECZEŃSTWA INFORMACJI		
			NISKI	UMIARKOWANY	WYSOKI
SI-14	Zapobieganie zaawansowanym długotrwałym atakom (ataki typu APT)	P0	–	–	–
SI-15	Filtrowanie informacji wyjściowych	P0	–	–	–
SI-16	Ochrona pamięci	P1	–	SI-16	SI-16
SI-17	Bezpieczne procedury	P0	–	–	–

KATEGORIA: KONTROLA DOSTĘPU

AC-1 POLITYKA I PROCEDURY KONTROLI DOSTĘPU

Zabezpieczenie: Organizacja[1]:

a. [*Realizacja[2]: personel lub role zdefiniowane przez organizację*] opracowuje, dokumentuje i rozpowszechnia:
   1. Politykę kontroli dostępu, która dotyczy celu, zakresu, ról, obowiązków, zaangażowania kierownictwa, koordynacji między jednostkami organizacyjnymi i ich przestrzegania;
   2. Procedury umożliwiające wdrożenie polityki kontroli dostępu i zabezpieczeń powiązanych;
b. Przegląda i aktualizuje z ustaloną częstotliwością:
   1. Politykę kontroli dostępu [*Realizacja: częstotliwość określona przez organizację*];
   2. Procedury kontroli dostępu [*Realizacja: częstotliwość określona przez organizację*].

Zabezpieczenia powiązane: PM-9.
Zabezpieczenia rozszerzone: Brak.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia[3]	**Potencjalny wpływ[4] na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji[5]**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń[6]		
	AC-1	AC-1	AC-1

[1] Organizacja – wyspecjalizowana jednostka o dowolnej wielkości, złożoności lub pozycjonowaniu w ramach struktury organizacyjnej (np. przedsiębiorstwo, urząd, itp., lub w stosownych przypadkach, którykolwiek z elementów operacyjnych przedsiębiorstwa, urzędu, itp.).
[2] *Realizacja* – proces dotyczy całego dokumentu. W tym miejscu Organizacja wstawia odpowiednie odwołanie nawiązujące do czynności, które powinny być wykonane w tym zabezpieczeniu.
[3] Priorytety wdrożenia środków bezpieczeństwa. Priorytet P1 – implementacja podstawowych zabezpieczeń w pierwszej kolejności; P2 – implementacja podstawowych zabezpieczeń po wdrożeniu priorytetu P1; P3 - implementacja podstawowych zabezpieczeń po wdrożeniu priorytetów P1 i P2; P0 - zabezpieczenia nieokreślone w katalogu podstawowych zabezpieczeń (załącznik nr 4) i stosowanie ich jest opcjonalne.
[4] Potencjalny wpływ: **Niski** - można oczekiwać, że utrata poufności, integralności lub dostępności będzie miała ograniczony negatywny wpływ na operacje organizacyjne, zasoby organizacyjne lub osoby fizyczne; **Umiarkowany** - można oczekiwać, że utrata poufności, integralności lub dostępności będzie miała poważny negatywny wpływ na operacje organizacyjne, zasoby organizacyjne lub osoby fizyczne; **Wysoki** - można oczekiwać, że utrata poufności, integralności lub dostępności będzie miała poważny lub katastrofalny niekorzystny wpływ na operacje organizacyjne, zasoby organizacyjne lub osoby fizyczne.
[5] Atrybuty bezpieczeństwa informacji (systemu teleinformatycznego) – poufność, integralność, dostępność.
[6] Minimalne wymagane środki bezpieczeństwa do zaimplementowania w systemie teleinformatycznym.

AC-2 ZARZĄDZANIE KONTEM

Zabezpieczenie: Organizacja:

a. Identyfikuje i ustanawia klasy kont w systemie teleinformatycznym z uwzględnieniem ról biznesowych w organizacji: [*Realizacja: typy kont systemu teleinformatycznego zdefiniowane przez organizację*];

b. Ustanawia zarządzających systemem kont;

c. Ustanawia zasady członkostwa w poszczególnych klasach kont oraz uprawnienia związane z przynależnością do danej klasy

d. Dla każdej klasy kont ustanawia uprawnienia związane z przynależnością do danej klasy;

e. Wymaga zatwierdzenia przez uprawnione [*Realizacja: personel lub role zdefiniowane przez organizację*] wniosków o utworzenie konta w systemie teleinformatycznym;

f. Tworzy, włącza, modyfikuje, wyłącza i usuwa konta w systemie teleinformatycznym zgodnie z [*Realizacja: procedury lub warunki zdefiniowane przez organizację*];

g. Monitoruje wykorzystanie kont w systemie teleinformatycznym;

h. Powiadamia zarządzających kontami w przypadkach gdy:

   1. Konta nie są już wymagane;

   2. Użytkownik konta zostaje zwolniony lub przeniesiony na inne stanowisko;

   3. Zajdą zmiany w zakresie obowiązków na danym stanowisku w zakresie korzystania z systemu teleinformatycznego lub zmieni się zakres wiedzy niezbędnej (need-to-know) na danym stanowisku;

i. Autoryzuje dostęp do systemu teleinformatycznego w oparciu o:

   1. Wymagane uprawnienia;

   2. Zamierzony cele użycia systemu;

   3. Inne atrybuty wymagane przez organizację lub powiązane z działaniami statutowymi lub funkcjami biznesowymi;

j. Przegląda konta pod kątem zgodności z ustalonymi wymogami zarządzania kontami [*Realizacja: częstotliwość określona przez organizację*];

k. Jeśli w systemie są konta współużytkowane ustanawia proces ponownego wystawiania środków uwierzytelniających do takiego konta po usunięciu osób z grona współużytkowników;

l. Dopasowuje procesy zarządzania kontem do procesów zwalniania i przenoszenia pracowników.

Zabezpieczenia powiązane: AC-3, AC-4, AC-5, AC-6, AC-10, AC-17, AC-19, AC-20, AU-9, IA-2, IA-4, IA-5, IA-8, CM-5, CM-6, CM-11, MA-3, MA-4, MA-5, PL-4, SC-13.

Zabezpieczenia rozszerzone:

(1) ZARZĄDZANIE KONTAMI | AUTOMATYCZNE ZARZĄDZANIE KONTEM SYSTEMU

Organizacja stosuje zautomatyzowane mechanizmy wspierające zarządzanie kontami systemów teleinformatycznych.

(2) ZARZĄDZANIE KONTAMI | USUWANIE KONT TYMCZASOWYCH / AWARYJNYCH

System teleinformatyczny automatycznie [*Realizacja: usuwa; wyłącza*] konta tymczasowe lub awaryjne po okresie zdefiniowanym przez organizację dla każdego rodzaju konta.

(3) ZARZĄDZANIE KONTAMI | WYŁĄCZANIE KONT NIEAKTYWNYCH

System teleinformatyczny automatycznie wyłącza nieaktywne konta po *[Realizacja: okres zdefiniowany przez organizację]*.

(4) ZARZĄDZANIE KONTAMI | AUTOMATYCZNE DZIAŁANIA AUDYTOWE

System teleinformatyczny automatycznie tworzy, modyfikuje, włącza, wyłącza i usuwa konta oraz powiadamia *[Realizacja: personel lub role zdefiniowane przez organizację].*

Zabezpieczenia powiązane: AU-2, AU-12.

(5) ZARZĄDZANIE KONTAMI | WYLOGOWANIE PO OKREŚLONYM OKRESIE NIEAKTYWNOŚCI

Organizacja wymaga, aby użytkownicy wylogowali się po [*Realizacja: zdefiniowany przez organizację okresie bezczynności lub automatyczne wylogowanie po ustalonym okresie bezczynności*].

Zabezpieczenia powiązane: SC-23.

(6) ZARZĄDZANIE KONTAMI | DYNAMICZNE ZARZĄDZANIE UPRAWNIENIAMI

W system teleinformatycznym zaimplementowane są możliwości dynamicznego zarządzania uprawnieniami zgodnie z [*Realizacja: przyjęty przez organizację wykaz możliwości dynamicznego zarządzania zdefiniowanymi uprawnieniami*].

Zabezpieczenia powiązane: AC-16.

(7) ZARZĄDZANIE KONTAMI | SCHEMATY KONTROLI DOSTĘPU OPARTE NA ROLACH

Organizacja:

(a) ustanawia konta użytkowników uprzywilejowanych i administruje nimi zgodnie ze schematem dostępu opartym na rolach. Schemat ten określa dozwolony dostęp i uprawnienia do systemu teleinformatycznego w oparciu o role użytkowników pełnione w organizacji;

(b) monitoruje żądania uprzywilejowanego przypisania ról;

(c) przeprowadza [*Realizacja: stosowne procedury zdefiniowane przez organizację*], gdy uprzywilejowane przypisania ról nie są już niezbędne.

(8) ZARZĄDZANIE KONTAMI | TWORZENIE KONTA DYNAMICZNEGO

System teleinformatyczny tworzy *[Realizacja: konta systemu teleinformatycznego zdefiniowane przez organizację]* dynamicznie.

Zabezpieczenia powiązane: AC- 16.

(9) ZARZĄDZANIE KONTAMI WSPÓLNYMI

Organizacja zezwala na korzystanie ze kont wspólnych / grupowych, które spełniają *[Realizacja: zdefiniowane przez organizację warunki zakładania kont wspólnych / grupowych].*

(10) ZARZĄDZANIE KONTAMI | ROZWIĄZANIE URUCHOMIENIA KONTA UDZIELONEGO | GRUPOWEGO

System teleinformatyczny uniemożliwia dostęp do konta wspólnego użytkownikowi opuszczającemu grupę.

(11) ZARZĄDZANIE KONTAMI | WARUNKI UŻYTKOWANIA

System teleinformatyczny wymusza [*Realizacja: działania według z góry zdefiniowanych przez organizację warunków*] w stosunku do systemu kont [*Realizacja: konta systemu teleinformatycznego zdefiniowane przez organizację]*.

(12)ZARZĄDZANIE KONTAMI | MONITOROWANIE KONTA, NIETYPOWE UŻYTKOWANIE KONTA

Organizacja:

(a) monitoruje konta dostępowe do systemu teleinformatycznego pod kątem [*Realizacja: nietypowe użycie według zdefiniowanych przez organizację zasad*];

(b) zgłasza nietypowe wykorzystanie kont systemu teleinformatycznego [*Realizacja: określonemu personelowi lub roli według zasad zdefiniowanych przez organizację*].

Zabezpieczenia powiązane: CA-7.

(13) ZARZĄDZANIE KONTAMI | WYŁĄCZANIE KONT DOSTĘPOWYCH UŻYTKOWNIKOM WYSOKIEGO RYZYKA

Organizacja niezwłocznie wyłącza konta użytkowników stwarzających znaczące ryzyko w ciągu *[Realizacja: okres zdefiniowany przez organizację] od* wykrycia ryzyka.

Zabezpieczenia Powiązane: PS-4.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa[7]

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	AC-2	AC-2 (1) (2) (3) (4)	AC-2 (1) (2) (3) (4) (5) (11) (12) (13)

[7] Interpretacja tabeli:

AC-3 EGZEKWOWANIE UPRAWNIEŃ DOSTĘPU

Zabezpieczenie: System teleinformatyczny wymusza na użytkowniku stosowanie zatwierdzonych zasad uzyskiwania uprawnień logicznego dostępu do informacji i zasobów systemowych zgodnie z obowiązującymi w organizacji zasadami kontroli dostępu.

Zabezpieczenia powiązane: AC-2, AC-4, AC-5, AC-6, AC-16, AC-17, AC-18, AC-19, AC-20, AC-21, AC-22, AU-9 , CM-5, CM-6, CM-11, MA-3, MA-4, MA-5, PE-3.

Zabezpieczenia rozszerzone:

(1) EGZEKWOWANIE UPRAWNIEŃ DOSTĘPU – OGRANICZONY DOSTĘP DO FUNKCJI UPRZYWILEJOWANYCH

Włączone do AC-6

(2) EGZEKWOWANIE UPRAWNIEŃ DOSTĘPU – PODWÓJNA AUTORYZACJA

Dla działań uprzywilejowanych [*Realizacja: uprzywilejowane polecenia zdefiniowane przez organizację i / lub inne działania zdefiniowane przez organizację]* system teleinformatyczny wymusza podwójną autoryzację.
Zabezpieczenia powiązane: CP-9, MP-6.

(3) EGZEKWOWANIE UPRAWNIEŃ DOSTĘPU – OBOWIĄZKOWA KONTROLA DOSTĘPU

System teleinformatyczny wymusza, zgodnie z *[Realizacja: obowiązkowa polityka kontroli dostępu zdefiniowana przez organizację*] w stosunku do wszystkich podmiotów [8]i obiektów[9], ustaloną w organizacji politykę kontroli dostępu, która:

(a) jest jednolicie egzekwowana wobec wszystkich podmiotów i obiektów w obszarze danego systemu teleinformatycznego;

(b) określa, że podmiot, któremu udzielono dostępu do informacji, nie może wykonywać żadnej z poniższych czynności:

- W systemie oszacowanym jako „Wysoki potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji" obligatoryjnie stosuje się w pierwszej kolejności, z priorytetem wdrożenia – P1, zabezpieczenia podstawowe Katalogu AC-2 (oraz odnoszące się do nich „Powiązane zabezpieczenia"), a także rozszerzone zabezpieczenia AC-2(1) (2) (3) (4) (5) (11) (12) (13). Rozszerzone zabezpieczenia AC-2(6) do AC-2(10) mogą być stosowane opcjonalnie w celu zwiększenia odporności systemu.
- W systemie oszacowanym jako „Umiarkowany potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji" obligatoryjnie stosuje się w pierwszej kolejności, z priorytetem wdrożenia – P1, zabezpieczenia podstawowe Katalogu AC-2 (oraz odnoszące się do nich „Powiązane zabezpieczenia"), a także rozszerzone zabezpieczenia AC-2 (1) (2) (3) (4). Pozostałe rozszerzone zabezpieczenia mogą być zastosowane opcjonalnie w celu zwiększenia odporności systemu.
- W systemie oszacowanym jako „Niski potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji" obligatoryjnie stosuje się, z priorytetem wdrożenia – P1, podstawowe zabezpieczenia (opisane pod hasłem Zabezpieczenia) Katalogu AC-2, oraz odnoszące się do nich „Zabezpieczenia powiązane". Implementacja Zabezpieczeń rozszerzonych nie jest wymagana. Mogą być one zastosowane opcjonalnie w celu zwiększenia odporności systemu.

[8] Podmiot - użytkownik lub proces działający w imieniu użytkownika.

[9] Obiekt - np. urządzenia, pliki, rekordy, domeny.

1) przekazywania informacji nieupoważnionym podmiotom lub obiektom;
2) udzielania przydzielonych przywilejów innym podmiotom;
3) jakiejkolwiek zmiany atrybutów (właściwości) bezpieczeństwa pomiotów, obiektów systemu teleinformatycznego lub jego elementów;
4) wyboru atrybutów bezpieczeństwa i ich wartości w odniesieniu do obiektów nowo tworzonych lub zmodyfikowanych;
5) zmiany zasad zarządzania kontrolą dostępu;

(c) stanowi, że dla jednoznacznie określonych w tej polityce podmiotów (podmioty zaufane) [*Realizacja: podmioty zdefiniowane przez organizację*] mogą zostać przyznane uprawnienia, które nie podlegają wybranym lub wszystkimi powyższym ograniczeniom [*Realizacja: uprawnienia zdefiniowane przez organizację*], tak aby podmioty te nie były ograniczone niektórymi lub wszystkimi powyższymi ograniczeniami.

Zabezpieczenia powiązane: AC-25, SC-11.

(4) EGZEKWOWANIE UPRAWNIEŃ DOSTĘPU – UZNANIOWA KONTROLA DOSTĘPU

Dla ściśle zdefiniowanych sytuacji może być stosowana uznaniowa polityka kontroli dostępu *[Realizacja: zdefiniowana przez organizację uznaniowa polityka kontroli dostępu]* według której podmioty lub obiekty, mogą wykonać co najmniej jedną z następujących czynności:

(a) Przekazywać informacje innym podmiotom lub obiektom;
(b) Przyznać swoje przywileje (atrybuty) innym obiektom;
(c) Zmienić atrybuty bezpieczeństwa dotyczące podmiotów, obiektów, systemu teleinformatycznego lub jego elementów;
(d) Wskazać atrybuty bezpieczeństwa, które zostaną powiązane z nowo utworzonymi lub skorygowanymi obiektami;
(e) Zmienić zasady dotyczące kontroli dostępu.

(5) EGZEKWOWANIE UPRAWNIEŃ DOSTĘPU – INFORMACJE DOTYCZĄCE BEZPIECZEŃSTWA

System teleinformatyczny uniemożliwia dostęp do [*Realizacja: określonej przez organizację informacji istotnej dla bezpieczeństwa*], za wyjątkiem sytuacji gdy system znajduje się w stanie nieoperacyjnym.

Zabezpieczenie Powiązane: CM-3.

(6) EGZEKWOWANIE UPRAWNIEŃ DOSTĘPU | OCHRONA INFORMACJI UŻYTKOWNIKA I SYSTEMU

[Włączone do MP-4 i SC-28].

(7) EGZEKWOWANIE UPRAWNIEŃ DOSTĘPU – KONTROLA DOSTĘPU DO ROLI (RBAC)

System teleinformatyczny wymusza zdefiniowaną przez organizację dla podmiotów i

obiektów politykę kontroli dostępu opartą na rolach[10] [*Realizacja: role zdefiniowane przez organizację i użytkownicy upoważnieni do przyjmowania takich ról*].

(8) EGZEKWOWANIE UPRAWNIEŃ DOSTĘPU – ODWOŁANIE ZEZWOLEŃ NA DOSTĘP

System teleinformatyczny wymusza według reguły zdefiniowanej przez organizację cofanie zezwoleń na dostęp w wyniku zmian atrybutów bezpieczeństwa podmiotów i obiektów, na podstawie [Realizacja: *reguły zdefiniowane przez organizację regulujące czas cofania zezwoleń na dostęp*].

(9) EGZEKWOWANIE UPRAWNIEŃ DOSTĘPU – KONTROLOWANE UDOSTĘPNIENIE INFORMACJI

System teleinformatyczny nie udostępnia informacji poza ustaloną granicą systemu, chyba że:

(a) Odbiorca informacji [*Realizacja: system teleinformatyczny lub komponent systemu zdefiniowany przez organizację*] spełnia wymagania zdefiniowane przez organizację [*Realizacja: środki bezpieczeństwa zdefiniowane przez organizację];*

(b) Istnieją podstawy prawne do udostępnienia informacji.

(10) EGZEKWOWANIE UPRAWNIEŃ DOSTĘPU – NADZOROWANE OBEJŚCIE MECHANIZMÓW KONTROLI DOSTĘPU

W warunkach [*Realizacja: warunkach zdefiniowanych przez organizację*] mogą być stosowane nadzorowane obejścia mechanizmów automatycznej kontroli dostępu.

Zabezpieczenia powiązane: AU-2, AU-6.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	AC-3	AC-3	AC-3

[10] Organizacje mogą tworzyć określone role na podstawie funkcji zadań i uprawnień do wykonywania niezbędnych operacji w systemach teleinformatycznych organizacji, powiązanych z rolami zdefiniowanymi przez organizację.

AC-4 EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI

Zabezpieczenie: System teleinformatyczny wymusza stosowanie określonych przez organizację zasad kontrolowania przepływu informacji w systemie i między systemem, a systemami współpracującymi na podstawie [*Realizacja: zasady kontroli przepływu informacji zdefiniowane przez organizację*].

Zabezpieczenia powiązane: AC-3, AC-17, AC-19, AC-21, CM-6, CM-7, SA-8, SC-2, SC-5, SC-7, SC-18.

Zabezpieczenia rozszerzone:

(1) EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI – ATRYBUTY BEZPIECZEŃSTWA PODMIOTU LUB OBIEKTU

Do wydania decyzji o możliwości przepływu informacji [*Realizacja: informacje zdefiniowane przez organizację]* pomiędzy jej źródłem i przeznaczeniem, system teleinformatyczny wykorzystuje zdefiniowane przez organizację atrybuty bezpieczeństwa *[Realizacja: atrybuty zabezpieczeń zdefiniowane przez organizację]* związane z tymi informacjami, *w* celu wymuszenia [Realizacja*: zasady kontroli przepływu informacji zdefiniowane przez organizację]*.

Zabezpieczenia powiązane: AC-16.

(2) EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI – PRZETWARZANIE DOMEN

W systemach teleinformatycznych stosujących przetwarzanie w chronionych domenach organizacja definiuje [*Realizacja: zdefiniowane przez organizację zasady kontroli przepływu informacji]* zasady sterowania przepływem informacji pomiędzy domenami.

(3) EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI – DYNAMICZNA KONTROLA PRZEPŁYWU INFORMACJI

System teleinformatyczny wymusza dynamiczną kontrolę przepływu informacji w oparciu o [*Realizacja: zasady zdefiniowane przez organizację*].

Zabezpieczenia powiązane: SI-4.

(4) EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI – SPRAWDZANIE ZAWARTOŚCI ZASZYFROWANEJ INFORMACJI

Organizacja ustala procedury [*Realizacja:* w*ybór*[11] *(jeden lub więcej): odszyfrowanie informacji; blokowanie przepływu zaszyfrowanych informacji; kończenie sesji komunikacyjnych próbujących przekazać zaszyfrowane informacje*] zabezpieczające system teleinformatyczny [*Realizacja: procedura lub metoda zdefiniowane przez organizację*] przed potencjalnie szkodliwym wpływem informacji zaszyfrowanej.

Zabezpieczenia powiązane: SI-4.

[11] *Wybór* - proces dotyczy całego dokumentu. W miejscu tym Organizacja dokonuje wyboru jednego lub kilku czynników wskazanych w danym zdaniu.

(5) EGZEKWOWANIE ZASAD PRZEPŁYWU INFORMACJI – WBUDOWANE RODZAJE DANYCH

System teleinformatyczny wymusza [*Realizacja: zdefiniowane przez organizację ograniczenia*] osadzanie określonych typów danych w miejsce innych typów danych.

(6) EGZEKWOWANIE PRZEPŁYWU INFORMACJI – METADANE

System teleinformatyczny wymusza kontrolę przepływu informacji na podstawie [*Realizacja: zdefiniowane przez organizację metadane*].

Zabezpieczenia powiązane: AC-16, SI-7.

(7) EGZEKWOWANIE PRZEPŁYWU INFORMACJI – MECHANIZMY PRZEPŁYWU JEDNOSTRONNEGO

System teleinformatyczny dla obszarów definiowanych przez organizacje wymusza za pomocą mechanizmów sprzętowych [*Realizacja: jednokierunkowe przepływy informacji zdefiniowane przez organizację*].

(8) EGZEKWOWANIE PRZEPŁYWU INFORMACJI – FILTRY POLITYKI BEZPIECZEŃSTWA

System teleinformatyczny wymusza zabezpieczenie przepływu informacji przy użyciu [*Realizacja: zdefiniowane przez organizację filtry bezpieczeństwa*] jako podstawy do decyzji dotyczących kontroli przepływu informacji [*Realizacja: przepływy informacji zdefiniowane przez organizację*].

(9) EGZEKWOWANIE PRZEPŁYWU INFORMACJI – OCENA PRZEZ UPRAWNIONĄ OSOBĘ

System teleinformatyczny dla informacji zdefiniowanych przez organizację wymusza stosowanie oceny dopuszczalności przepływu przez uprawnioną osobę, pod następującymi warunkami *[Realizacja: warunki zdefiniowane przez organizację].*

(10) EGZEKWOWANIE PRZEPŁYWU INFORMACJI – WŁĄCZANIE/ WYŁĄCZANIE FILTRÓW POLITYKI BEZPIECZEŃSTWA

System teleinformatyczny umożliwia upoważnionym osobom włączanie lub wyłączanie filtrów zdefiniowanych przez polityki bezpieczeństwa [Realizacja: *filtry polityki bezpieczeństwa zdefiniowane przez organizację]* pod ustalonymi przez organizację warunkami [*Realizacja: warunki zdefiniowane przez organizację].*

(11) EGZEKWOWANIE PRZEPŁYWU INFORMACJI – KONFIGURACJA FILTRÓW POLITYKI BEZPIECZEŃSTWA

System teleinformatyczny umożliwia upoważnionym osobom konfigurowanie filtrów bezpieczeństwa [*Realizacja: filtry bezpieczeństwa zdefiniowane przez organizację*] w celu obsługi różnych polityk bezpieczeństwa.

(12) EGZEKWOWANIE PRZEPŁYWU INFORMACJI – IDENTYFIKATORY TYPU DANYCH

System teleinformatyczny do sprawdzania poprawności danych niezbędnych przy podejmowaniu decyzji dotyczących przepływu informacji, przesyłając informacje między różnymi domenami bezpieczeństwa, wykorzystuje identyfikatory typu danych zdefiniowane przez organizację [*Realizacja: identyfikatory typu danych zdefiniowane przez organizację]*.

(13) EGZEKWOWANIE PRZEPŁYWU INFORMACJI – DEKOMPOZYCJA INFORMACJI NA ODPOWIEDNIE PODSKŁADNIKI

System teleinformatyczny w celu podporządkowania się mechanizmom egzekwowania polityki, przesyłając informacje między różnymi domenami bezpieczeństwa może je rozkładać na zdefiniowane przez organizację odpowiednie podskładniki, istotne dla polityki bezpieczeństwa *[Realizacja: zdefiniowane przez organizację podskładniki istotne dla polityki bezpieczeństwa*].

(14) EGZEKWOWANIE PRZEPŁYWU INFORMACJI – POLITYKA STOSOWANIA FILTRÓW BEZPIECZEŃSTWA

System teleinformatyczny, przesyłając informacje między różnymi domenami bezpieczeństwa, implementuje [*Realizacja: zdefiniowane przez organizację filtry polityki bezpieczeństwa*], wymagając określonych formatów, które ograniczają strukturę i zawartość danych.

(15) EGZEKWOWANIE PRZEPŁYWU INFORMACJI – WYKRYWANIE INFORMACJI NIEAKCEPTOWANYCH

System teleinformatyczny, przesyłając informacje między różnymi domenami bezpieczeństwa, sprawdza informacje pod kątem obecności informacji nieakceptowanych [*Realizacja: informacje nieakceptowane określone przez organizację*] przez [*Realizacja: określoną politykę bezpieczeństwa zdefiniowana przez organizację*] i zabrania przesyłania takich informacji.

Zabezpieczenia powiązane: SI-3.

(16) EGZEKWOWANIE PRZEPŁYWU INFORMACJI | PRZEKAZYWANIE INFORMACJI POMIĘDZY SYSTEMAMI TELEINFORMATYCZNYMI

[Włączone do AC-4].

(17) EGZEKWOWANIE PRZEPŁYWU INFORMACJI | UWIERZYTELNIANIE DOMEN

System teleinformatyczny w celu przekazania informacji jednoznacznie identyfikuje i uwierzytelnia punkty źródłowe i docelowe według ustalonych w organizacji kryteriów przypisanych do [*Realizacja: Wybór (jeden lub więcej): organizacja, system, aplikacja, osoba*].

Zabezpieczenia powiązane: IA-2, IA-3, IA-4, IA-5.

(18) EGZEKWOWANIE PRZEPŁYWU INFORMACJI | POWIĄZANIE ATRYBUTÓW BEZPIECZEŃSTWA

System teleinformatyczny w celu ułatwienia egzekwowania polityki przepływu informacji wiąże atrybuty bezpieczeństwa z informacjami za pomocą [*Realizacja: zasady wiązania zdefiniowane przez organizację*].

Zabezpieczenia powiązane: AC-16, SC-16.

(19) EGZEKWOWANIE PRZEPŁYWU INFORMACJI | UWIERZYTELNIANIE METADANYCH

System teleinformatyczny, przenosząc informacje między różnymi domenami bezpieczeństwa, stosuje te same zasad bezpieczeństwa filtrowania metadanych, jakie mają zastosowanie do danych właściwych.

(20) EGZEKWOWANIE PRZEPŁYWU INFORMACJI | ZATWIERDZONE ROZWIĄZANIA BEZPIECZEŃSTWA

Organizacja do kontrolowania przepływu informacji [*Realizacja: zdefiniowane przez organizację informacje*] między domenami bezpieczeństwa stosuje rozwiązania określone przez tą organizację w zatwierdzonych konfiguracjach [*Realizacja: rozwiązania zdefiniowane przez organizację w zatwierdzonych konfiguracjach]*.

(21) EGZEKWOWANIE PRZEPŁYWU INFORMACJI | FIZYCZNA LUB LOGICZNA SEPARACJA PRZEPŁYWÓW INFORMACJI

System teleinformatyczny rozdziela przepływy informacji logicznie lub fizycznie przy użyciu [*Realizacja: mechanizmy lub techniki zdefiniowane przez organizację*] w celu [*Realizacja: zdefiniowane przez organizację wymagane rozdzielenie przepływów informacji według rodzajów informacji*].

(22) EGZEKWOWANIE PRZEPŁYWU INFORMACJI |TYLKO DOSTĘP

System teleinformatyczny zapewnia dostęp do platform obliczeniowych, aplikacji lub danych znajdujących się w wielu różnych domenach bezpieczeństwa z jednego urządzenia, zapobiegając jednocześnie przepływowi informacji między różnymi domenami bezpieczeństwa.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	AC-4 (opcjonalnie)	AC-4	AC-4

AC-5 ROZDZIAŁ OBOWIĄZKÓW

Zabezpieczenie:

Organizacja:

a) Wyodrębnia [*Realizacja: obowiązki osób określone w organizacji*];

b) Dokumentuje rozdział zadań osób;

c) Określa uprawnienia dostępu do systemu teleinformatycznego w celu wsparcia podziału zadań.

Zabezpieczenia powiązane: AC-3, AC-6, PE-3, PE-4, PS-2.

Zabezpieczenia rozszerzone: Brak.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	AC-5 (opcjonalnie)	AC-5	AC-5

AC-6 ZASADA WIEDZY KONIECZNEJ

Zabezpieczenie: Organizacja stosuje zasadę wiedzy koniecznej (zasadę najniższych uprawnień), zezwalając jedynie na dostęp autoryzowanych użytkowników (lub procesów działających w imieniu użytkowników), które są niezbędne do wykonania przydzielonych zadań zgodnie z misjami organizacyjnymi i funkcjami biznesowymi.

Zabezpieczenia powiązane: AC-2, AC-3, AC-5, CM-6, CM-7, PL-2.

Zabezpieczenia rozszerzone:

(1) ZASADA WIEDZY KONIECZNEJ | UPOWAŻNIONY DOSTĘP DO FUNKCJI BEZPIECZEŃSTWA

Organizacja zezwala wyłącznie na dostęp do poniższych funkcji bezpieczeństwa[12] [*Realizacja: funkcje bezpieczeństwa zdefiniowane przez organizację (wdrożone w sprzęcie, aplikacjach i oprogramowaniu układowym) oraz informacje dotyczące bezpieczeństwa*[13]].

Zabezpieczenia powiązane: AC-17, AC-18, AC-19.

(2) *ZASADA WIEDZY KONIECZNEJ* | NIEUPRZYWILEJOWANY DOSTĘP DO FUNKCJI NIEZWIĄZANYCH Z BEZPIECZEŃSTWEM

Organizacja wymaga aby użytkownicy kont systemowych lub ról systemu teleinformatycznego, którzy mają dostęp do [*Realizacja: funkcje bezpieczeństwa zdefiniowane przez organizację lub informacje istotne dla bezpieczeństwa*], używali nieuprzywilejowanych kont / ról podczas uzyskiwania dostępu do funkcji niezwiązanych z bezpieczeństwem.

Zabezpieczenia powiązane: PL-4.

[12] Funkcje bezpieczeństwa - np. zakładanie kont systemowych, konfigurowanie autoryzacji dostępu (tj. uprawnień, przywilejów), definiowanie zdarzeń do audytu oraz ustawianie parametrów wykrywania włamań.

[13] Informacje związane z bezpieczeństwem - np. reguły filtrowania routerów / zapór, informacje dotyczące zarządzania kluczami kryptograficznymi, parametry konfiguracji usług bezpieczeństwa oraz listy kontroli dostępu.

(3) ZASADA WIEDZY KONIECZNEJ | DOSTĘP SIECIOWY DO UPRZYWILEJOWANYCH POLECEŃ

Organizacja zezwala na dostęp sieciowy (dostęp zdalny) do [*Realizacja: uprzywilejowane polecenia zdefiniowane przez* organizację] tylko w przypadku *[Realizacja: istotne potrzeby operacyjne zdefiniowane przez organizację*] i dokumentuje uzasadnienie takiego dostępu w planie bezpieczeństwa systemu teleinformatycznego.

Zabezpieczenia powiązane: AC-17.

(4) ZASADA WIEDZY KONIECZNEJ | ODDZIELNE DOMENY PRZETWARZANIA

System teleinformatyczny zapewnia oddzielne domeny przetwarzania, aby umożliwić bardziej szczegółowe przydzielanie uprawnień użytkownika.

Zabezpieczenia powiązane: AC-4, SC-3, SC-30, SC-32.

(5) ZASADA WIEDZY KONIECZNEJ | UPRZYWILEJOWANE KONTA

Organizacja ogranicza przydzielanie kont uprzywilejowanych (administratora systemu) w systemie teleinformatycznym do [*Realizacja: personel lub role zdefiniowane przez organizację*].

Zabezpieczenia powiązane: CM-6.

(6) ZASADA WIEDZY KONIECZNEJ | OGRANICZONY DOSTĘP PRZEZ UŻYTKOWNIKÓW SPOZA ORGANIZACJI

Organizacja zabrania uprzywilejowanego dostępu do systemu teleinformatycznego użytkownikom niebędącym pracownikami (współpracownikami) organizacji.

Zabezpieczenia powiązane: IA-8.

(7) ZASADA WIEDZY KONIECZNEJ | PRZEGLĄD UPRAWNIEŃ UŻYTKOWNIKA

Organizacja:

(a) Przegląda [*Realizacja: częstotliwość zdefiniowana przez organizację*] uprawnienia przypisane do [*Realizacja: role lub klasy użytkowników zdefiniowane przez organizację*] w celu potwierdzenia konieczności posiadania tych uprawnień i dokonuje ich aktualizacji;

(b) W razie potrzeby ponownie nadaje lub odbiera uprawnienia, aby poprawnie odzwierciedlać misję / potrzeby biznesowe organizacji.

Zabezpieczenia powiązane: CA-7.

(8) ZASADA WIEDZY KONIECZNEJ | POZIOMY UPRAWNIEŃ DO URUCHAMIANIA KODU

S**y**stem teleinformatyczny uniemożliwia użytkownikom działania na oprogramowaniu [*Realizacja: oprogramowanie zdefiniowane przez organizację*] na wyższych poziomach uprawnień niż programiści tworzący oprogramowanie (tworzący kod).

(9) ZASADA WIEDZY KONIECZNEJ | KONTROLA WYKORZYSTANIA UPRZYWILEJOWANYCH FUNKCJI

System teleinformatyczny kontroluje wykonywanie funkcji uprzywilejowanych. Rejestracja (logowanie w dziennikach) użycia uprzywilejowanych funkcji jest jednym ze sposobów wykrycia takiego niewłaściwego użycia, a dzięki temu pomaga zminimalizować ryzyko związane z zagrożeniami wewnętrznymi i zagrożeniem atakami zaawansowanymi (z ang. advanced persistent threat - APT[14]).

Zabezpieczenia powiązane: AU- 2.

(10) ZASADA WIEDZY KONIECZNEJ | ODMOWA WYKONYWANIA PRZEZ NIEUPRZYWILEJOWANYCH UŻYTKOWNIKÓW UPRZYWILEJOWANYCH FUNKCJI

System teleinformatyczny uniemożliwia nieuprzywilejowanym użytkownikom [15]wykonywanie uprzywilejowanych funkcji[16], takich jak wyłączanie, obchodzenie lub zmiana zaimplementowanych zabezpieczeń / środków zaradczych.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	AC-6 (opcjonalnie)	AC-6 (1) (2) (5) (9) (10)	AC-6 (1) (2) (5) (9) (10)

AC-7 NIEUDANE PRÓBY LOGOWANIA

Zabezpieczenie: System teleinformatyczny:

a) Wymusza limit [*Realizacja: liczba zdefiniowana przez organizację*] kolejnych nieudanych prób logowania przez użytkownika w okresie [*Realizacja: okres zdefiniowany przez organizację*];

b) Automatycznie [*Realizacja: blokuje konto / węzeł dostępowy na [Realizacja: okres zdefiniowany przez organizację]; blokuje konto / węzeł dostępowy do momentu odblokowania przez administratora; opóźnia udostępnienie znaku zgłoszenia gotowości systemu do kolejnego logowania zgodnie z [Realizacja: algorytm opóźnienia zdefiniowany przez organizację*]], w przypadku przekroczenia maksymalnej liczby nieudanych prób połączeń.

[14] Cyberprzestępcy wybierają sobie na ofiarę jeden konkretny podmiot, np. instytucję lub przedsiębiorstwo. W tym konkretnym podmiocie, po wstępnej inwigilacji, bardzo często wybierają jedną konkretną osobę, która stanie się wektorem ataku i posłuży do tego, by na starannie wyselekcjonowanej ofierze zarobić możliwie jak najwięcej.
[15] Użytkownicy nieuprzywilejowani to osoby, które nie posiadają odpowiednich uprawnień.
[16] Uprzywilejowane funkcje obejmują np. zakładanie kont w systemie teleinformatycznym, przeprowadzanie kontroli integralności systemu lub zarządzanie kluczami kryptograficznymi.

Zabezpieczenia powiązane: AC-2, AC-9, AC-14, IA-5.

Zabezpieczenia rozszerzone:

(1) NIEUDANE PRÓBY LOGOWANIA | AUTOMATYCZNE ZAMKNIĘCIE KONTA

[Włączone do AC-7].

(2) NIEUDANE PRÓBY LOGOWANIA | USUWANIE INFORMACJI Z URZĄDZEŃ PRZENOŚNYCH

System teleinformatyczny usuwa informacje z [*Realizacja: urządzenia przenośne zdefiniowane przez organizację*] na podstawie [*Realizacja: zdefiniowane przez organizację wymagania / techniki dotyczące usuwania informacji*] po [*Realizacja: liczba zdefiniowany przez organizację próbach zalogowania*] kolejnych, nieudanych próbach zalogowania na urządzeniu.

Zabezpieczenia powiązane: AC-19, MP-5, MP-6, SC-13.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P2	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	AC-7	AC-7	AC-7

AC-8 POWIADOMIENIE O ZASADACH UŻYCIA SYSTEMU

Zabezpieczenie: System teleinformatyczny:

a. Przed przyznaniem dostępu do systemu, użytkownikom wyświetlany jest *[Realizacja: zdefiniowany przez organizację komunikat lub baner powiadamiający o użyciu systemu*], który powiadamia o prywatności i bezpieczeństwie (zgodne z obowiązującymi przepisami, zarządzeniami wykonawczymi, dyrektywami, politykami, przepisami, standardami i wytycznymi) oraz informuje, że:

   1. Użytkownicy uzyskują dostęp do systemu teleinformatycznego danej organizacji;
   2. Wykorzystanie systemu teleinformatycznego może być monitorowane, rejestrowane i poddawane audytowi;
   3. Niedozwolone (nieautoryzowane) korzystanie z systemu teleinformatycznego jest zabronione i podlega sankcjom służbowym, karnym lub cywilnym;
   4. Korzystanie z systemu teleinformatycznego oznacza zgodę na monitorowanie i rejestrowanie działań użytkownika;

b. Zachowuje powiadomienie lub baner na ekranie, dopóki użytkownicy nie potwierdzą warunków użytkowania i nie podejmą wyraźnych działań w celu zalogowania się do systemu teleinformatycznego lub uzyskania dalszego dostępu do niego;

c. W przypadku publicznie dostępnych systemów:

   1. Wyświetla informacje o użytkowaniu systemu na warunkach *[Realizacja: warunki zdefiniowane przez organizację*], przed przyznaniem dalszego dostępu;

   2. Wyświetla ewentualne odniesienia informujące o monitorowaniu, rejestrowaniu lub audycie, które są zgodne z zasadami prywatności w takich systemach, a które generalnie zabraniają takich działań;

   3. Zawiera opis dozwolonych zastosowań systemu.

Zabezpieczenia rozszerzone: Brak.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	AC-8	AC-8	AC-8

AC-9 POWIADOMIENIE O ZALOGOWANIU

Zabezpieczenie: System teleinformatyczny powiadamia użytkownika, po udanym zalogowaniu (dostępie) do systemu, o dacie i godzinie ostatniego logowania (dostępu).

Zabezpieczenia powiązane: AC-7, PL-4.

Zabezpieczenia rozszerzone:

(1) POWIADOMIENIE O ZALOGOWANIU | NIEPOPRAWNE LOGOWANIE

System teleinformatyczny informuje użytkownika, po udanym zalogowaniu / dostępie, o liczbie nieudanych prób logowania / dostępu od ostatniego udanego logowania / dostępu.

(2) POWIADOMIENIE O ZALOGOWANIU | POMYŚLNE / NIEUDANE LOGOWANIA

System teleinformatyczny powiadamia użytkownika o liczbie *[Realizacja: udane logowanie / dostęp; nieudane próby logowania / dostępu; oba wybory*] w okresie[*Realizacja: okres zdefiniowany przez organizację*].

(3) POWIADOMIENIE O ZALOGOWANIU | POWIADOMIENIE O ZMIANACH W KONCIE

System teleinformatyczny powiadamia użytkownika o zmianach w logowaniu dotyczących [*Realizacja: charakterystyka / parametry związane z bezpieczeństwem konta zdefiniowane przez organizację*] w czasie [*Realizacja: okres zdefiniowany przez organizację*].

(4) POWIADOMIENIE O ZALOGOWANIU | DODATKOWE INFORMACJE DOTYCZĄCE LOGOWANIA

System teleinformatyczny powiadamia użytkownika, po udanym zalogowaniu (dostępie), o następujących dodatkowych informacjach: *[Realizacja: informacje zdefiniowane przez organizację, które oprócz daty i godziny ostatniego logowania (dostępu) uwzględniają, np. lokalizację ostatniego logowania*].

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P0	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	AC-9 (opcjonalnie)	AC-9 (opcjonalnie wraz z rozszerzonymi zabezpieczeniami)	AC-9 (opcjonalnie wraz z rozszerzonymi zabezpieczeniami)

AC-10 KONTROLA ILOŚCI RÓWNOCZESNYCH SESJI

Zabezpieczenie: system teleinformatyczny ogranicza liczbę równoczesnych sesji dla każdego konta *[Realizacja: konto zdefiniowane przez organizację i / lub typ konta*] do [*Realizacja: ilość równoczesnych sesji zdefiniowana przez organizację*].

Zabezpieczenia rozszerzone: Brak.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P3	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	AC-10 (opcjonalnie)	AC-10 (opcjonalnie)	AC-10

AC-11 ZAMKNIĘCIE / BLOKADA SESJI

Zabezpieczenie: System teleinformatyczny:

a. Zapobiega dalszemu dostępowi do systemu poprzez zainicjowanie zamknięcia / blokady sesji po czasie [*Realizacja: okres zdefiniowany przez organizację*] bezczynności na koncie lub po otrzymaniu żądania blokady / zamknięcia od użytkownika;

b. Utrzymuje zamknięcie / blokadę sesji, dopóki użytkownik nie przywróci dostępu przy użyciu ustanowionych procedur identyfikacji i uwierzytelniania.

Zabezpieczenia powiązane: AC-7.

Zabezpieczenia rozszerzone:

(1) ZAMKNIĘCIE / BLOKADA SESJI | WYGASZACZ EKRANU

Na czas blokady / zamknięcia sesji, , informacje wcześniej widoczne na ekranie zastępowane są wygaszaczem ekranu ukazującym publicznie dostępny obraz.

Zabezpieczenia powiązane: Brak.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P3	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	AC-11 (opcjonalnie)	AC-11 (1)	AC-11 (1)

AC-12 ZAKOŃCZENIE SESJI

Zabezpieczenie: System teleinformatyczny automatycznie kończy sesję użytkownika po [*Realizacja: warunki zdefiniowane przez organizację lub zdarzenia wyzwalające wymagające zakończenia sesji*]. Zabezpieczenie to dotyczy zakończenia sesji logicznych zainicjowanych przez użytkownika, w przeciwieństwie do zabezpieczenia SC-10, które dotyczy zakończenia połączeń sieciowych związanych z sesjami komunikacyjnymi (tj. rozłączeniem sieci).

Zabezpieczenia powiązane: SC-10, SC-23.

Zabezpieczenia rozszerzone:

(1) ZAKOŃCZENIE SESJI | WYLOGOWANIE INICJOWANE PRZEZ UŻYTKOWNIKA / WYŚWIETLANIE KOMUNIKATU WYLOGOWANIA

System teleinformatyczny:

(a) Zapewnia możliwość wylogowania się z sesji komunikacyjnych inicjowanych przez użytkownika, ilekroć uwierzytelnianie jest używane w celu uzyskania dostępu do zasobów [*Realizacja: zasoby informacyjne zdefiniowane przez organizację*];

(b) Wyświetla użytkownikom wyraźny komunikat wylogowania wskazujący wiarygodne zakończenie uwierzytelnionych sesji komunikacyjnych.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P2	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	AC-12 (opcjonalnie)	AC-12	AC-12

AC-13 NADZÓR I PRZEGLĄD – KONTROLA DOSTĘPU

[Włączony do AC-2 i AU-6].

AC-14 DZIAŁANIA DOZWOLONE BEZ IDENTYFIKACJI LUB UWIERZYTELNIANIA

Zabezpieczenie: Organizacja:

a. Określa działania [*Realizacja: działania użytkownika zdefiniowane przez organizację*], które można wykonać w systemie teleinformatycznym bez identyfikacji lub uwierzytelnienia, zgodne z misjami organizacyjnymi / funkcjami biznesowymi;

b. Dokumentuje i uzasadnienia w planie bezpieczeństwa systemu teleinformatycznego działania użytkownika niewymagające identyfikacji ani uwierzytelnienia.

Zabezpieczenia powiązane: CP-2, IA-2.

Zabezpieczenia rozszerzone: Brak.

(1) DZIAŁANIA DOZWOLONE BEZ IDENTYFIKACJI LUB UWIERZYTELNIENIA | NIEZBĘDNE ZASTOSOWANIA

[Włączone do AC-14].

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P3	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	AC-14	AC-14	AC-14

AC-15 ZAUTOMATYZOWANE ZNAKOWANIE

[Włączone do MP-3].

AC-16 ATRYBUTY BEZPIECZEŃSTWA

Zabezpieczenie: Organizacja:

a. Zapewnia środki dołączające atrybutów bezpieczeństwa [*Realizacja: typy atrybutów bezpieczeństwa zdefiniowane przez organizację*] posiadające [*Realizacja: wartości atrybutu bezpieczeństwa zdefiniowane przez organizacj*ę] do przetwarzanych (przechowywanych, opracowywanych i / lub przesyłanych) informacji;

b. Zapewnia, że powiązania atrybutów bezpieczeństwa są tworzone i przypisane do informacji, których dotyczą;

c. Ustanawia dozwolone atrybuty bezpieczeństwa [*Realizacja: atrybuty bezpieczeństwa zdefiniowane przez organizację*] w odniesieniu do [*Realizacja: systemy informacyjne zdefiniowane przez organizację*];

d. Określa dozwolone [*Realizacja: wartości lub zakresy zdefiniowane przez organizację*] dla każdego z ustalonych atrybutów bezpieczeństwa.

Zabezpieczenia powiązane: AC-3, AC-4, AC-6, AC-21, AU-2, AU-10, SC-16, MP-3.

Zabezpieczenia rozszerzone:

(1) ATRYBUTY BEZPIECZEŃSTWA | DYNAMICZNE KOJARZENIE ATRYBUTÓW

System teleinformatyczny, podczas tworzenia i łączenia informacji, dynamicznie kojarzy atrybuty bezpieczeństwa z [*Realizacja: podmioty i obiekty zdefiniowane przez organizację*] zgodnie z *[Realizacja: zasady bezpieczeństwa zdefiniowane przez organizację*] .

Zabezpieczenia powiązane: AC-4.

(2) ATRYBUTY BEZPIECZEŃSTWA | ZMIANA WARTOŚCI ATRYBUTÓW PRZEZ UPOWAŻNIONE OSOBY

System teleinformatyczny zapewnia upoważnionym osobom (lub procesom działającym w imieniu osób fizycznych) możliwość zdefiniowania lub zmiany wartości powiązanych atrybutów bezpieczeństwa.

Zabezpieczenia powiązane: AC-6, AU-2.

(3) ATRYBUTY BEZPIECZEŃSTWA | UTRZYMANIE KOJARZENIA ATRYBUTÓW PRZEZ SYSTEM TELEINFORMATYCZNY

System teleinformatyczny utrzymuje kojarzenie i integralność [*Realizacja: atrybuty bezpieczeństwa zdefiniowane przez organizację*] do / z [*Realizacja: podmioty i obiekty zdefiniowane przez organizację*].

(4) ATRYBUTY BEZPIECZEŃSTWA | KOJARZENIE ATRYBUTÓW PRZEZ AUTORYZOWANY PERSONEL

System teleinformatyczny obsługuje łączenie przez upoważnione osoby (lub procesy działające w imieniu osób fizycznych) zdefiniowane przez organizację [*Realizacja: atrybuty bezpieczeństwa zdefiniowane przez organizację*] z [*Realizacja: podmioty i obiekty zdefiniowane przez organizację*].

(5) ATRYBUTY BEZPIECZEŃSTWA | ATRYBUTY BEZPIECZEŃSTWA PREZENTOWANE NA WYŚWIETLACZACH URZĄDZEŃ WYJŚCIOWYCH

System teleinformatyczny wyświetla, w postaci czytelnej dla użytkownika, atrybuty bezpieczeństwa każdego obiektu, które dany system przesyła do urządzeń wyjściowych w celu identyfikacji [*Realizacja: specjalne instrukcje rozpowszechniania, obchodzenia się lub dystrybucji określone przez organizację*] przy użyciu [*Realizacja: organizacyjne zidentyfikowany czytelny dla człowieka standard określony umowami*].

(6) ATRYBUTY BEZPIECZEŃSTWA | ZARZĄDZANIE POWIĄZANYMI ATRYBUTAMI BEZPIECZEŃSTWA

Organizacja umożliwia personelowi powiązanie i zarządzanie powiązaniem [*Realizacja: atrybuty zabezpieczeń zdefiniowane przez organizację*] z [*Realizacja: podmioty i obiekty zdefiniowane przez organizację*] zgodnie z [*Realizacja: zasady bezpieczeństwa zdefiniowane przez organizację*].

(7) ATRYBUTY BEZPIECZEŃSTWA | INTERPRETACJA WSPÓLNYCH ATRYBUTÓW BEZPIECZEŃSTWA

Organizacja zapewnia spójną interpretację atrybutów bezpieczeństwa przesyłanych między komponentami rozproszonego systemu teleinformatycznego.

(8) ATRYBUTY BEZPIECZEŃSTWA | POWIĄZANIE TECHNIKI / TECHNOLOGII Z ATRYBUTAMI BEZPIECZEŃSTWA

System teleinformatyczny wdraża *[Realizacja: techniki lub technologie zdefiniowane przez organizację*] z [*Realizacja: poziom zaufania zdefiniowany przez organizację*] skojarzone z atrybutami bezpieczeństwa informacji, wiążąc atrybuty bezpieczeństwa z informacjami przetwarzanymi w systemach teleinformatycznych.

(9) ATRYBUTY BEZPIECZEŃSTWA | PONOWNY PRZYDZIAŁ ATRYBUTU BEZPIECZEŃSTWA

Organizacja zapewnia, że atrybuty bezpieczeństwa związane z informacjami są ponownie przypisywane tylko za pomocą wiarygodnych mechanizmów ponownej oceny (przeklasyfikowania), sprawdzonych przy użyciu [*Realizacja: techniki lub procedury zdefiniowane przez organizację*].

(10) ATRYBUTY BEZPIECZEŃSTWA | KONFIGURACJA ATRYBUTÓW BEZPIECZEŃSTWA PRZEZ UPOWAŻNIONE OSOBY

System teleinformatyczny zapewnia uprawnionym osobom możliwość definiowania lub zmiany rodzaju i wartości atrybutów bezpieczeństwa dostępnych do powiązania z podmiotami i obiektami.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P0	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	AC-16 (opcjonalnie)	AC-16 (opcjonalnie)	AC-16 (opcjonalnie)

AC-17 ZDALNY DOSTĘP

Zabezpieczenie: Organizacja:

a. Ustanawia i dokumentuje ograniczenia użytkowania systemu teleinformatycznego, wymagania dotyczące konfiguracji / połączenia oraz wytyczne dotyczące wdrażania dla każdego rodzaju dozwolonego dostępu zdalnego;

b. Autoryzuje zdalny dostęp do systemu teleinformatycznego przed zezwoleniem na dokonanie połączenia.

Zabezpieczenia powiązane: AC-2, AC-3, AC-18, AC-19, AC-20, CA-3, CA-7, CM-8, IA-2, IA-3, IA-8, MA-4 , PE-17, PL-4, SC-10, SI-4.

Zabezpieczenia rozszerzone:

(1) ZDALNY DOSTĘP | AUTOMATYCZNE MONITOROWANIE | KONTROLA

System teleinformatyczny monitoruje i kontroluje metody dostępu zdalnego.

Zabezpieczenia powiązane: AU-2, AU-12.

(2) ZDALNY DOSTĘP | OCHRONA POUFNOŚCI / INTEGRALNOŚCI Z WYKORZYSTANIEM SZYFROWANIA

System teleinformatyczny wdraża mechanizmy kryptograficzne w celu ochrony poufności i integralności sesji dostępu zdalnego.

(3) ZDALNY DOSTĘP | ZARZĄDZANIE PUNKTAMI KONTROLI DOSTĘPU

System teleinformatyczny steruje wszystkimi zdalnymi dostępami przez zarządzane punkty kontroli dostępu do sieci [*Realizacja: liczba punktów kontroli dostępu zdalnego zdefiniowana przez organizację*].

Zabezpieczenia powiązane: SC-7.

(4) ZDALNY DOSTĘP | POLECENIA UPRZYWILEJOWANE / DOSTĘP

Organizacja:

(a) zezwala na wykonywanie uprzywilejowanych poleceń i dostęp do istotnych z punktu widzenia bezpieczeństwa informacji za pośrednictwem zdalnego dostępu tylko w przypadku [*Realizacja: potrzeby zdefiniowane przez organizację*];

(b) Dokumentuje uzasadnienie takiego dostępu w planie bezpieczeństwa systemu teleinformatycznego.

Zabezpieczenia powiązane: AC-6.

(5) ZDALNY DOSTĘP | MONITOROWANIE NIEAUTORYZOWANYCH POŁĄCZEŃ

[Włączono do SI-4].

(6) ZDALNY DOSTĘP | OCHRONA MECHANIZMÓW ZDALNEGO DOSTĘPU

Organizacja zapewnia, że informacje o stosowanych mechanizmach zdalnego dostępu przed nieuprawnionym użyciem i ujawnieniem są chronione przez użytkowników.

Zabezpieczenia powiązane: AT-2, AT-3, PS-6.

(7) ZDALNY DOSTĘP | DODATKOWA OCHRONA DOSTĘPU DO FUNKCJI BEZPIECZEŃSTWA

[Włączono do AC-3 (10)].

(8) ZDALNY DOSTĘP | DEZAKTYWACJA NIEZABEZPIECZONYCH PROTOKOŁÓW SIECIOWYCH

[Włączone do CM-7].

(9) ZDALNY DOSTĘP | WYŁĄCZANIE / DEZAKTYWACJA DOSTĘPU

Organizacja zapewnia możliwość szybkiego wyłączenia lub dezaktywacji zdalnego dostępu do systemu teleinformatycznego w ciągu [*Realizacja: okres zdefiniowany przez organizację*].

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	AC-17	AC-17 (1) (2) (3) (4)	AC-17 (1) (2) (3) (4)

AC-18 DOSTĘP BEZPRZEWODOWY

Zabezpieczenie: Organizacja:

a. Ustanawia ograniczenia użytkowania, wymagania dotyczące konfiguracji / połączenia oraz wytyczne dotyczące implementacji dostępu bezprzewodowego;

b. Autoryzuje bezprzewodowy dostęp do systemu teleinformatycznego przed zezwoleniem na zestawienie takiego połączenia.

Zabezpieczenia rozszerzone:

(1) DOSTĘP BEZPRZEWODOWY | UWIERZYTELNIANIE I SZYFROWANIE

System teleinformatyczny chroni bezprzewodowy dostęp do systemu za pomocą uwierzytelnienia [*Realizacja (jeden lub więcej): użytkowników; urządzenia*] i szyfrowania.

Zabezpieczenia powiązane: SC-8, SC-13.

(2) DOSTĘP BEZPRZEWODOWY | MONITOROWANIE POŁĄCZEŃ NIEAUTORYZOWANYCH

[Włączono do SI-4].

(3) DOSTĘP BEZPRZEWODOWY | DEZAKTYWACJA SIECI BEZPRZEWODOWEJ

Organizacja wyłącza (dezaktywuje), przed wydaniem zezwolenia do użycia i wdrożenia, nieprzeznaczone do użytku funkcje sieci bezprzewodowej wbudowane w wewnętrznie komponenty systemu teleinformatycznego.

Zabezpieczenia powiązane: AC-19.

(4) DOSTĘP BEZPRZEWODOWY **|** OGRANICZENIE DOKONYWANIA KONFIGURACJI PRZEZ UŻYTKOWNIKÓW

Organizacja identyfikuje i autoryzuje użytkowników do samodzielnego konfigurowania funkcji sieci bezprzewodowej.

Zabezpieczenia powiązane: AC-3, SC-15.

(5) DOSTĘP BEZPRZEWODOWY | POZIOMY MOCY ANTEN / TRANSMISJI

Organizacja wybiera anteny radiowe i kalibruje poziomy mocy transmisji elementów nadawczych urządzeń, w celu zmniejszenia prawdopodobieństwa odbierania sygnałów radiowych poza granicami przestrzeni kontrolowanej przez organizację.

Zabezpieczenia powiązane: PE-19.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	AC-18	AC-18 (1)	AC-18 (1) (4) (5)

AC-19 KONTROLA DOSTĘPU REALIZOWANEGO Z URZĄDZEŃ PRZENOŚNYCH (MOBILNYCH)

Zabezpieczenie: Organizacja:

a. Ustanawia ograniczenia użytkowania, wymagania dotyczące konfiguracji, wymagania dotyczące połączenia oraz wskazówki dotyczące realizacji dostępu do systemu informacyjnego z urządzeń przenośnych (mobilnych) kontrolowanych przez organizację;

b. Autoryzuje połączenie urządzeń mobilnych z systemami teleinformatycznymi organizacji.

Zabezpieczenia powiązane: AC-3, AC-7, AC-18, AC-20, CA-9, CM-2, IA-2, IA-3, MP-2, MP-4, MP-5, PL-4 , SC-7, SC-43, SI-3, SI-4.

Zabezpieczenia rozszerzone:

(1) KONTROLA DOSTĘPU REALIZOWANEGO Z URZĄDZEŃ PRZENOŚNYCH | KORZYSTANIE Z ZAPISYWALNYCH / PRZENOŚNYCH URZĄDZEŃ MAGAZYNUJĄCYCH

[Włączone do MP-7].

(2) KONTROLA DOSTĘPU REALIZOWANEGO Z URZĄDZEŃ PRZENOŚNYCH | WYKORZYSTANIE OSOBISTYCH PRZENOŚNYCH URZĄDZEŃ MAGAZYNUJĄCYCH

[Włączono do MP-7].

(3) KONTROLA DOSTĘPU REALIZOWANEGO Z URZĄDZEŃ PRZENOŚNYCH | WYKORZYSTANIE OGÓLNODOSTĘPNYCH PRZENOŚNYCH URZĄDZEŃ MAGAZYNUJĄCYCH

[Włączone do MP-7].

(4) KONTROLA DOSTĘPU REALIZOWANEGO Z URZĄDZEŃ PRZENOŚNYCH **|** OGRANICZENIA DOTYCZĄCE INFORMACJI NIEJAWNYCH[17]

(5) KONTROLA DOSTĘPU REALIZOWANEGO Z URZĄDZEŃ PRZENOŚNYCH | SZYFROWANIE ZAWARTOŚCI CAŁEGO URZĄDZENIA / WYBRANYCH ZASOBÓW URZĄDZENIA

Organizacja stosuje [*Realizacja: szyfrowanie zawartości całego urządzenia; szyfrowanie zawartości kontenerów*] w celu ochrony poufności i integralności informacji w [*Realizacja: urządzenia mobilne zdefiniowane przez organizację*].

Zabezpieczenia powiązane: MP-5, SC-13, SC-28.

Zabezpieczenia powiązane: Brak.

[17] Realizowane zgodnie z przepisami ustawy o ochronie informacji niejawnych.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	AC-19	AC-19 (5)	AC-19 (5)

AC-20 WYKORZYSTANIE ZEWNĘTRZNYCH SYSTEMÓW TELEINFORMATYCZNYCH

Zabezpieczenie: Organizacja ustanawia warunki, zgodne z relacjami zaufania wdrożonymi z innymi organizacjami posiadającymi, działającymi i / lub utrzymującymi zewnętrzne systemy teleinformacyjne, umożliwiając upoważnionym osobom:

a. Dostęp do systemu teleinformatycznego z zewnętrznych systemów teleinformatycznych;

b. Przetwarzanie, przechowywanie i przesyłanie informacji kontrolowanych przez organizację za pomocą zewnętrznych systemów teleinformatycznych.

Zabezpieczenia powiązane: AC-3, AC-17, AC-19, CA-3, PL-4, SA-9.

Zabezpieczenia rozszerzone:

(1) WYKORZYSTANIE ZEWNĘTRZNYCH SYSTEMÓW TELEINFORMATYCZNYCH | OGRANICZENIA AUTORYZOWANEGO DOSTĘPU

Organizacja zezwala upoważnionym osobom na korzystanie z zewnętrznego systemu teleinformatycznego w celu uzyskania dostępu do systemu teleinformatycznego organizacji i przetwarzania, przechowywania lub przekazywania informacji kontrolowanych przez organizację tylko wtedy, gdy organizacja:

(a) Weryfikuje wdrożenie wymaganych środków bezpieczeństwa (zabezpieczeń) w systemie zewnętrznym, określonych w polityce bezpieczeństwa informacji i planie bezpieczeństwa organizacji;

(b) Posiada umowy o połączeniu systemów teleinformatycznych lub przetwarzaniu informacji w tych systemach teleinformatycznych z jednostką organizacyjną obsługującą zewnętrzny system teleinformatyczny.

Zabezpieczenia powiązane: CA-2.

(2) WYKORZYSTANIE ZEWNĘTRZNYCH SYSTEMÓW TELEINFORMATYCZNYCH | PRZENOŚNE URZĄDZENIA MAGAZYNUJĄCE

Organizacja [*Realizacja: ogranicza; zabrania*] używania przez upoważnione osoby, kontrolowanych przez organizację przenośnych urządzeń pamięci masowej (urządzeń magazynujących) w zewnętrznych systemach teleinformatycznych.

(3) WYKORZYSTANIE ZEWNĘTRZNYCH SYSTEMÓW TELEINFORMATYCZNYCH | KOMPONENTY / URZĄDZENIA INNYCH SYSTEMÓW

Organizacja [*Realizacja: ogranicza; zabrania*] wykorzystywania systemów teleinformatycznych, komponentów systemu lub urządzeń niebędących własnością organizacji do przetwarzania, przechowywania lub przekazywania informacji organizacyjnych.

(4) WYKORZYSTANIE ZEWNĘTRZNYCH SYSTEMÓW TELEINFORMATYCZNYCH | SIECIOWE URZĄDZENIA MAGAZYNUJĄCE

Organizacja zabrania używania [*Realizacja: zdefiniowane przez organizację dostępne w sieci urządzenia magazynujące*] w zewnętrznych systemach teleinformatycznych.

Odniesienia Brak

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	AC-20	AC-20 (1) (2)	AC-20 (1) (2)

AC-21 UDOSTĘPNIANIE INFORMACJI

Zabezpieczenie: Organizacja:

a. Umożliwia udostępnianie informacji, pozwalając autoryzowanym użytkownikom na ustalenie, czy autoryzacje dostępu przypisane partnerowi, któremu udostępniane są informacje, są zgodne z ograniczeniami dostępu do informacji do [*Realizacja: okoliczności wymiany informacji zdefiniowane przez organizację, w których wymagane jest zachowanie tajemnicy*];

b. Wykorzystuje [*Realizacja: zdefiniowane przez organizację zautomatyzowane mechanizmy lub procesy ręczne udostępniania informacji*], aby pomóc użytkownikom w podejmowaniu decyzji dotyczących udostępniania / wymiany informacji.

Zabezpieczenia powiązane: AC-3.

Zabezpieczenia rozszerzone:

(1) UDOSTĘPNIANIE INFORMACJI | AUTOMATYCZNE WSPARCIE DECYZJI

System teleinformatyczny egzekwuje decyzje dotyczące udostępniania informacji przez upoważnionych użytkowników na podstawie autoryzacji dostępu partnerów udostępniających i ograniczeń dostępu do współużytkowanych informacji.

(2) UDOSTĘPNIANIE INFORMACJI | WYSZUKIWANIE I ODZYSKIWANIE INFORMACJI

System teleinformatyczny wdraża usługi wyszukiwania i odzyskiwania informacji, które egzekwują [*Realizacja: ograniczenia udostępniania informacji zdefiniowane przez organizację*].

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P2	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	AC-21 (opcjonalnie)	AC-21	AC-21

AC-22 TREŚCI PUBLICZNIE DOSTĘPNE

Zabezpieczenie: Organizacja:

a. Wyznacza osoby upoważnione do publikowania informacji w publicznie dostępnym systemie teleinformatycznym;

b. Szkoli upoważnione osoby, aby zapewnić, że publicznie dostępne informacje nie zawierają informacji niepublicznych;

c. Dokonuje przeglądu proponowanej do upublicznienia treści informacji przed opublikowaniem w publicznie dostępnym systemie teleinformatycznym, aby zapewnić, że informacje niepubliczne nie zostały udostępnione;

d. Sprawdza upubliczniana treść w publicznie dostępnym systemie teleinformatycznym pod kątem informacji niepublicznych z częstotliwością *[Realizacja: częstotliwość określona przez organizację*] i usuwa takie informacje, jeśli zostaną wykryte.

Zabezpieczenia powiązane: AC-3, AC-4, AT-2, AT-3, AU-13.

Zabezpieczenia rozszerzone: Brak.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P3	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	AC-22	AC-22	AC-22

AC-23 OCHRONA PRZED PRZESZUKIWANIEM DANYCH

Zabezpieczenie: Organizacja stosuje [*Realizacja: zdefiniowane przez organizację techniki zapobiegania i wykrywania inwigilacji danych*] w odniesieniu do [*Realizacja: obiekty przechowywania danych zdefiniowane przez organizację*] w celu odpowiedniego wykrywania i ochrony przed penetracją danych.

Zabezpieczenia rozszerzone: Brak.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P0	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	AC-23 (opcjonalnie)	AC-23 (opcjonalnie)	AC-23 (opcjonalnie)

AC-24 PRZYZNAWANIE PRAW DOSTĘPU

Zabezpieczenie: Organizacja ustanawia procedury w celu zapewnienia, że prawa dostępu są przyznawane zgodnie z [*Realizacja: decyzje kontroli dostępu określone przez organizację*] i są stosowane do każdego żądania dostępu przed potwierdzeniem (udzieleniem) dostępu.

Zabezpieczenia rozszerzone:

(1) PRZYZNAWANIE PRAW DOSTĘPU | PRZESYŁANIE INFORMACJI O AUTORYZACJI DOSTĘPU

System teleinformatyczny przesyła *[Realizacja: informacje o autoryzacji dostępu zdefiniowane przez organizację*] za pomocą [*Realizacja: środki bezpieczeństwa zdefiniowane przez organizację*] do [*Realizacja: systemy informacyjne zdefiniowane przez organizację*], które egzekwują decyzje dotyczące kontroli dostępu.

(2) PRZYZNAWANIE PRAW DOSTĘPU | BRAK TOŻSAMOŚCI UŻYTKOWNIKA LUB PROCESU

System teleinformatyczny egzekwuje decyzje dotyczące kontroli dostępu na podstawie [*Realizacja: atrybuty zabezpieczeń zdefiniowane przez organizację*], które nie posiadają tożsamości użytkownika ani procesu działającego w imieniu użytkownika.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P0	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	AC-24 (opcjonalnie)	AC-24 (opcjonalnie)	AC-24 (opcjonalnie)

AC-25 MONITOROWANIE REFERENCYJNE

Zabezpieczenie: System teleinformatyczny wdraża monitor referencyjny dla [*Realizacja: zdefiniowane przez organizację zasady kontroli dostępu*], który jest odporny na manipulacje, zawsze wywoływany i „mało waży" (aby zapewnić kompletność analizy i testów).

Zabezpieczenia powiązane: AC-3, AC-16, SC-3, SC-39.

Zabezpieczenia rozszerzone: Brak.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P0	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	AC-25 (opcjonalnie)	AC-25 (opcjonalnie)	AC-25 (opcjonalnie)

KATEGORIA: UŚWIADAMIANIE I SZKOLENIA

AT-1 ŚWIADOMOŚĆ BEZPIECZEŃSTWA, POLITYKA I PROCEDURY SZKOLENIOWE

Zabezpieczenie: Organizacja:

a. Opracowuje, dokumentuje i rozpowszechnia w odniesieniu do [*Realizacja: personel lub role zdefiniowane przez organizację*]:

   1. Świadomość bezpieczeństwa i politykę szkoleniową uwzględniającą cel, zakres, role, obowiązki, zaangażowanie kierownictwa, koordynację między jednostkami organizacyjnymi oraz ich podatności;

   2. Procedury ułatwiające wdrażanie polityki w zakresie świadomości bezpieczeństwa i szkoleń oraz związane z tym środki w zakresie bezpieczeństwa i szkolenia;

b. Recenzuje i aktualizuje:

   1. Politykę uświadamiania i szkolenia w zakresie bezpieczeństwa z częstotliwością [*Realizacja: częstotliwość określona przez organizację*];

   2. Procedury uświadamiania szkolenia w zakresie bezpieczeństwa z częstotliwością [*Realizacja: częstotliwość określona przez organizację*].

Zabezpieczenia powiązane: PM-9.

Zabezpieczenia rozszerzone: Brak.

Zabezpieczenia powiązane: Brak.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	AT-1	AT-1	AT-1

AT-2 SZKOLENIE W ZAKRESIE UŚWIADAMIANIA BEZPIECZEŃSTWA

Zabezpieczenie: Organizacja zapewnia podstawowe szkolenie w zakresie uświadamiania bezpieczeństwa użytkownikom systemów teleinformatycznych (w tym menedżerom, wyższemu kierownictwu i kontrahentom):

a. W ramach wstępnego szkolenia dla nowych użytkowników systemów;

b. Gdy wymagają tego zmiany wprowadzane w systemie teleinformatycznym;

c. Okresowo, co najmniej z częstotliwością [*Realizacja: częstotliwość określona przez organizację]* w okresie działalności organizacji.

Zabezpieczenia powiązane: AT-3, AT-4, PL-4.

Zabezpieczenia rozszerzone:

(1) SZKOLENIE W ZAKRESIE UŚWIADAMIANIA BEZPIECZEŃSTWA | ĆWICZENIA PRAKTYCZNE

Organizacja przeprowadza praktyczne ćwiczenia w szkoleniu uświadamiającym w zakresie bezpieczeństwa, które symulują faktyczne cyberataki.

Zabezpieczenia powiązane: CA-2, CA-7, CP-4, IR-3.

(2) SZKOLENIE W ZAKRESIE UŚWIADAMIANIA BEZPIECZEŃSTWA | ZAGROŻENIE WEWNĘTRZNE

Organizacja przeprowadza szkolenie uświadamiające w zakresie bezpieczeństwa dotyczące rozpoznawania i zgłaszania potencjalnych kierunków zagrożenia wewnętrznego.

Zabezpieczenia powiązane: PL-4, PM-12, PS-3, PS-6.

Zabezpieczenia powiązane: Brak

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	AT-2	AT-2 (2)	AT-2 (2)

AT-3 SZKOLENIE W ZAKRESIE BEZPIECZEŃSTWA OPARTEGO NA ROLACH

Zabezpieczenie: Organizacja zapewnia szkolenia w zakresie bezpieczeństwa opartego na rolach dla personelu z przypisanymi rolami i obowiązkami w zakresie bezpieczeństwa:

a. Przed udzieleniem zezwolenia na dostęp do systemu teleinformatycznego lub wykonaniem przydzielonych obowiązków;

b. Gdy wymagają tego zmiany systemu teleinformatycznego;

c. Okresowo, co najmniej z częstotliwością[*Realizacja: częstotliwość określona przez organizację]* w okresie działalności organizacji.

Zabezpieczenia powiązane: AT-2, AT-4, PL-4, PS-7, SA-3, SA-12, SA-16.

Zabezpieczenia rozszerzone:

(1) SZKOLENIE W ZAKRESIE BEZPIECZEŃSTWA OPARTEGO NA ROLACH | ZABEZPIECZENIA ŚRODOWISKOWE

Organizacja zapewnia pracownikom / współpracownikom *[Realizacja: pracownicy / współpracownicy organizacji lub zdefiniowane role*] z częstotliwością [*Realizacja: częstotliwość organizacja zdefiniowane*] szkolenia w zakresie ustanawiania i funkcjonowania zabezpieczeń środowiskowych[18].

Powiązane zabezpieczenia: PE-1, PE-13, PE-14, PE-15.

(2) SZKOLENIE W ZAKRESIE BEZPIECZEŃSTWA OPARTEGO NA ROLACH | ŚRODKI BEZPIECZEŃSTWA FIZYCZNEGO

Organizacja określa [*Realizacja: personel lub role*] podlegający szkoleniu początkowemu oraz szkoleniu okresowemu w zakresie ustanawiania i eksploatacji fizycznych środków bezpieczeństwa[19] z częstotliwością [*Realizacja: częstotliwość organizacja zdefiniowane*].

Zabezpieczenia powiązane: PE-2, PE-3, PE-4, PE-5.

(3) SZKOLENIE W ZAKRESIE BEZPIECZEŃSTWA OPARTEGO NA ROLACH | ĆWICZENIA PRAKTYCZNE

Organizacja przeprowadza praktyczne ćwiczenia z zakresu bezpieczeństwa, utrwalające nabyta wiedzę teoretyczną.

(4) SZKOLENIE W ZAKRESIE BEZPIECZEŃSTWA OPARTEGO NA ROLACH | PODEJRZANE TRANSMISJE I ANOMALIE ZACHOWANIA SYSTEMU

Organizacja przeprowadza szkolenia na temat [*Realizacja: zdefiniowane przez organizację wskaźniki złośliwego kodu*] w celu rozpoznawania podejrzanej transmisji i nietypowych zachowań w systemach teleinformatycznych organizacji.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	AT-3	AT-3	AT-3

[18] Zabezpieczenia środowiskowe obejmują zainstalowane w obiekcie, np. urządzenia / systemy gaszenia i wykrywania pożaru, systemy zraszaczy, gaśnice ręczne, stałe węże pożarowe, czujniki dymu i temperatury / wilgotności, systemy zasilania, klimatyzacji i chłodzenia.

[19] Fizyczne środki bezpieczeństwa obejmują, np. fizyczne urządzenia kontroli dostępu, fizyczne alarmy włamaniowe, sprzęt do monitorowania / nadzoru oraz pracowników ochrony (procedury rozmieszczania i obsługi).

AT-4 REJESTROWANIE SZKOLEŃ Z ZAKRESU BEZPIECZEŃSTWA

Zabezpieczenie: Organizacja:

a. Dokumentuje i monitoruje indywidualne działania szkoleniowe w zakresie bezpieczeństwa systemu teleinformatycznego, w tym podstawowe szkolenia uświadamiające w zakresie bezpieczeństwa i szczegółowe szkolenia w zakresie bezpieczeństwa systemu teleinformatycznego;

b. Przechowuje indywidualne rekordy szkolenia przez okres [*Realizacja: okres zdefiniowany przez organizację*].

Zabezpieczenia powiązane: AT-2, AT-3, PM-14.

Zabezpieczenia rozszerzone: Brak.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P3	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	AT-4	AT-4	AT-4

AT-5 UTRZYMYWANIE KONTAKTÓW Z ZESPOŁAMI I STOWARZYSZENIAMI SPECJALIZUJĄCYMI SIĘ W CYBERBEZPIECZEŃSTWIE

[Włączony do PM-15].

KATEGORIA: AUDYT I ROZLICZALNOŚĆ

AU-1 POLITYKA ORAZ PROCEDURY W ZAKRESIE AUDYTU I ROZLICZALNOŚCI

Zabezpieczenie: Organizacja:

a. Opracowuje, dokumentuje i rozpowszechnia w odniesieniu do [*Realizacja: personel lub role zdefiniowane przez organizację*]:

   1. Politykę audytu i rozliczalności, która dotyczy celu, zakresu, ról, obowiązków, zaangażowania kierownictwa, koordynacji między jednostkami organizacyjnymi oraz ich podatności;

   2. Procedury ułatwiające wdrażanie polityki audytu i rozliczalności oraz powiązane audyty i zabezpieczenia rozliczalności;

b. Recenzuje i aktualizuje aktualne:

   1. Polityki audytu i rozliczalności z częstotliwością [*Realizacja: częstotliwość określona przez organizację*];

   2. Procedury audytu i rozliczalności z częstotliwością [Realizacja: częstotliwość określona przez organizację].

Zabezpieczenia powiązane: PM-9.

Zabezpieczenia rozszerzone: Brak.

Zabezpieczenia powiązane: Brak.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	AU-1	AU-1	AU-1

AU-2 AUDYT ZDARZEŃ

Zabezpieczenie: Organizacja:

a. Określa następujące zdarzenia kontrolowane w systemie teleinformatycznym: [*Realizacja: zdarzenia kontrolowane zdefiniowane przez organizację*];

b. Koordynuje funkcje audytu bezpieczeństwa z innymi jednostkami organizacyjnymi żądającymi pozyskania informacji związanych z audytem, aby zwiększyć wzajemne wsparcie i pomóc w wyborze właściwego audytu;

c. Uzasadnia konieczność przeprowadzania audytu zdarzeń celem wsparcia postępowania wyjaśniającego prowadzonego po fakcie wystąpienia zdarzenia naruszającego bezpieczeństwo;

d. Ustala, że następujące zdarzenia mają być audytowane w systemie teleinformatycznym: [*Realizacja: zdarzenia kontrolowane zdefiniowane przez organizację (podzbiór zdarzeń kontrolowanych zdefiniowany w katalogu AU-2 podkatalog a.) z częstotliwością (lub wymaganą sytuacją) audytu dla każdego zidentyfikowanego zdarzenia*].

Zabezpieczenia powiązane: AC-6, AC-17, AU-3, AU-12, MA-4, MP-2, MP-4, SI-4.

Zabezpieczenia rozszerzone:

(1) AUDYT ZDARZEŃ | KOMPILACJA ZAPISÓW AUDYTU Z WIELU ŹRÓDEŁ

[Włączone do AU-12].

(2) AUDYT ZDARZEŃ | WYBÓR WYDARZEŃ AUDYTOWYCH WEDŁUG KOMPONENTÓW

[Włączono do AU-12].

(3) AUDYT ZDARZEŃ | OPINIE I AKTUALIZACJE

Organizacja przegląda i aktualizuje kontrolowane zdarzenia z częstotliwością [*Realizacja: częstotliwość zdefiniowana przez organizację*].

(4) AUDYT ZDARZEŃ | UPRZYWILEJOWANE FUNKCJE

[Włączone do AC-6 (9)].

Zabezpieczenia powiązane: Brak.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	AU-2	AU-2 (3)	AU-2 (3)

AU-3 ZAWARTOŚĆ REJESTRÓW AUDYTU

Zabezpieczenie: System teleinformatyczny generuje rekordy monitoringu zawierające informacje, które określają, jaki rodzaj zdarzenia miał miejsce, kiedy zdarzenie miało miejsce, gdzie zdarzenie miało miejsce, źródło zdarzenia, wynik zdarzenia oraz tożsamość osób lub podmiotów powiązanych ze zdarzeniem.

Zabezpieczenia powiązane: AU-2, AU-8, AU-12, SI-11.

Zabezpieczenia rozszerzone:

(1) ZAWARTOŚĆ REJESTRÓW AUDYTU | DODATKOWE INFORMACJE KONTROLNE

System teleinformatyczny generuje rekordy monitoringu zawierające następujące dodatkowe informacje: [*Realizacja: dodatkowe, bardziej szczegółowe zdefiniowane przez organizację*].

(2) ZAWARTOŚĆ REJESTRÓW AUDYTU | CENTRALNE ZARZĄDZANIE TREŚCIĄ PLANOWANEGO REJESTRU AUDYTU

System teleinformatyczny zapewnia scentralizowane zarządzanie i konfigurację treści, które mają być zawarte w rekordach monitoringu generowanych przez [*Realizacja: elementy systemu teleinformatycznego zdefiniowane przez organizację*].

Zabezpieczenia powiązane: AU- 6, AU-7.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	AU-3	AU-3 (1)	AU-3 (1) (2)

AU-4 POJEMNOŚĆ PAMIĘCI ZAPISÓW AUDYTU

Zabezpieczenie: Celem zmniejszenia prawdopodobieństwa potencjalnej utraty lub ograniczenia możliwości audytu, organizacja przydziela wystarczający obszar (pojemność) pamięci do przechowywania rekordów audytu zgodnie z [*Realizacja: wymagania dotyczące przechowywania rekordów audytu zdefiniowane przez organizację*].

Zabezpieczenia powiązane: AU-2, AU-5, AU-6, AU-7, AU-11, SI-4.

Zabezpieczenia rozszerzone:

(1) POJEMNOŚĆ PAMIĘCI ZAPISÓW AUDYTU | TRANSFER REKORDÓW DO ALTERNATYWNYCH URZĄDZEŃ MAGAZYNUJĄCYCH

System teleinformatyczny przekazuje rekordy audytu z częstotliwością [*Realizacja: częstotliwość zdefiniowana przez organizację*] do innego systemu lub nośnika niż nadzorowany system.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	AU-4	AU-4	AU-4

AU-5 REAKCJA NA BŁĘDY PROCESÓW AUDYTU

Zabezpieczenie: System teleinformatyczny:

a. Powiadamia [*Realizacja: personel lub role zdefiniowane przez organizację*] w przypadku niewykonywania procesów audytu;

b. Podejmuje następujące dodatkowe działania: [*Realizacja: działania zdefiniowane przez organizację, które należy podjąć (np. zamknąć system teleinformatyczny, zastąpić najstarsze rekordy audytu, przestać generować rekordy audytu)*].

Zabezpieczenia powiązane: AU-4, SI-12.

Zabezpieczenia rozszerzone:

(1) REAKCJA NA BŁĘDY PROCESÓW AUDYTU | PAMIĘĆ PRZECHOWYWANIA REKORDÓW AUDYTU

System teleinformatyczny wyświetla ostrzeżenie dla [*Realizacja: personel, role i / lub lokalizacje zdefiniowane przez organizację*] w ciągu [*Realizacja: okres zdefiniowany przez organizację)*], gdy przydzielona ilość pamięci rekordów kontroli osiągnie [*Realizacja: określony procent pojemności zdefiniowany przez organizację*] maksimum z przydzielonej pojemności do zapisu danych audytu.

(2) REAKCJA NA BŁĘDY PROCESÓW AUDYTU | ALERTY CZASU RZECZYWISTEGO

System teleinformatyczny wyświetla alert w [*Realizacja: okres czasu zdefiniowany przez organizację*] informujący [*Realizacja: personel zdefiniowany przez organizację, role i / lub lokalizacje*], gdy wystąpią następujące zdarzenia niepowodzenia audytu: [*Realizacja: błąd audytu zdefiniowany przez organizację wymagający alertów w czasie rzeczywistym*].

(3) REAKCJA NA BŁĘDY PROCESÓW AUDYTU | KONFIGUROWALNE PROGI NATĘŻENIA RUCHU

System teleinformatyczny wymusza konfigurowalne progi natężenia ruchu w komunikacji sieciowej, odzwierciedlające ograniczenia możliwości audytowanego systemu i [*Realizacja: odrzuca; opóźnienia*] ruch sieciowy powyżej tych progów.

(4) REAKCJA NA BŁĘDY PROCESÓW AUDYTU | WYŁĄCZENIE W PRZYPADKU AWARII

System teleinformatyczny wywołuje opcję [*Realizacja: pełne zamknięcie systemu; częściowe zamknięcie systemu; awaryjny tryb operacyjny z ograniczoną dostępną funkcją misji / działalności biznesowej*] w przypadku [*Realizacja: niepowodzenia audytu zdefiniowanego przez organizację*], chyba że istnieje alternatywna możliwość prowadzenia audytu.

Zabezpieczenia powiązane: AU-15.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	AU-5	AU-5	AU-5 (1) (2)

AU-6 PRZEGLĄD AUDYTU, ANALIZA I RAPORTOWANIE

Zabezpieczenie: Organizacja:

a. Przegląda i analizuje zapisy audytu systemu teleinformatycznego z częstotliwością [*Realizacja: częstotliwość zdefiniowana przez organizację*] pod kątem wskazania [*Realizacja: zdefiniowane przez organizację nieodpowiednie lub nietypowe działania*];

b. Raportuje wyniki audytu do [*Realizacja: personel lub role zdefiniowane przez organizację*].

Zabezpieczenia powiązane: AC-2, AC-3, AC-6, AC-17, AT-3, AU-7, AU-16, CA-7, CM-5, CM-10, CM-11, IA-3 , IA-5, IR-5, IR-6, MA-4, MP-4, PE-3, PE-6, PE-14, PE-16, RA-5, SC-7, SC-18, SC -19, SI-3, SI-4, SI-7.

Zabezpieczenia rozszerzone:

(1) PRZEGLĄD AUDYTU, ANALIZA I RAPORTOWANIE | INTEGRACJA PROCESU

Organizacja stosuje zautomatyzowane mechanizmy do zintegrowania procesów przeglądu, analizy i raportowania wspierania procesów organizacyjnych celem wykrywania i reagowania na podejrzane działania.

Zabezpieczenia powiązane: AU-12, PM-7.

(2) PRZEGLĄD AUDYTU, ANALIZA I RAPORTOWANIE | AUTOMATYCZNE ALARMY BEZPIECZEŃSTWA

[Włączone do SI-4].

(3) PRZEGLĄD AUDYTU, ANALIZA I RAPORTOWANIE | KORELACJA ZBIORÓW AUDYTU

Organizacja analizuje i koreluje (powiązuje ze sobą) zapisy z kontroli w różnych zbiorach (składach) audytu w celu uzyskania szerokiej świadomości sytuacyjnej w całej organizacji.

Zabezpieczenia powiązane: AU-12, IR-4.

(4) PRZEGLĄD AUDYTU, ANALIZA I RAPORTOWANIE | CENTRALNE PRZEGLĄDANIE I ANALIZY

System teleinformatyczny umożliwia centralne przeglądanie i analizowanie zapisów audytu z wielu komponentów systemu.

Zabezpieczenia powiązane: AU-2, AU-12.

(5) PRZEGLĄD AUDYTU, ANALIZA I RAPORTOWANIE | MOŻLIWOŚCI INTEGRACJI / SKANOWANIA I MONITOROWANIA

Organizacja integruje analizę zapisów audytu z analizą [*Wybór (jednego lub więcej): informacji o skanowaniu podatności; dane o wydajności; informacje o monitorowaniu systemu teleinformatycznego; [Realizacja: dane / informacje zdefiniowane przez organizację zebrane z innych źródeł]*] w celu dalszego zwiększania możliwości identyfikowania niewłaściwych lub nietypowych działań.

Zabezpieczenia powiązane: AU-12, IR-4, RA-5.

(6) PRZEGLĄD AUDYTU, ANALIZA I RAPORTOWANIE | KORELACJA AUDYTU Z MONITOROWANIEM FIZYCZNYM

Organizacja koreluje informacje z zapisów audytu z informacjami uzyskanymi z monitorowania fizycznego dostępu w celu dalszego zwiększenia zdolności do identyfikowania podejrzanej, nieodpowiedniej, nietypowej lub szkodliwej działalności.

(7) PRZEGLĄD AUDYTU, ANALIZA I RAPORTOWANIE | DOPUSZCZALNE DZIAŁANIA

Organizacja określa dozwolone działania dla każdego [Realizacja: (w*ybór jednego lub więcej): procesu systemu teleinformatycznego; rola; użytkownik*] związane z przeglądem, analizą i raportowaniem informacji z audytu.

(8) PRZEGLĄD AUDYTU, ANALIZA I RAPORTOWANIE | PEŁNA ANALIZA TEKSTU UPRZYWILEJOWANYCH POLECEŃ

Organizacja przeprowadza pełną analizę tekstową audytowanych uprzywilejowanych poleceń w fizycznie odrębnym komponencie lub podsystemie systemu teleinformatycznego lub innym systemie teleinformatycznym dedykowanym do przeprowadzania tej analizy**.**

Zabezpieczenia powiązane: AU-3, AU-9, AU-11, AU-12.

(9) PRZEGLĄD AUDYTU, ANALIZA I RAPORTOWANIE | KORELACJA Z INFORMACJAMI UZYSKANYMI ZE ŹRÓDEŁ NIETECHNICZNYCH[20]

Organizacja koreluje informacje ze źródeł niedotyczących techniki z informacjami z audytu, w celu zwiększenia świadomości sytuacyjnej w całej organizacji.

Zabezpieczenia powiązane: AT-2.

(10) PRZEGLĄD AUDYTU, ANALIZA I RAPORTOWANIE | KORYGOWANIE POZIOMU AUDYTU

Organizacja dostosowuje (koryguje) poziom przeglądu audytu, analizy i raportowania w systemie teleinformatycznym, w przypadku zmiany poziomu ryzyka oszacowanego na podstawie informacji uzyskanych od organów ścigania, danych wywiadowczych lub innych

[20] Źródła nietechniczne obejmują np. dokumentację dotyczącą zasobów ludzkich, dokumentującą naruszenia zasad organizacyjnych (np. przypadki molestowania seksualnego, niewłaściwe wykorzystanie zasobów informacji organizacyjnych).

wiarygodnych źródeł informacji.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	AU-6	AU-6 (1) (3)	AU-6 (1) (3) (5) (6)

AU-7 REDUKCJA TREŚCI ZAPISÓW AUDYTU I GENEROWANIE RAPORTÓW

Zabezpieczenie: System teleinformatyczny zapewnia możliwość ograniczenia zawartości zapisów audytu i generowania raportów, które:

a. Dostarcza na żądanie przeprowadzenia przeglądu audytu, analizy i sprawozdawczości oraz dochodzenia po fakcie wystąpienia incydentów bezpieczeństwa;

b. Nie zmienia oryginalnej treści ani kolejności uporządkowania rekordów audytu.

Zabezpieczenia powiązane: AU-6.

Zabezpieczenia rozszerzone:

(1) REDUKCJA TREŚCI ZAPISÓW AUDYTU I GENEROWANIE RAPORTÓW | AUTOMATYZACJA PROCESU

System teleinformatyczny umożliwia przetwarzanie rekordów kontroli dotyczących zdarzeń będących przedmiotem zainteresowania[21] na podstawie [*Realizacja: pola kontroli zdefiniowane przez organizację w ramach rekordów kontroli*].

Zabezpieczenia powiązane: AU-2, AU-12.

(2) REDUKCJA TREŚCI ZAPISÓW AUDYTU I GENEROWANIE RAPORTÓW | AUTOMATYCZNE SORTOWANIE I WYSZUKIWANIE

System teleinformatyczny umożliwia sortowanie i wyszukiwanie rekordów audytu pod kątem zdarzeń będących przedmiotem zainteresowania na podstawie treści pól rekordów *audytu [Realizacja: pola kontroli zdefiniowane przez organizację w obrębie rekordów kontroli, na przykład: (i) data / godzina zdarzeń; (ii) identyfikatory użytkowników; (iii) adresy protokołu internetowego (IP) biorące udział w wydarzeniu; (iv) rodzaj zdarzenia; lub (v) sukces / porażka zdarzenia*].

[21] Zdarzenia będące przedmiotem zainteresowania można zidentyfikować na podstawie zawartości konkretnych pól rekordu kontroli, w tym na przykład tożsamości osób, typów zdarzeń, lokalizacji zdarzeń, godzin zdarzeń, dat zdarzeń, zaangażowanych zasobów systemowych, zaangażowanych adresów IP lub obiektów teleinformatycznych do których uzyskano dostęp.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P2	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	AU-7 (opcjonalnie)	AU-7 (1)	AU-7 (1)

AU-8 ZNACZNIKI CZASU

Zabezpieczenie: System teleinformatyczny:

a. Wykorzystuje wewnętrzne zegary systemowe do generowania znaczników czasu dla rekordów audytu;

b. Rejestruje znaczniki czasu dla rekordów audytu, które mogą być odwzorowane do czasu uniwersalnego koordynowanego (UTC) lub czasu uniwersalny Greenwich (GMT) i spełniają [*Realizacja: ziarnistość pomiaru zdefiniowana przez organizację*].

Zabezpieczenia powiązane: AU-3, AU-12.

Zabezpieczenia rozszerzone:

(1) ZNACZNIKI CZASU | SYNCHRONIZACJA Z AUTORYZOWANYM ŹRÓDŁEM CZASU ODNIESIENIA

System teleinformatyczny:

(a) Porównuje zegary wewnętrznego systemu teleinformatycznego z częstotliwością [*Realizacja: częstotliwość określona przez organizację*] z autoryzowanym źródłem czasu odniesienia [*Realizacja: wiarygodne źródło czasu zdefiniowane przez organizację*];

(b) Synchronizuje wewnętrzne zegary systemowe z wiarygodnym źródłem czasu, gdy różnica czasu jest większa niż [*Realizacja: okres zdefiniowany przez organizację*].

(2) ZNACZNIKI CZASU | WTÓRNE ŹRÓDŁO CZASU ODNIESIENIA

System teleinformatyczny identyfikuje wtórne wiarygodne źródło czasu, które znajduje się w innym regionie geograficznym niż główne autoryzowane źródło czasu.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	AU-8	AU-8 (1)	AU-8 (1)

AU-9 OCHRONA INFORMACJI AUDYTOWYCH

Zabezpieczenie: system teleinformatyczny chroni informacje i narzędzia kontroli przed nieautoryzowanym dostępem, modyfikacją i usunięciem.

Zabezpieczenia powiązane: AC-3, AC-6, MP-2, MP-4, PE-2, PE-3, PE-6,

Zabezpieczenia rozszerzone:

(1) OCHRONA INFORMACJI AUDYTOWYCH | NOŚNIKI JEDNOKROTNEGO ZAPISU

System teleinformatyczny zapisuje ścieżki audytu na wprowadzonym do użycia nośniku jednorazowego zapisu.

Zabezpieczenia powiązane: AU-4, AU-5.

(2) OCHRONA INFORMACJI AUDYTOWYCH | BACKUP AUDYTU W ODSEPAROWANYM FIZYCZNIE SYSTEMIE / KOMPONENCIE

System teleinformatyczny tworzy kopię zapasową zapisów audytu z częstotliwością [*Realizacja: częstotliwość zdefiniowana przez organizację*] na innym systemie fizycznym lub innym elemencie systemu niż audytowany system lub komponent.

Zabezpieczenia powiązane: AU-4, AU-5, AU-11.

(3) OCHRONA INFORMACJI AUDYTOWYCH | OCHRONA KRYPTOGRAFICZNA

System teleinformatyczny wdraża mechanizmy kryptograficzne w celu zapewnienia integralności informacji oraz ochrony narzędzi audytu.

Zabezpieczenia powiązane: AU-10, SC-12, SC-13.

(4) OCHRONA INFORMACJI AUDYTOWYCH | DOSTĘP DO PODZBIORU UPRAWNIONYCH UŻYTKOWNIKÓW

Organizacja zezwala na dostęp do zarządzania funkcjami audytu tylko [*Realizacja: zdefiniowany przez organizację podzbiór uprzywilejowanych użytkowników*].

Zabezpieczenia powiązane: AC-5.

(5) OCHRONA INFORMACJI AUDYTOWYCH | PODWÓJNA AUTORYZACJA

Organizacja wymusza podwójną autoryzację[22] dla [*Realizacja: Wybór (jeden lub więcej): [przemieszczanie; usunięcie*] *informacji audytu zdefiniowanej przez organizację*].

Zabezpieczenia powiązane: AC-3, MP-2.

(6) OCHRONA INFORMACJI AUDYTOWYCH | DOSTĘP TYLKO DO ODCZYTU

Organizacja zezwala na dostęp tylko do odczytu do informacji audytu przez [*Realizacja: zdefiniowany przez organizację podzbiór uprzywilejowanych użytkowników*].

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	AU-9	AU-9 (4)	AU-9 (2) (3) (4)

AU-10 NIEZAPRZECZALNOŚĆ

Zabezpieczenie: system teleinformatyczny zabezpiecza przed fałszywym zaprzeczeniem osoby fizycznej (lub procesu działającego w jej imieniu), że wykonała [*Realizacja: działania zdefiniowane przez organizację, które mają być objęte niezaprzeczalnością*[23]].

Zabezpieczenia powiązane: SC-12, SC-8, SC-13, SC-16, SC-17, SC-23.

Zabezpieczenia rozszerzone:

(1) NIEZAPRZECZALNOŚĆ | POŁĄCZENIE TOŻSAMOŚCI

System teleinformatyczny:

(a) Wiąże tożsamość twórcy informacji z informacją z [*Realizacja: siła wiązania zdefiniowana przez organizację*];

(b) Zapewnia upoważnionym osobom środki do ustalenia tożsamości twórcy informacji.

Zabezpieczenia powiązane: AC-4, AC-16.

[22] Mechanizmy podwójnej autoryzacji wymagają zgody dwóch upoważnionych osób w celu dokonania audytu.

[23] Rodzaje indywidualnych działań objętych niezaprzeczalnością obejmują na przykład tworzenie informacji, wysyłanie i odbieranie wiadomości, zatwierdzanie informacji (np. wskazanie zgodności lub podpisanie umowy).

(2) NIEZAPRZECZALNOŚĆ | POWIĄZANIE INFORMACJI Z TOŻSAMOŚCIĄ TWÓRCY

System teleinformatyczny:

(a) Zatwierdza powiązanie tożsamością autora informacji z informacjami z częstotliwością [*Realizacja: częstotliwość określona przez organizację*];

(b) Wykonuje [*Realizacja: działania zdefiniowane przez organizację*] w przypadku błędu sprawdzania poprawności powiązania.

Zabezpieczenia powiązane: AC-3, AC-4, AC-16.

(3) NIEZAPRZECZALNOŚĆ | ŁAŃCUCH NADZORU

System teleinformatyczny utrzymuje tożsamość recenzenta / wydawcy i poświadczenia w ramach ustanowionego łańcucha dowodowego w odniesieniu do wszystkich informacji poddanych przeglądowi lub opublikowaniu.

Zabezpieczenia powiązane: AC-4, AC-16.

(4) NIEZAPRZECZALNOŚĆ | POTWIERDZANIE TOŻSAMOŚCI PRZEGLĄDAJĄCEGO INFORMACJE

System teleinformatyczny:

(a) Sprawdza, czy tożsamość osoby dokonującej przeglądu informacji w punktach wymiany lub udostępniania, powiązana została z tą informacją przed jej udostępnieniem / przekazaniem między [*Realizacja: domeny bezpieczeństwa zdefiniowane przez organizację*];

(b) Wykonuje [*Realizacja: działania zdefiniowane przez organizację*] w przypadku błędu sprawdzenia poprawności.

Zabezpieczenia powiązane: AC-4, AC-16.

(5) NIEZAPRZECZALNOŚĆ | PODPISY CYFROWE

[Włączone do SI-7].

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P2	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	AU-10 (opcjonalnie)	AU—10 (opcjonalnie)	AU-10

AU-11 RETENCJA ZAPISÓW AUDYTU

Zabezpieczenie: Organizacja przechowuje zapisy z audytu przez okres [*Realizacja: okres zdefiniowany przez organizację zgodnie z polityką przechowywania rejestru*] w celu zapewnienia wsparcia procesów dochodzeniowych dotyczących incydentów bezpieczeństwa oraz w celu spełnienia wymagań prawnych i organizacyjnych dotyczących przechowywania informacji.

Zabezpieczenia powiązane: AU-4, AU-5, AU-9, MP-6.

Zabezpieczenia rozszerzone:

(1) RETENCJA ZAPISÓW AUDYTU | DŁUGOTERMINOWA ZDOLNOŚĆ DO ODZYSKU

Organizacja stosuje [*Realizacja: środki zdefiniowane przez organizację*], w celu zapewnienia długoterminowej zdolności systemu teleinformatycznego do odzyskania rekordów audytu wygenerowanych przez system.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P3	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	AU-11	AU-11	AU-11

AU-12 TWORZENIE ZAPISÓW AUDYTU

Zabezpieczenie: System teleinformatyczny:

a. Zapewnia możliwość generowania rekordów audytu zdarzeń podlegających sprawdzeniu zdefiniowanemu w zabezpieczeniu AU-2a. w obszarze [*Realizacja: komponenty systemu teleinformatycznego zdefiniowane przez organizację*];

b. Pozwala [*Realizacja: personel lub role zdefiniowane przez organizację*] na określenie, które zdarzenia podlegające audytowi będą sprawdzane przez określone elementy systemu teleinformatycznego;

c. Generuje rekordy audytu dla zdarzeń zdefiniowanych w zabezpieczeniu AU-2d. o treści zdefiniowanej w kategorii AU-3.

Zabezpieczenia powiązane: AC-3, AU-2, AU-3, AU-6, AU-7.

Zabezpieczenia rozszerzone:

(1) TWORZENIE ZAPISÓW AUDYTU | OGÓLNOSYSTEMOWE / SKORELOWANE W CZASIE ŚCIEŻKI AUDYTU

System teleinformatyczny kompiluje rekordy audytu z [*Realizacja: komponenty systemu teleinformatycznego zdefiniowane przez organizację*] w ogólnosystemowej (logicznej lub fizycznej) ścieżce audytu, która jest skorelowana w czasie z [*Realizacja: poziom tolerancji zdefiniowany przez organizację dla relacji między znacznikami czasowymi i poszczególnymi zapisami w ścieżce audytu*].

Zabezpieczenia powiązane: AU-8, AU-12.

(2) TWORZENIE ZAPISÓW AUDYTU | UJEDNOLICONE FORMATY

System teleinformatyczny tworzy ogólnosystemową (logiczną lub fizyczną) ścieżkę audytu złożoną z rekordów audytu w znormalizowanym (ujednoliconym) formacie.

(3) TWORZENIE ZAPISÓW AUDYTU | ZMIANY DOKONYWANE PRZEZ UPRAWNIONE OSOBY

System teleinformatyczny umożliwia personelowi [*Realizacja: osoby lub role zdefiniowane przez organizację*], dokonywanie zmian audytu, który ma być przeprowadzony w [*Realizacja: komponenty systemu teleinformatycznego zdefiniowanego przez organizację*] w oparciu o [*Realizacja: zdefiniowane przez organizację kryteria wyboru zdarzenia*] w czasie [*Realizacja: progi czasowe zdefiniowane przez organizację*].

Zabezpieczenia powiązane: AU-7.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	AU-12	AU-12	AU-12 (1) (3)

AU-13 MONITOROWANIE UJAWNIANIA INFORMACJI

Zabezpieczenie: organizacja monitoruje [*Realizacja: zdefiniowane przez organizację informacje o otwartym kodzie źródłowym i / lub witryny informacyjne*] z [*Realizacja: częstotliwość zdefiniowana przez organizację*] pod kątem rejestracji dowodów nieuprawnionego ujawnienia informacji organizacyjnych.

Zabezpieczenia powiązane: PE-3, SC-7.

Zabezpieczenia rozszerzone:

(1) MONITOROWANIE UJAWNIANIA INFORMACJI | WYKORZYSTANIE ZAUTOMATYZOWANYCH NARZĘDZI

Organizacja stosuje zautomatyzowane mechanizmy monitorujące w celu ustalenia, czy informacje organizacyjne zostały ujawnione w nieautoryzowany sposób.

(2) MONITOROWANIE UJAWNIANIA INFORMACJI | PRZEGLĄD MONITOROWANYCH STRON

Organizacja dokonuje przeglądu monitorowanych witryn teleinformatycznych otwartym kodzie źródłowym **(**typu open source) z częstotliwością [*Realizacja: częstotliwość określona przez organizację*].

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P0	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	AU-13 (opcjonalnie)	AU-13 (opcjonalnie)	AU-13 (opcjonalnie)

AU-14 AUDYT SESJI

Zabezpieczenie: System teleinformatyczny umożliwia autoryzowanym użytkownikom wybranie sesji dowolnego użytkownika celem jej przechwytywania / nagrywania lub przeglądania / utrwalania.

Zabezpieczenia powiązane: AC-3, AU-4, AU-5, AU-9, AU-11.

Zabezpieczenia rozszerzone:

(1) AUDYT SESJI | URUCHAMIANIE SYSTEMU

System teleinformatyczny inicjuje audyty sesji podczas uruchamiania systemu.

(2) AUDYT SESJI | PRZECHWYTY / NAGRYWANIE I ZAWARTOŚĆ DZIENNIKÓW LOGOWANIA

System teleinformatyczny umożliwia uprawnionym użytkownikom przechwytywanie / rejestrowanie treści i przeglądanie logów związanych z sesją użytkownika.

(3) AUDYT SESJI | ZDALNE WYŚWIETLANIE / ODSŁUCHIWANIE

System teleinformatyczny umożliwia uprawnionym użytkownikom zdalne przeglądanie / odsłuchiwanie w czasie rzeczywistym wszystkich treści związanych z ustanowioną sesją użytkownika.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P0	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	AU-14 (opcjonalnie)	AU-14 (opcjonalnie)	AU-14 (opcjonalnie)

AU-15 ZDOLNOŚĆ DO ALTERNATYWNEGO AUDYTU

Zabezpieczenie: Organizacja zapewnia alternatywną możliwość audytu w przypadku awarii podstawowej funkcji kontrolnej, która zapewnia [*Realizacja: funkcjonalność alternatywnej kontroli zdefiniowana przez organizację*].

Ponieważ alternatywną funkcją audytu może być ochrona krótkoterminowa stosowana do czasu usunięcia awarii w podstawowej funkcji audytu, organizacje mogą ustalić, że ta alternatywna funkcja audytu musi zapewniać tylko podzbiór podstawowej funkcji audytu, na który wpływ ma ta awaria.

Zabezpieczenia powiązane: AU-5.

Zabezpieczenia rozszerzone: Brak.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P0	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	AU-15 (opcjonalnie)	AU-15 (opcjonalnie)	AU-15 (opcjonalnie)

AU-16 AUDYT MIĘDZYORGANIZACYJNY

Zabezpieczenie: Organizacja stosuje *[Realizacja: metody zdefiniowane przez organizację*] do koordynowania [*Realizacja: informacje kontrolne zdefiniowane przez organizację*] między organizacjami zewnętrznymi, gdy informacje audytu są przekazywane poza organizację.

Zabezpieczenia powiązane: AU-6.

Zabezpieczenia rozszerzone:

(1) AUDYT MIĘDZYORGANIZACYJNY | OCHRONA TOŻSAMOŚCI

Organizacja wymaga zachowania tożsamości osób w ścieżkach audytu między organizacjami.

(2) AUDYT MIĘDZYORGANIZACYJNY | UDOSTĘPNIANIE INFORMACJI AUDYTOWYCH

Organizacja przekazuje informacje dotyczące audytu między organizacjami do [*Realizacja: jednostek zdefiniowanych przez organizację*] na podstawie [*Realizacja: zdefiniowane przez organizację porozumienia dotyczące wymiany zapisów audytu między organizacjami*].

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P0	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	AU-16 (opcjonalnie)	AU-16 (opcjonalnie)	AU-16 (opcjonalnie)

KATEGORIA: OCENA BEZPIECZEŃSTWA I AUTORYZACJA

CA-1 OCENA BEZPIECZEŃSTWA I AUTORYZACJA – POLITYKA I PROCEDURY

Zabezpieczenie: Organizacja:

a. Opracowuje, dokumentuje i rozpowszechnia w strukturach [*Realizacja: personel lub role zdefiniowane przez organizację*]:

1. Politykę oceny bezpieczeństwa i autoryzacji, która dotyczy celu, zakresu, ról, obowiązków, zaangażowania kierownictwa, koordynacji między jednostkami organizacyjnymi oraz ich podatności;

2. Procedury ułatwiające wdrażanie polityki oceny bezpieczeństwa i autoryzacji oraz powiązanie szacowania ryzyka utraty bezpieczeństwa (oceny bezpieczeństwa) i uwierzytelnione zabezpieczenia;

b. Recenzuje i aktualizuje obowiązujące:

   1. Oceny bezpieczeństwa i polityki autoryzacji z częstotliwością [*Realizacja: częstotliwość określona przez organizację*];

   2. Procedury szacowania ryzyka utraty bezpieczeństwa i autoryzacji z częstotliwością [*Realizacja: częstotliwość określona przez organizację*].

Zabezpieczenia powiązane: PM-9.

Zabezpieczenia rozszerzone: Brak.

Zabezpieczenia powiązane: Brak.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	CA-1	CA-1	CA-1

CA-2 OCENA BEZPIECZEŃSTWA

Zabezpieczenie: Organizacja:

a. Opracowuje plan oceny bezpieczeństwa (szacowanie ryzyka utraty bezpieczeństwa), który opisuje zakres oceny, w tym:

   1. Środki bezpieczeństwa (zabezpieczenia) i ulepszenia zabezpieczeń podlegające oszacowaniu;

   2. Procedury oceny bezpieczeństwa stosowane w celu ustalenia skuteczności zabezpieczeń;

   3. Środowisko oceniające, zespół oceniający oraz role i obowiązki;

b. Ocenia środki bezpieczeństwa stosowane w systemie teleinformatycznym i jego środowisku działania z częstotliwością [*Realizacja: częstotliwość zdefiniowana przez organizację*], w celu określenia zakresu, w jakim zabezpieczenia są wdrażane prawidłowo, działają zgodnie z przeznaczeniem i osiągają pożądany wynik w odniesieniu do spełnienia ustalonych wymagań bezpieczeństwa;

c. Tworzy raport z oceny bezpieczeństwa dokumentujący wyniki oceny;

d. Dostarcza wyniki oceny kontroli bezpieczeństwa [*Realizacja: osoby lub role zdefiniowane przez organizację*].

Zabezpieczenia powiązane: CA-5, CA-6, CA-7, PM-9, RA-5, SA-11, SA-12, SI-4.

Zabezpieczenia rozszerzone:

(1) OCENA BEZPIECZEŃSTWA | NIEZALEŻNI AUDYTORZY

Organizacja zatrudnia audytorów lub zespoły oceniające z [*Realizacja: poziom niezależności zdefiniowany przez organizację*[24]] do przeprowadzania oceny stosowanych środków bezpieczeństwa.

(2) OCENA BEZPIECZEŃSTWA | OCENY SPECJALISTYCZNE

Organizacja przeprowadza, w ramach oceny kontroli bezpieczeństwa, oceny specjalistyczne [[*Realizacja: częstotliwość określona przez organizację], [Realizacja: ogłoszony; niezapowiedziany], [Wybór (jeden lub więcej): dogłębne monitorowanie; skanowanie podatności; testowanie złośliwych użytkowników; ocena zagrożenia wewnętrznego; testowanie wydajności / obciążenia; [Realizacja: inne formy oceny bezpieczeństwa zdefiniowane przez organizację*]].

Zabezpieczenia powiązane: PE-3, SI-2.

(3) OCENA BEZPIECZEŃSTWA | ORGANIZACJE ZEWNĘTRZNE

Organizacja akceptuje wyniki oceny systemu [*Realizacja: system teleinformatyczny zdefiniowany przez organizację*] przeprowadzonej przez [*Realizacja: organizacja zewnętrzna zdefiniowana przez organizację*] jedynie w przypadku, gdy ocena spełnia [*Realizacja: wymagania zdefiniowane przez organizację*].

Zabezpieczenia powiązane: Brak.

[24] Podmiot zewnętrzny lub wewnętrzna komórka audytu.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P2	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	CA-2	CA-2 (1)	CA-2 (1) (2)

CA-3 POŁĄCZENIA MIĘDZYSYSTEMOWE

Zabezpieczenie: Organizacja:

a. Autoryzuje podłączenia własnego systemu teleinformatycznego do innych systemów teleinformatycznych za pomocą umów o wzajemnym połączeniu;

b. Dokumentuje, w odniesieni do każdego połączenia, charakterystyki interfejsu, wymagania bezpieczeństwa i charakter przekazywanych informacji;

c. Przegląda i aktualizuje umowy o wzajemnych połączeniach (umowy interkonektowe) w zakresie dotyczącym środków bezpieczeństwa z częstotliwością [*Realizacja: częstotliwość określona przez organizację*].

Zabezpieczenia powiązane: AC-3, AC-4, AC-20, AU-2, AU-12, AU-16, CA-7, IA-3, SA-9, SC-7, SI-4.

Zabezpieczenia rozszerzone:

(1) POŁĄCZENIA MIĘDZYSYSTEMOWE | POŁĄCZENIA JAWNYCH BEZPIECZNYCH SYSTEMÓW KRAJOWYCH

Organizacja zabrania bezpośredniego połączenia [*Realizacja: zdefiniowany przez organizację jawny, bezpieczny system krajowy*] do sieci zewnętrznej bez użycia [*Realizacja: zdefiniowane przez organizację urządzenie brzegowe*].

(2) POŁĄCZENIA MIĘDZYSYSTEMOWE | POŁĄCZENIA NIEJAWNYCH SYSTEMÓW KRAJOWYCH

Organizacja zabrania bezpośredniego połączenia niejawnego systemu z siecią zewnętrzną bez użycia [*Realizacja: brzegowe urządzenie zabezpieczające zdefiniowane przez organizację*]. Zgodnie obowiązującymi przepisami połączenie systemu niejawnego z siecią zewnętrzną odbywa się po spełnieniu wymogów określonych w przepisach wydanych na podstawie ustawy o ochronie informacji niejawnych.

(3) POŁĄCZENIA MIĘDZYSYSTEMOWE | POŁĄCZENIA JAWNYCH BEZPIECZNYCH SYSTEMÓW TRANSGRANICZNYCH

Organizacja zabrania bezpośredniego przyłączenia *[Realizacja: zdefiniowany przez organizację jawny bezpieczny system transgraniczny*] do sieci zewnętrznej bez użycia [*Realizacja: brzegowe urządzenie zabezpieczające zdefiniowane przez organizację*].

(4) POŁĄCZENIA MIĘDZYSYSTEMOWE | POŁĄCZENIA Z SIECIAMI PUBLICZNYMI

Organizacja zabrania bezpośredniego połączenia *[Realizacja: system teleinformatyczny zdefiniowany przez organizację*] z siecią publiczną (np. Internet i ekstranety organizacyjne z dostępem publicznym).

(5) POŁĄCZENIA MIĘDZYSYSTEMOWE | OGRANICZENIA DOTYCZĄCE POŁĄCZEŃ SYSTEMU ZEWNĘTRZNEGO

Organizacja stosuje polityki [*Realizacja: zezwalające na wszystko za wyjątkiem; odmawiające wszystkiego za wyjątkiem*] umożliwiające systemowi teleinformatycznemu [*Realizacja: systemy informacyjne zdefiniowane przez organizację*] na połączenie z zewnętrznymi systemami teleinformatycznymi.

Zabezpieczenia powiązane: CM-7.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	CA-3	CA-3 (5)	CA-3 (5)

CA-4 CERTYFIKACJA BEZPIECZEŃSTWA

[Włączony do CA-2].

CA-5 PLAN I ETAPY DZIAŁANIA

Zabezpieczenie: Organizacja:

a. Opracowuje plan i etapy działania systemu teleinformatycznego w celu udokumentowania planowanych przez organizację działań naprawczych mających za zadanie skorygowanie słabości lub usunięcie braków odnotowanych podczas oceny kontroli bezpieczeństwa oraz w celu zmniejszenia lub wyeliminowania znanych słabych punktów w systemie;

b. Aktualizuje istniejący plan i etapy działania z częstotliwością [*Realizacja: częstotliwość określona przez organizację*] w oparciu o ustalenia z oceny kontroli bezpieczeństwa, analiz wpływu na bezpieczeństwo i ciągłego monitorowania użycia systemu.

Zabezpieczenia powiązane: CA-2, CA-7, CM-4, PM-4.

Zabezpieczenia rozszerzone:

(1) PLAN I ETAPY DZIAŁANIA | AUTOMATYZACJA WSPIERAJĄCA AKTUALNOŚĆ / SZCZEGÓŁOWOŚĆ PLANÓW

Organizacja stosuje zautomatyzowane mechanizmy zapewniające szczegółowość, aktualność i dostępność planu i etapów działania systemu teleinformatycznego.

Zabezpieczenia powiązane: Brak.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P3	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	CA-5	CA-5	CA-5

CA-6 AUTORYZACJA BEZPIECZEŃSTWA

Zabezpieczenie: Organizacja:

a. Dopuszcza system teleinformatyczny do przetwarzania informacji. Dokonuje tego kierownik jednostki organizacyjnej lub osoba przez niego wyznaczona.

b. Zapewnia, że dopuszczenie systemu teleinformatycznego do przetwarzania informacji następuje przed rozpoczęciem przetwarzania informacji w systemie;

c. Aktualizuje autoryzację bezpieczeństwa z częstotliwością [*Realizacja: częstotliwość zdefiniowana przez organizację*].

Zabezpieczenia powiązane: CA-2, CA-7, PM-9, PM-10.

Zabezpieczenia rozszerzone: Brak.

Zabezpieczenia powiązane: Brak

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P2	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	CA-6	CA-6	CA-6

CA-7 CIĄGŁOŚĆ MONITOROWANIA

Zabezpieczenie: Organizacja opracowuje strategię ciągłego monitorowania i wdraża program ciągłego monitorowania, który obejmuje:

a. Ustanowienie [*Realizacja: dane / metryki zdefiniowane przez organizację*] do monitorowania;

b. Ustanowienie [*Realizacja: częstotliwości określone przez organizację*] do monitorowania i [*Realizacja: częstotliwości określone przez organizację*] do oceny wspierającej takie monitorowanie;

c. Bieżące oceny kontroli bezpieczeństwa zgodnie ze strategią ciągłego monitorowania organizacji;

d. Bieżące monitorowanie stanu bezpieczeństwa metryk zdefiniowanych przez organizację zgodnie ze strategią ciągłego monitorowania organizacji;

e. Korelacje i analizy informacji związanych z bezpieczeństwem, wygenerowanych przez procesy oceny ryzyka i monitorowania;

f. Podejmowanie reakcji na uzyskane wyniki analizy informacji związanych z bezpieczeństwem;

g. Zgłaszanie statusu bezpieczeństwa organizacji i systemu teleinformatycznego do [*Realizacja: personel lub role zdefiniowane przez organizację*] z częstotliwością [*Realizacja: częstotliwość zdefiniowana przez organizację*].

Zabezpieczenia powiązane: CA-2, CA-5, CA-6, CM-3, CM-4, PM-6, PM-9, RA-5, SA-11, SA-12, SI-2, SI-4.

Zabezpieczenia rozszerzone:

(1) CIĄGŁOŚĆ MONITOROWANIA | NIEZALEŻNA OCENA

Organizacja zatrudnia audytorów lub zespoły oceniające o odpowiednich poziomach niezależności [*Realizacja: poziom niezależności zdefiniowany przez organizację*] do bieżącego monitorowania środków bezpieczeństwa w systemie teleinformatycznym.

(2) CIĄGŁOŚĆ MONITOROWANIA | RODZAJE OCEN

[Włączone do CA-2].

(3) CIĄGŁOŚĆ MONITOROWANIA | ANALIZY TRENDÓW

Organizacja stosuje analizy trendów w celu ustalenia, czy wdrażane środki bezpieczeństwa, częstotliwość ciągłego monitorowania i / lub rodzaje działań wykorzystywanych w procesie ciągłego monitorowania wymagają modyfikacji w oparciu o dane empiryczne.

Zabezpieczenia powiązane: Brak

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P2	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	CA-7	CA-7 (1)	CA-7 (1)

CA-8 TESTY PENETRACYJNE

Zabezpieczenie: Organizacja przeprowadza testy penetracyjne z częstotliwością [*Realizacja: częstotliwość zdefiniowana przez organizację*] w systemach teleinformatycznych [*Realizacja: zdefiniowane przez organizację systemy teleinformatyczne lub komponenty systemu teleinformatycznego*].

Zabezpieczenia powiązane: SA-12.

Zabezpieczenia rozszerzone:

(1) TESTY PENETRACYJNE | NIEZALEŻNY TESTER LUB ZESPÓŁ PENETRACYJNY

Organizacja zatrudnia niezależnego testera penetracyjnego lub zespół penetracyjny do przeprowadzania testów penetracyjnych w systemie teleinformatycznym lub jego komponentach**.**
Zabezpieczenia powiązane: CA-2.

(2) TESTY PENETRACYJNE | ĆWICZENIA ZESPOŁU ATAKUJĄCEGO TYPU „RED TEAM"

Organizacja stosuje [*Realizacja: zdefiniowane przez organizację ćwiczenia zespołu ofensywnego typu "Red Team"*] w celu symulacji prób naruszenia przez przeciwników systemów teleinformatycznych organizacji zgodnie z [*Realizacja: reguły określone przez organizację*].

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P2	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	CA-8 (opcjonalnie)	CA-8 (opcjonalnie)	CA-8

CA-9 POŁĄCZENIA WEWNĄTRZSYSTEMOWE

Zabezpieczenie: Organizacja:

a. Autoryzuje wewnętrzne połączenia [*Realizacja: komponenty systemu teleinformatycznego zdefiniowane przez organizację lub klasy komponentów*] z systemem teleinformatycznym;

b. Opracowuje dokumenty dla każdego połączenia wewnętrznego, charakterystykę interfejsu, wymagania bezpieczeństwa i charakter przekazywanych informacji.

Zabezpieczenia powiązane: AC-3, AC-4, AC-18, AC-19, AU-2, AU-12, CA-7, CM-2, IA-3, SC-7, SI-4.

Zabezpieczenia rozszerzone:

(1) POŁĄCZENIA WEWNĄTRZSYSTEMOWE | KONTROLE ZGODNOŚCI BEZPIECZEŃSTWA

System teleinformatyczny przeprowadza kontrole zgodności bezpieczeństwa elementów systemu (np. weryfikację odpowiedniej konfiguracji podstawowej) przed nawiązaniem połączenia wewnętrznego**.**

Zabezpieczenia powiązane: CM-6.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P2	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	CA-9	CA-9	CA-9

KATEGORIA: ZARZĄDZANIE KONFIGURACJĄ

CM-1 ZARZĄDZANIA KONFIGURACJĄ – POLITYKA I PROCEDURY

Zabezpieczenie: Organizacja:

a. Opracowuje, dokumentuje i rozpowszechnia w odniesieniu do [*Realizacja: personel lub role zdefiniowane przez organizację*]:

   1. Politykę zarządzania konfiguracją, która dotyczy celu, zakresu, ról, obowiązków, zaangażowania w zarządzanie, koordynacji między jednostkami organizacyjnymi oraz ich podatności;

   2. Procedury ułatwiające wdrożenie polityki zarządzania konfiguracją i powiązane środki zarządzania konfiguracją;

b. Przegląda i aktualizuje aktualne:

   1. Politykę zarządzania konfiguracją z częstotliwością [*Realizacja: częstotliwość określona przez organizację*];

   2. Procedury zarządzania konfiguracją z częstotliwością [*Realizacja: częstotliwość określona przez organizację*].

Zabezpieczenia powiązane: PM-9.

Zabezpieczenia rozszerzone: Brak.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	CM-1	CM-1	CM-1

CM-2 KONFIGURACJA PODSTAWOWA

Zabezpieczenie: organizacja opracowuje, dokumentuje i utrzymuje pod bieżącą kontrolą konfigurację bazową systemu teleinformatycznego.

Zabezpieczenia powiązane: CM-3, CM-6, CM-8, CM-9, SA-10, PM-5, PM-7.

Zabezpieczenia rozszerzone:

(1) KONFIGURACJA PODSTAWOWA | PRZEGLĄD I AKTUALIZACJE

Organizacja przegląda i aktualizuje podstawową konfigurację systemu teleinformatycznego:

(a) Z określoną częstotliwością [*Realizacja: częstotliwość określona przez organizację*];

(b) Gdy jest to wymagane ze względu na [*Realizacja: okoliczności zdefiniowane przez organizację*];

(c) Jako integralną część instalacji i aktualizacji komponentów systemu teleinformatycznego.

Zabezpieczenia powiązane: CM-5.

(2) KONFIGURACJA PODSTAWOWA | AUTOMATYZACJA WSPIERAJĄCA AKTUALNOŚĆ / SZCZEGÓŁOWOŚĆ

Organizacja wykorzystuje zautomatyzowane mechanizmy do utrzymywania aktualnej, kompletnej, dokładnej i łatwo dostępnej konfiguracji systemu teleinformatycznego.

Zabezpieczenia powiązane: CM-7, RA-5.

(3) KONFIGURACJA PODSTAWOWA | RETENCJA ZACHOWANYCH KONFIGURACJI

Organizacja zachowuje [*Realizacja: zdefiniowane przez organizację poprzednie wersje podstawowych konfiguracji systemu teleinformatycznego*] w celu obsługi wycofanych wersji podstawowych konfiguracji.

(4) KONFIGURACJA PODSTAWOWA | NIEAUTORYZOWANE OPROGRAMOWANIE

[Włączone do CM-7].

(5) KONFIGURACJA PODSTAWOWA | AUTORYZOWANE OPROGRAMOWANIE

[Włączone do CM-7].

(6) KONFIGURACJA PODSTAWOWA | ROZBUDOWA SYSTEMÓW I ŚRODOWISKA BADAWCZE

Organizacja utrzymuje konfigurację podstawową do rozbudowy systemów teleinformatycznych i środowiska testowego, które są zarządzane niezależnie od operacyjnej konfiguracji bazowej.

Zabezpieczenia powiązane: CM-4, SC-3, SC-7.

(7) KONFIGURACJA PODSTAWOWA | KONFIGUROWANIE SYSTEMU, KOMPONENTÓW LUB URZĄDZEŃ W OBSZARACH WYSOKIEGO RYZYKA

Organizacja:

(a) Przydziela do użytkowania [*Realizacja: zdefiniowane przez organizację systemy teleinformatyczne, komponenty systemu lub urządzenia*] z [*Realizacja: konfiguracje zdefiniowane przez organizację*] osobom podróżującym do miejsc, które organizacja uważa za stanowiące znaczące ryzyko;

(b) Stosuje zabezpieczenia [*Realizacja: środki bezpieczeństwa zdefiniowane przez organizację*] w zwracanych do organizacji urządzeniach.

Zabezpieczenia powiązane: Brak.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	CM-2	CM-2 (1) (3) (7)	CM-2 (1) (2) (3) (7)

CM-3 ZABEZPIECZANIE ZMIAN KONFIGURACJI

Zabezpieczenie: Organizacja:

a. Określa rodzaje dozwolonych zmian w zabezpieczeniach konfiguracji systemu teleinformatycznego;

b. Przegląda proponowane zmiany konfiguracji zabezpieczeń w systemie teleinformatycznym i zatwierdza lub odrzuca takie zmiany, z wyraźnym uwzględnieniem analiz wpływu na bezpieczeństwo systemu;

c. Dokumentuje decyzje o zmianie konfiguracji związanej z systemem teleinformatycznym;

d. Wprowadza dozwolone zmiany w zabezpieczeniach konfiguracji systemu teleinformatycznego;

e. Przechowuje zapisy dokonanych zmian w zabezpieczeniach systemu teleinformatycznego przez okres [*Realizacja: okres zdefiniowany przez organizację*];

f. Przeprowadza audyty i przeglądy dokonanych zmian w zabezpieczeniach systemu teleinformatycznego;

g. Koordynuje i zapewnia nadzór nad dokonywanymi zmianami konfiguracji przez [*Realizacja: element zabezpieczenia systemu teleinformatycznego zdefiniowany przez organizację*], który wywołuje [*Wybór (jeden lub więcej): [Realizacja: częstotliwość zdefiniowana przez organizację]; [Realizacja: warunki zmian w zabezpieczeniach konfiguracji zdefiniowanych przez organizację*]].

Zabezpieczenia powiązane: CA-7, CM-2, CM-4, CM-5, CM-6, CM-9, SA-10, SI-2, SI-12.

Zabezpieczenia rozszerzone:

(1) ZABEZPIECZANIE ZMIANY KONFIGURACJI | AUTOMATYCZNA DOKUMENTACJA / POWIADAMIANIE / ZAKAZ ZMIAN

Organizacja stosuje zautomatyzowane mechanizmy do:

(a) Udokumentowania proponowanych zmian w systemie teleinformatycznym;

(b) Powiadamiania [*Realizacja: zdefiniowane organy zatwierdzające*] o proponowanych zmianach w systemie teleinformatycznym i żądaniu zatwierdzenia zmian;

(c) Wykazania proponowanych zmian w systemie teleinformatycznym, które nie zostały zatwierdzone lub odrzucone przez okres [*Realizacja: okres zdefiniowany przez organizację*];

(d) Uniemożliwiania wprowadzania zmian w systemie teleinformatycznym do czasu otrzymania autoryzacji do wykonania tych zmian;

(e) Dokumentowania wszystkich zmian w systemie teleinformatycznym;

(f) Powiadamiania [*Realizacja: personel zdefiniowany w organizacji*] o zakończeniu zatwierdzonych zmian w systemie teleinformatycznym.

(2) ZABEZPIECZANIE ZMIANY KONFIGURACJI | TESTY / WALIDACJA / ZMIANY DOKUMENTÓW

Organizacja testuje, sprawdza i dokumentuje zmiany w systemie teleinformatycznym przed wdrożeniem zmian w systemie operacyjnym.

(3) ZABEZPIECZANIE ZMIANY KONFIGURACJI | AUTOMATYCZNEJ ZMIANY IMPLEMENTACJI

Organizacja stosuje zautomatyzowane mechanizmy implementacji zmian w aktualnych bazach systemów teleinformatycznych poprzez dokonanie instalacji zaktualizowanej bazy w systemie.

(4) ZABEZPIECZANIE ZMIANY KONFIGURACJI | PRZEDSTAWICIEL BEZPIECZEŃSTWA

Organizacja wymaga, aby osoba odpowiedzialna za nadzór nad bezpieczeństwem teleinformatycznym była członkiem zespołu [*Realizacja: element kontroli zmian konfiguracji zdefiniowany przez organizację*].

(5) ZABEZPIECZANIE ZMIANY KONFIGURACJI | AUTOMATYCZNA REAKCJA BEZPIECZEŃSTWA

System informacyjny wdraża automatycznie [*Realizacja: środki bezpieczeństwa zdefiniowane przez organizację*] w sytuacji, gdy podstawowe konfiguracje są zmieniane w sposób nieuprawniony.

(6) ZABEZPIECZANIE ZMIANY KONFIGURACJI | ZARZĄDZANIE KRYPTOGRAFICZNE

Organizacja zapewnia, że mechanizmy kryptograficzne używane do zapewnienia [*Realizacja: środki bezpieczeństwa zdefiniowane przez organizację*] podlegają zarządzaniu konfiguracji.

Zabezpieczenia powiązane: SC-13.

Zabezpieczenia powiązane: Brak

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	CM-3 (opcjonalnie)	CM-3 (2	CM-3 (1) (2)

CM-4 ANALIZA ZMIAN WPŁYWAJĄCYCH NA BEZPIECZEŃSTWO

Zabezpieczenie: Organizacja analizuje zmiany w systemie teleinformatycznym, aby określić potencjalny wpływ na bezpieczeństwo systemu przed wdrożeniem zmiany.

Zabezpieczenia powiązane: CA-2, CA-7, CM-3, CM-9, SA-4, SA-5, SA-10, SI-2.

Zabezpieczenia rozszerzone:

(1) ANALIZA ZMIAN WPŁYWAJĄCYCH NA BEZPIECZEŃSTWO | ODDZIELNE ŚRODOWISKA BADAWCZE

Przed wdrożeniem do środowiska operacyjnego, organizacja analizuje zmiany w systemie teleinformatycznym w oddzielnym środowisku testowym, szukając wpływu na poziom bezpieczeństwa wynikającego z wad, słabości, niekompatybilności lub umyślnej złośliwości.

Zabezpieczenia powiązane: SA-11, SC-3, SC-7.

(2) ANALIZA ZMIAN WPŁYWAJĄCYCH NA BEZPIECZEŃSTWO | WERYFIKACJA FUNKCJI BEZPIECZEŃSTWA

Po zmianie wprowadzonej do systemu teleinformatycznego, organizacja sprawdza funkcje bezpieczeństwa, weryfikując, czy funkcje zostały poprawnie zaimplementowane, działają zgodnie z przeznaczeniem i dają pożądany wynik w odniesieniu do spełnienia wymagań bezpieczeństwa systemu.

Zabezpieczenia powiązane: SA-11.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P2	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	CM-4	CM-4	CM-4 (1)

CM-5 OGRANICZENIA MOŻLIWOŚCI DOKONYWANIA ZMIAN

Zabezpieczenie: Organizacja definiuje, dokumentuje, zatwierdza i egzekwuje fizyczne i logiczne ograniczenia dostępu związane ze zmianami w systemie teleinformatycznym.

Zabezpieczenia powiązane: AC-3, AC-6, PE-3.

Zabezpieczenia rozszerzone:

(1) OGRANICZENIA MOŻLIWOŚCI DOKONYWANIA ZMIAN | REALIZACJA AUTOMATYCZNEGO DOSTĘPU / AUDYTU

System teleinformatyczny automatycznie egzekwuje ograniczenia dostępu i wspiera audyt działań wykonawczych.

Zabezpieczenia powiązane: AU-2, AU-12, AU-6, CM-3, CM-6.

(2) OGRANICZENIA MOŻLIWOŚCI DOKONYWANIA ZMIAN | PRZEGLĄD ZMIAN SYSTEMU

Organizacja dokonuje przeglądu zmian w systemie teleinformatycznym z częstotliwością [*Realizacja: częstotliwość zdefiniowana przez organizację*] i przeprowadza działania [*Realizacja: okoliczności opisane przez organizację*] w celu ustalenia, czy nastąpiły nieautoryzowane zmiany.

Zabezpieczenia powiązane: AU-6, AU-7, CM-3, CM-5, PE-6, PE-8.

(3) OGRANICZENIA MOŻLIWOŚCI DOKONYWANIA ZMIAN | PODPISANE KOMPONENTY

System teleinformatyczny uniemożliwia instalację [*Realizacja: oprogramowanie zdefiniowane przez organizację i komponenty oprogramowania układowego*] bez weryfikacji, czy składnik został podpisany cyfrowo za pomocą certyfikatu uznanego i zatwierdzonego przez organizację.

Zabezpieczenia powiązane: CM-7, SC-13, SI-7.

(4) OGRANICZENIA MOŻLIWOŚCI DOKONYWANIA ZMIAN | PODWÓJNA AUTORYZACJA

Organizacja wymusza podwójną autoryzację do wprowadzania zmian w [*Realizacja: komponenty systemu teleinformatycznego zdefiniowane przez organizację i informacje na poziomie systemu*].

Zabezpieczenia powiązane: AC-5, CM-3.

(5) OGRANICZENIA MOŻLIWOŚCI DOKONYWANIA ZMIAN | OGRANICZENIA PRODUKTOWE / UPRAWNIENIA OPERACYJNE

Organizacja:

(a) Ogranicza uprawnienia do zmiany komponentów systemu teleinformatycznego i informacji związanych z systemem w środowisku produkcyjnym lub operacyjnym;

(b) Przegląda i ponownie ocenia uprawnienia z częstotliwością [*Realizacja: częstotliwość określona przez organizację*].

Zabezpieczenia powiązane: AC-2.

(6) OGRANICZENIA MOŻLIWOŚCI DOKONYWANIA ZMIAN | OGRANICZENIE PRZYWILEJÓW W BIBLIOTEKACH OPROGRAMOWANIA

Organizacja ogranicza uprawnienia do zmiany rezydenta oprogramowania w bibliotekach oprogramowania zawierających programy uprzywilejowane.

Biblioteki oprogramowania zawierają programy uprzywilejowane.

Zabezpieczenia powiązane: AC-2.

(7) OGRANICZENIA MOŻLIWOŚCI DOKONYWANIA ZMIAN | AUTOMATYCZNA REALIZACJA ZABEZPIECZEŃ BEZPIECZEŃSTWA

[Włączono do SI-7].

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	CM-5 (opcjonalnie)	CM-5	CM-5 (1) (2) (3)

CM-6 USTAWIENIA KONFIGURACJI

Zabezpieczenie: Organizacja:

a. Ustanawia i dokumentuje ustawienia konfiguracji produktów informatycznych stosowanych w systemie teleinformatycznym przy użyciu [*Realizacja: listy kontrolne konfiguracji zabezpieczeń zdefiniowane przez organizację*], które odzwierciedlają najbardziej restrykcyjny tryb zgodny z wymaganiami operacyjnymi;

b. Implementuje ustawienia konfiguracji;

c. Identyfikuje, dokumentuje i zatwierdza wszelkie odchylenia od ustalonych ustawień konfiguracji dla [*Realizacja: elementy systemu teleinformatycznego zdefiniowane przez organizację*] na podstawie [*Realizacja: wymagania operacyjne określone przez organizację*];

d. Monitoruje i kontroluje zmiany w ustawieniach konfiguracji zgodnie z zasadami i procedurami organizacyjnymi.

Zabezpieczenia powiązane: AC-19, CM-2, CM-3, CM-7, SI-4.

Zabezpieczenia rozszerzone:

(1) USTAWIENIA KONFIGURACJI | AUTOMATYCZNE ZCENTRALIZOWANE ZARZĄDZANIE / APLIKACJA / WERYFIKACJA

Organizacja wykorzystuje zautomatyzowane mechanizmy do centralnego zarządzania, zastosowania i weryfikacji ustawień konfiguracji dla [*Realizacja: komponenty systemu teleinformatycznego zdefiniowane przez organizację*].

Zabezpieczenia powiązane: CA-7, CM-4.

(2) USTAWIENIA KONFIGURACJI | ODPOWIEDŹ NA NIEAUTORYZOWANE ZMIANY

Organizacja stosuje [*Realizacja: zabezpieczenia bezpieczeństwa zdefiniowane przez organizację*], wymuszające reakcje[25] na nieautoryzowane zmiany w [*Realizacja: ustawienia konfiguracji zdefiniowane przez organizację*].

Zabezpieczenia powiązane: IR-4, SI-7.

(3) USTAWIENIA KONFIGURACJI | WYKRYWANIE NIEAUTORYZOWANYCH ZMIAN

[Włączono do SI-7].

(4) USTAWIENIA KONFIGURACJI | PREZENTACJA ZGODNOŚCI

[Włączono do CM-4].

Zabezpieczenia powiązane: Brak

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	CM-6	CM-6	CM-6 (1) (2)

[25] Reakcje na nieautoryzowane zmiany w ustawieniach konfiguracji mogą obejmować np. alarmowanie wyznaczonego personelu organizacyjnego, przywracanie ustalonych ustawień konfiguracji lub, w skrajnych przypadkach, zatrzymywanie przetwarzania systemu teleinformatycznego, którego dotyczy problem.

CM-7 ZASADA MINIMALNEJ FUNKCJONALNOŚCI

Zabezpieczenie: Organizacja:

a. Konfiguruje system teleinformatyczny tak, aby zapewniał tylko niezbędne wymagane funkcje;

b. Zabrania lub ogranicza korzystanie z następujących funkcji, portów, protokołów i / lub usług: [Realizacja: zdefiniowane przez organizację funkcje zabronione lub ograniczone, porty, protokoły i / lub usługi].

Zabezpieczenia powiązane: AC-6, CM-2, RA-5, SA-5, SC-7.

Zabezpieczenia rozszerzone:

(1) ZASADA MINIMALNEJ FUNKCJONALNOŚCI **|** OKRESOWE PRZEGLĄDY

Organizacja:

(a) Dokonuje przeglądu systemu teleinformatycznego z częstotliwością [*Realizacja: częstotliwość zdefiniowana przez organizację*], celem zidentyfikowania niepożądanych i / lub niezabezpieczonych funkcji, portów, protokołów i usług;

(b) Wyłącza [*Realizacja: funkcje, porty, protokoły i usługi zdefiniowane przez organizację w systemie teleinformatycznym uznane za niepotrzebne i / lub niezabezpieczone*].

Zabezpieczenia powiązane: AC-18, CM-7, IA-2.

(2) ZASADA MINIMALNEJ FUNKCJONALNOŚCI | ZAPOBIEGANIE WYKONYWANIA PROGRAMU

System teleinformatyczny uniemożliwia wykonanie programu zgodnie z [*Wybór (jeden lub więcej): [Realizacja: zdefiniowane przez organizację zasady dotyczące korzystania z oprogramowania i ograniczeń*]; zasady autoryzujące warunki użytkowania oprogramowania]].

Zabezpieczenia powiązane: CM-8, PM-5.

(3) ZASADA MINIMALNEJ FUNKCJONALNOŚCI | STOSOWANIE REJESTRACJI

Organizacja zapewnia stosowanie [*Realizacja: zdefiniowane przez organizację wymagania rejestracyjne dla funkcji, portów, protokołów i usług*].

(4) ZASADA MINIMALNEJ FUNKCJONALNOŚCI | NIEAUTORYZOWANE OPROGRAMOWANIE / **„**CZARNA LISTA”

Organizacja:

(a) Identyfikuje [*Realizacja: oprogramowanie zdefiniowane przez organizację, które nie ma uprawnień do rezydowania w systemie teleinformatycznym*];

(b) stosuje zasadę „zezwalaj na wszystko za wyjątkiem”, aby zabronić wykonywania nieautoryzowanych programów w systemie teleinformatycznym;

(c) Przegląda i aktualizuje listę nieautoryzowanych programów z częstotliwością [*Realizacja: częstotliwość określona przez organizację*].

Zabezpieczenia powiązane: CM-6, CM-8, PM-5.

(5) ZASADA MINIMALNEJ FUNKCJONALNOŚCI | AUTORYZOWANE OPROGRAMOWANIE / „BIAŁA LISTA"

Organizacja:

(a) Identyfikuje [*Realizacja: oprogramowanie zdefiniowane przez organizację uprawnione do zainstalowania w systemie teleinformatycznym*];

(b) Stosuje zasadę „odmawiaj wszystkiego za wyjątkiem", aby umożliwić wykonanie autoryzowanego oprogramowania w systemie teleinformatycznym;

(c) Przegląda i aktualizuje listę autoryzowanych programów z częstotliwością [*Realizacja: częstotliwość określona przez organizację*].

Zabezpieczenia powiązane: CM-2, CM-6, CM-8, PM-5, SA-10, SC-34, SI-7.

Zabezpieczenia powiązane: Brak

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	CM-7	CM-7 (1) (2) (4)	CM-7 (1) (2) (5)

CM-8 INWENTARYZACJA KOMPONENTÓW SYSTEMU TELEINFORMATYCZNEGO

Zabezpieczenie: Organizacja:

a. Opracowuje i dokumentuje spis komponentów systemu teleinformatycznego, który:

   1. Dokładnie odzwierciedla architekturę eksploatowanego systemu teleinformatycznego;
   2. Obejmuje wszystkie elementy autoryzowanego systemu teleinformatycznego;
   3. Jest na poziomie szczegółowości uznanym za niezbędny do śledzenia i raportowania;
   4. Obejmuje [*Realizacja: informacje zdefiniowane przez organizację uznane za niezbędne do osiągnięcia skutecznej rozliczalności komponentów systemu teleinformatycznego*[26]];

b. Przegląda i aktualizuje spis komponentów systemu teleinformatycznego z częstotliwością *[Realizacja: częstotliwość określona przez organizację*].

[26] Informacje uznane za niezbędne do skutecznego rozliczenia komponentów systemu teleinformatycznego obejmują, np., specyfikacje inwentaryzacyjne sprzętu, informacje o licencji oprogramowania, numery wersji oprogramowania, właścicieli komponentów oraz komponenty lub urządzenia w sieci, nazwy maszyn i adresy sieciowe. Specyfikacje zapasów obejmują na przykład producenta, typ urządzenia, model, numer seryjny i lokalizację fizyczną.

Zabezpieczenia powiązane: CM-2, CM-6, PM-5.

Zabezpieczenia rozszerzone:

(1) INWENTARYZACJA KOMPONENTÓW SYSTEMU TELEINFORMATYCZNEGO | AKTUALIZACJE INSTALACJI / USUWANIA KOMPONENTÓW

Organizacja aktualizuje spis komponentów systemu teleinformatycznego jako integralną część instalacji, usuwania i aktualizacji komponentów systemu teleinformatycznego.

(2) INWENTARYZACJA KOMPONENTÓW SYSTEMU TELEINFORMATYCZNEGO | AUTOMATYCZNA UTRZYMANIE

Organizacja stosuje zautomatyzowane mechanizmy pomagające w utrzymaniu aktualnego, pełnego, dokładnego i łatwo dostępnego spisu komponentów systemu teleinformatycznego.

Zabezpieczenia powiązane: SI-7.

(3) INWENTARYZACJA KOMPONENTÓW SYSTEMU TELEINFORMATYCZNEGO | AUTOMATYCZNE WYKRYWANIE KOMPONENTÓW NIEAUTORYZOWANYCH

Organizacja:

(a) Stosuje zautomatyzowane mechanizmy [*Realizacja: częstotliwość zdefiniowana przez organizację*] do wykrywania obecności nieautoryzowanego sprzętu, oprogramowania i komponentów oprogramowania układowego (sprzętowego) w systemie teleinformatycznym;

(b) Podejmuje następujące działania po wykryciu nieautoryzowanych komponentów: [*Wybór (jeden lub więcej): wyłącza dostęp do sieci przez takie komponenty; izoluje komponenty; powiadamia [Realizacja: personel lub role zdefiniowane przez organizację*]].

Zabezpieczenia powiązane: AC-17, AC-18, AC-19, CA-7, SI-3, SI-4, SI-7, RA-5.

(4) INWENTARYZACJA KOMPONENTÓW SYSTEMU TELEINFORMATYCZNEGO | INFORMACJE O ODPOWIEDZIALNOŚCI I ROZLICZALNOŚCI

Organizacja zawiera w wykazie informacji o komponencie systemu teleinformatycznego sposób identyfikacji poprzez [*Wybór (jeden lub więcej): nazwa; pozycja; rola], osoby odpowiedzialne / rozliczane za administrowanie tymi komponentami*].

(5) INWENTARYZACJA KOMPONENTÓW SYSTEMU TELEINFORMATYCZNEGO | BRAK DUPLIKACJI KOMPONENTÓW

Organizacja sprawdza, czy żaden komponent autoryzowanego systemu teleinformatycznego nie jest duplikowany w wykazach komponentów innych systemów teleinformatycznych.

(6) INWENTARYZACJA KOMPONENTÓW SYSTEMU TELEINFORMATYCZNEGO | OCENA KONFIGURACJI / ZATWIERDZONE ODSTĘPSTWA

Organizacja uwzględnia w spisie komponentów systemu teleinformatycznego wszelkie dokonane konfiguracje komponentów i zatwierdzone odchylenia od obecnie stosowanych konfiguracji.

Zabezpieczenia powiązane: CM-2, CM-6.

(7) INWENTARYZACJA KOMPONENTÓW SYSTEMU TELEINFORMATYCZNEGO | SCENTRALIZOWANE REPOZYTORIUM

Organizacja zapewnia scentralizowane repozytorium spisu komponentów systemu teleinformatycznego.

(8) INWENTARYZACJA KOMPONENTÓW SYSTEMU TELEINFORMATYCZNEGO | AUTOMATYCZNE ŚLEDZENIE LOKALIZACJI

Organizacja stosuje zautomatyzowane mechanizmy do obsługi śledzenia komponentów systemu teleinformatycznego według lokalizacji geograficznej.

(9) INWENTARYZACJA KOMPONENTÓW SYSTEMU TELEINFORMATYCZNEGO | PRZYPISANIE KOMPONENTÓW DO SYSTEMÓW

Organizacja:

(a) przypisuje [*Realizacja: zdefiniowane przez organizację pozyskane elementy systemu teleinformatycznego*] do systemu teleinformatycznego;

(b) Otrzymuje potwierdzenie od właściciela systemu teleinformatycznego wykonanie tego zadania.

Zabezpieczenia powiązane: SA-4.

Zabezpieczenia powiązane: Brak

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	CM-8	CM-8 (1) (3) (5)	CM-8 (1) (2) (3) (4) (5)

CM-9 PLAN ZARZĄDZANIA KONFIGURACJĄ

Zabezpieczenie: Organizacja opracowuje, dokumentuje i wdraża plan zarządzania konfiguracją systemu teleinformatycznego, który:

a. Uwzględnia role, obowiązki oraz procesy i procedury zarządzania konfiguracją;

b. Ustanawia proces identyfikacji elementów konfiguracji w całym cyklu życia systemu i zarządzania konfiguracją elementów konfiguracyjnych;

c. Definiuje elementy konfiguracji systemu teleinformatycznego i umieszcza elementy konfiguracyjne w zarządzaniu konfiguracją;

d. Chroni plan zarządzania konfiguracją przed nieuprawnionym ujawnieniem i modyfikacją.

Zabezpieczenia powiązane: CM-2, CM-3, CM-4, CM-5, CM-8, SA-10.

Zabezpieczenia rozszerzone:

(1) PLAN ZARZĄDZANIA KONFIGURACJĄ | PRZYPISANIE ODPOWIEDZIALNOŚCI

Organizacja przypisuje odpowiedzialność za opracowanie procesu zarządzania konfiguracją pracownikom organizacji, którzy nie są bezpośrednio zaangażowani w rozwój systemu teleinformatycznego.

Zabezpieczenia powiązane: Brak

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	CM-9 (opcjonalnie)	CM-9	CM-9

CM-10 OGRANICZENIA W UŻYCIU OPROGRAMOWANIA

Zabezpieczenie: Organizacja:

a. Korzysta z oprogramowania i powiązanej dokumentacji zgodnie z postanowieniami umownymi i prawami autorskimi;

b. Śledzi wykorzystanie oprogramowania i związanej z nim dokumentacji chronionej licencjami ilościowymi w celu kontroli kopiowania i dystrybucji;

c. Kontroluje i dokumentuje użycie technologii udostępniania plików peer-to-peer, aby zapewnić, że ta funkcja nie będzie wykorzystywana do nieautoryzowanego rozpowszechniania, wyświetlania, wykonywania lub reprodukcji dzieł chronionych prawem autorskim.

Zabezpieczenia powiązane: AC-17, CM-8, SC-7.

Zabezpieczenia rozszerzone:

(1) OGRANICZENIA W UŻYCIU OPROGRAMOWANIA | OPROGRAMOWANIE OTWARTE (OPEN SOURCE)

Organizacja ustanawia następujące ograniczenia dotyczące korzystania z oprogramowania źródłowego (typu open source): [Rea*lizacja: ograniczenia zdefiniowane przez organizację*].

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P2	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	CM-10	CM-10	CM-10

CM-11 OPROGRAMOWANIE INSTALOWANE PRZEZ UŻYTKOWNIKA

Zabezpieczenie: Organizacja:

a. Ustanawia politykę [*Realizacja: zasady zdefiniowane przez organizację*] regulujące instalację oprogramowania przez użytkowników;

b. Egzekwuje zasady instalacji oprogramowania poprzez [*Realizacja: metody zdefiniowane przez organizację*];

c. Monitoruje zgodność polityki z częstotliwością [*Realizacja: częstotliwość zdefiniowana przez organizację*].

Zabezpieczenia powiązane: AC-3, CM-2, CM-3, CM-5, CM-6, CM-7, PL-4.

Zabezpieczenia rozszerzone:

(1) OPROGRAMOWANIE INSTALOWANE PRZEZ UŻYTKOWNIKA | OSTRZEGANIE O NIEAUTORYZOWANYCH INSTALACJACH

System teleinformatyczny ostrzega [*Realizacja: personel lub role zdefiniowane przez organizację*] w przypadku wykrycia nieautoryzowanej instalacji oprogramowania.

Zabezpieczenia powiązane: CA-7, SI-4.

(2) OPROGRAMOWANIE INSTALOWANE PRZEZ UŻYTKOWNIKA | ZABRONIONA INSTALACJA BEZ POSIADANIA STOSOWNYCH UPRAWNIEŃ

System teleinformatyczny zabrania instalowania oprogramowania przez użytkownika nieposiadającego statusu użytkownika uprzywilejowanego.

Zabezpieczenia powiązane: AC-6.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	CM-11	CM-11	CM-11

KATEGORIA: PLANOWANIE AWARYJNE / CIĄGŁOŚĆ DZIAŁANIA

CP-1 POLITYKA I PROCEDURY PLANOWANIA CIĄGŁOŚCI DZIAŁANIA

Zabezpieczenie: Organizacja:

a. Opracowuje, dokumentuje i rozpowszechnia w odniesieniu do [*Realizacja: personel lub role zdefiniowane przez organizację*]:

   1. Politykę planowania awaryjnego, która dotyczy celu, zakresu, ról, obowiązków, zaangażowania kierownictwa, koordynacji między jednostkami organizacyjnymi oraz ich podatności;

   2. Procedury ułatwiające wdrożenie polityki planowania awaryjnego i powiązane zabezpieczenia planowania awaryjnego;

b. Przegląda i aktualizuje aktualne:

   1. Politykę planowania awaryjnego z częstotliwością [*Realizacja: częstotliwość określona przez organizację*];

   2. Procedury planowania awaryjnego z częstotliwością [*Realizacja: częstotliwość określona przez organizację*].

Zabezpieczenia powiązane: PM-9.

Zabezpieczenia rozszerzone: Brak.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	CP-1	CP-1	CP-1

CP-2 PLAN CIĄGŁOŚCI DZIAŁANIA

Zabezpieczenie: Organizacja:

a. Opracowuje plan awaryjny dotyczący systemu teleinformatycznego, który:
   1. Identyfikuje podstawowe funkcje biznesowe oraz powiązane działania awaryjne;
   2. Zapewnia cele odzyskiwania, priorytety przywracania i ich parametry[27];
   3. Adresuje role awaryjne i obowiązki, przypisuje osoby z danymi kontaktowymi;
   4. Zajmuje się utrzymywaniem podstawowych misji i funkcji biznesowych pomimo wystąpienia zakłócenia, incydentu lub awarii systemu teleinformatycznego;
   5. Wskazuje środki prowadzące do końcowego pełnego przywrócenia systemu teleinformatycznego bez pogorszenia pierwotnie zaplanowanych i wdrożonych zabezpieczeń;
   6. Jest weryfikowany i zatwierdzany przez [*Realizacja: personel lub role zdefiniowane przez organizację*];
b. Przekazuje kopie planu awaryjnego do [*Realizacja: kluczowy personel zdefiniowany przez organizację do działań awaryjnych (identyfikowany według nazwiska i / lub roli) oraz elementy organizacyjne*];
c. Koordynuje działania związane z planowaniem awaryjnym z działaniami związanymi z incydentami;
d. Przegląda plan awaryjny systemu teleinformatycznego z częstotliwością [*Realizacja: częstotliwość określona przez organizację*];
e. Aktualizuje plan awaryjny w celu uwzględnienia zmian w organizacji, systemie teleinformatycznym lub środowisku działania oraz problemów napotkanych podczas wdrażania, wykonywania lub testowania planu awaryjnego;
f. Ogłasza zmiany planu awaryjnego [*Realizacja: kluczowy personel awaryjny zdefiniowany przez organizację (identyfikowany według nazwiska i / lub roli) oraz elementy organizacyjne*];
g. Chroni plan awaryjny przed nieuprawnionym ujawnieniem i modyfikacją.

Zabezpieczenia powiązane: AC-14, CP-6, CP-7, CP-8, CP-9, CP-10, IR-4, IR-8, MP-2, MP-4, MP-5, PM-8 , PM-11.

[27] Np. wartości Recovery Point Objective (RPO) - pozwala określić częstotliwość wykonywania backupu, co w praktyce oznacza okres czasu, za jaki następuje utrata danych, oraz Recovery Time Objective (RTO) - czas potrzebny do przywrócenia systemu do pracy, w tym do odzyskania danych.

Zabezpieczenia rozszerzone:

(1) PLAN CIĄGŁOŚCI DZIAŁANIA | KOORDYNACJA Z POWIĄZANYMI PLANAMI

Organizacja koordynuje opracowywanie planów awaryjnych z jednostkami organizacyjnymi odpowiedzialnymi za opracowywanie spokrewnionych planów (np. plany ciągłości działania, plany odzyskiwania po awarii, plany ciągłości operacji, plany komunikacji kryzysowej, plany ochrony infrastruktury krytycznej, plany reagowania na incydenty komputerowe, plany przeciwdziałania zagrożeniom wewnętrznym).

(2) PLAN CIĄGŁOŚCI DZIAŁANIA | PLANOWANIE ZDOLNOŚCI FUNKCJONOWANIA

Organizacja prowadzi planowanie zdolności funkcjonowania tak, aby podczas stanów awaryjnych istniała niezbędna zdolność do przetwarzania informacji, telekomunikacji i wsparcia środowiskowego.

(3) PLAN CIĄGŁOŚCI DZIAŁANIA | WZNAWIANIE PODSTAWOWYCH DZIAŁAŃ / FUNKCJI BIZNESOWYCH

Organizacja planuje wznowienie podstawowych działań i funkcji biznesowych w ciągu [*Realizacja: okres zdefiniowany przez organizację*] od momentu aktywacji planu awaryjnego.

Zabezpieczenia powiązane: PE-12.

(4) PLAN CIĄGŁOŚCI DZIAŁANIA | PRZYWRÓCENIE DZIAŁANIA WSZYSTKICH FUNKCJI BIZNESOWYCH

Organizacja planuje wznowienie wszystkich misji i funkcji biznesowych w ciągu [*Realizacja: okres zdefiniowany przez organizację*] od momentu aktywacji planu awaryjnego.

Zabezpieczenia powiązane: PE-12.

(5) PLAN CIĄGŁOŚCI DZIAŁANIA | KONTYNUACJA NIEZBĘDNYCH DZIAŁAŃ / FUNKCJI BIZNESOWYCH

Organizacja planuje kontynuację podstawowych (niezbędnych) działań i funkcji biznesowych z minimalną ciągłością operacyjną lub bez jej utraty i utrzymuje tą ciągłość aż do pełnego przywrócenia pierwotnego działania systemu teleinformatycznego.

Zabezpieczenia powiązane: PE-12.

(6) PLAN CIĄGŁOŚCI DZIAŁANIA | PROCESY ALTERNATYWNE / ZAPASOWE MIEJSCA PRZETWARZANIA

Organizacja planuje przeniesienie niezbędnych procesów funkcjonowania i funkcji biznesowych do alternatywnych miejsc przetwarzania i / lub przechowywania z minimalną ciągłością operacyjną lub bez jej utraty i utrzymuje takie funkcjonowanie systemu do momentu możliwości przywrócenia systemu teleinformatycznego do pierwotnych miejsc przetwarzania i / lub przechowywania.

Zabezpieczenia powiązane: PE-12.

(7) PLAN CIĄGŁOŚCI DZIAŁANIA | KOORDYNACJA Z USŁUGODAWCAMI ZEWNĘTRZNYMI

Organizacja koordynuje swój plan awaryjny z planami awaryjnymi zewnętrznych dostawców usług, celem zapewnienia spełnienia wymagań ciągłości działania.

Zabezpieczenia powiązane: SA-9.

(8) PLAN CIĄGŁOŚCI DZIAŁANIA | IDENTYFIKACJA ZASOBÓW KRYTYCZNYCH

Organizacja identyfikuje zasoby krytycznego systemu teleinformatycznego wspierające podstawowe działania i funkcje biznesowe.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	CP-2	CP-2 (1) (3) (8)	CP-2 (1) (2) (3) (4) (5) (8)

CP-3 SZKOLENIE W ZAKRESIE PLANOWANIA CIĄGŁOŚCI DZIAŁANIA

Zabezpieczenie: Organizacja zapewnia użytkownikom systemów teleinformatycznych szkolenia w zakresie planowania ciągłości działania na wypadek awarii, zgodnie z przypisanymi rolami i obowiązkami:

a. W ciągu [*Realizacja: okres zdefiniowany przez organizację*] od przyjęcia roli lub odpowiedzialności w zakresie planowania ciągłości działania;

b. W przypadku wystąpienia zmian konfiguracji systemu teleinformatycznego;

c. Z częstotliwością [Realizacja: częstotliwość określona przez organizację w danym okresie czasowym].

Zabezpieczenia powiązane: AT-2, AT-3, CP-2, IR-2.

Zabezpieczenia rozszerzone:

(1) SZKOLENIE W ZAKRESIE PLANOWANIA CIĄGŁOŚCI DZIAŁANIA | WYDARZENIA SYMULOWANE

Organizacja wprowadza symulowane zdarzenia do szkolenia w zakresie planowania ciągłości działania, celem ułatwienia skutecznego reagowania personelu w sytuacjach kryzysowych.

(2) SZKOLENIE W ZAKRESIE PLANOWANIA CIĄGŁOŚCI DZIAŁANIA| ZAUTOMATYZOWANE ŚRODOWISKA SZKOLENIOWE

Organizacja stosuje zautomatyzowane mechanizmy zapewniające wszechstronne i realistyczne środowisko szkolenia w zakresie planowania ciągłości działania.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P2	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	CP-3	CP-3	CP-3 (1)

CP-4 TESTOWANIE PLANU CIĄGŁOŚCI DZIAŁANIA

Zabezpieczenie: Organizacja:

a. Testuje plan awaryjny danego systemu teleinformatycznego z częstotliwością [*Realizacja: częstotliwość zdefiniowana przez organizację*] przy użyciu [*Realizacja: testy zdefiniowane przez organizację*] w celu ustalenia skuteczności planu i gotowości organizacyjnej do wykonania planu;

b. Przegląda wyniki testu planu awaryjnego;

c. W razie potrzeby inicjuje działania korygujące i / lub naprawcze.

Zabezpieczenia powiązane: CP-2, CP-3, IR-3.

Zabezpieczenia rozszerzone:

(1) TESTOWANIE PLANU CIĄGŁOŚCI DZIAŁANIA | KOORDYNACJA Z POWIĄZANYMI PLANAMI

Organizacja koordynuje testowanie planów awaryjnych z jednostkami organizacyjnymi odpowiedzialnymi za powiązane plany.

Zabezpieczenia powiązane: IR-8, PM-8.

(2) TESTOWANIE PLANU CIĄGŁOŚCI DZIAŁANIA | ZAPASOWE MIEJSCE PRZETWARZANIA

Organizacja testuje plan awaryjny w zapasowym miejscu przetwarzania:

(a) W celu zapoznania personelu przeznaczonego do działań w trybie awaryjnym z obiektami i dostępnymi zasobami organizacji;

(b) Oceny możliwości zapasowego miejsca przetwarzania do obsługi operacji awaryjnych.

Zabezpieczenia powiązane: CP-7.

(3) TESTOWANIE PLANU CIĄGŁOŚCI DZIAŁANIA | TESTOWANIE AUTOMATYCZNE

Organizacja wykorzystuje zautomatyzowane mechanizmy wszechstronnego i skutecznego testowania planu awaryjnego.

(4) TESTOWANIE PLANU CIĄGŁOŚCI DZIAŁANIA | PEŁNE ODZYSKIWANIE / ODTWARZANIE

Organizacja przeprowadza pełne przywrócenie i odtworzenie systemu teleinformatycznego do pierwotnego stanu w ramach testowania planu awaryjnego.

Zabezpieczenia powiązane: CP-10, SC-24.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P2	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	CP-4	CP-4 (1)	CP-4 (1) (2)

CP-5 AKTUALIZACJA PLANU CIĄGŁOŚCI DZIAŁANIA

[Włączony do CP-2].

CP-6 ZAPASOWE MIEJSCE PRZECHOWYWANIA KOPII

Zabezpieczenie: Organizacja:

a. Ustanawia alternatywne miejsce przechowywania, w tym podpisuje niezbędne umowy umożliwiające przechowywanie i wyszukiwanie informacji o kopii zapasowej systemu teleinformatycznego;

b. Zapewnia, że alternatywne miejsce przechowywania zapewnia środki bezpieczeństwa informacji równoważne z zabezpieczeniami stosowanymi w miejscu głównym (podstawowym).

Zabezpieczenia powiązane: CP-2, CP-7, CP-9, CP-10, MP-4.

Zabezpieczenia rozszerzone:

(1) ZAPASOWE MIEJSCE PRZECHOWYWANIA KOPII | SEPARACJA OD MIEJSCA GŁÓWNEGO

Organizacja identyfikuje zapasowe miejsce przetwarzania / przechowywania, które jest oddzielone od głównego miejsca, celem zmniejszenia podatności na oddziaływanie tego samego rodzaju zagrożenia.

Zabezpieczenia powiązane: RA-3.

(2) ZAPASOWE MIEJSCE PRZECHOWYWANIA KOPII | CZAS ODZYSKIWANIA / CELE PUNKTOWE

Organizacja konfiguruje alternatywne miejsce przechowywania, aby ułatwić operacje odzyskiwania zgodnie z czasem odzyskiwania (RTO) i celami punktu odtworzenia (RPO).

(3) ZAPASOWE MIEJSCE PRZECHOWYWANIA KOPII | DOSTĘPNOŚĆ

Organizacja identyfikuje potencjalne problemy z dostępnością do alternatywnego miejsca przetwarzania / przechowywania w przypadku zakłócenia lub katastrofy na całym obszarze i określa jednoznaczne działania minimalizujące.

Zabezpieczenia powiązane: RA-3.

Zabezpieczenia powiązane: Brak

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	CP-6 (opcjonalnie)	CP-6 (1) (3)	CP-6 (1) (2) (3)

CP-7 ZAPASOWE MIEJSCE PRZETWARZANIA

Zabezpieczenie: Organizacja:

a. Ustanawia alternatywne miejsce przetwarzania, w tym podpisuje niezbędne umowy w celu umożliwienia przeniesienia i wznowienia [*Realizacja: operacje systemu teleinformatycznego zdefiniowanego przez organizację] dla niezbędnych misji / funkcji biznesowych*] w czasie [*Realizacja: okres zdefiniowany przez organizację zgodny z czasem odzyskiwania i celami punktu odzyskiwania*], w przypadku niedostępności podstawowej możliwości przetwarzania;

b. Zapewnia, że sprzęt i materiały wymagane do przeniesienia i wznowienia operacji są dostępne w alternatywnym miejscu przetwarzania lub, że istnieją umowy wspierające dostawę do tego miejsca w wyznaczonym przez organizację terminie transferu / wznowienia;

c. Zapewnia, że alternatywna miejsce przetwarzania zapewnia środki bezpieczeństwa informacji równoważne z zabezpieczeniami stosowanymi w miejscu głównym (podstawowym).

Zabezpieczenia powiązane: CP-2, CP-6, CP-8, CP-9, CP-10, MA-6.

Zabezpieczenia rozszerzone:

(1) ZAPASOWE MIEJSCE PRZETWARZANIA | ODSEPAROWANIE OD LOKALIZACJI PODSTAWOWEJ

Organizacja identyfikuje alternatywne miejsce przetwarzania, które jest oddzielone od głównego miejsca przetwarzania, celem zmniejszenia podatności na oddziaływanie tych samych zagrożeń.

Zabezpieczenia powiązane: RA-3.

(2) ZAPASOWE MIEJSCE PRZETWARZANIA | DOSTĘPNOŚĆ

Organizacja identyfikuje potencjalne problemy z dostępnością do alternatywnego miejsca przetwarzania w przypadku zagrożenia lub katastrofy na całym obszarze i określa jednoznaczne działania minimalizujące**.**

Zabezpieczenia powiązane: RA-3.

(3) ZAPASOWE MIEJSCE PRZETWARZANIA | PRIORYTET USŁUG

Organizacja opracowuje alternatywne umowy dotyczące lokalizacji przetwarzania, które zawierają postanowienia dotyczące priorytetowego świadczenia usług zgodnie z wymogami dostępności organizacji (w tym z celami dotyczącymi czasu odzyskiwania).

(4) ZAPASOWE MIEJSCE PRZETWARZANIA | GOTOWOŚĆ DO UŻYCIA

Organizacja przygotowuje alternatywne miejsce przetwarzania, dzięki czemu jest ono gotowe do użycia jako miejsce operacyjne obsługujące podstawowe działania i funkcje biznesowe.

Zabezpieczenia powiązane: CM-2, CM-6.

(5) ZAPASOWE MIEJSCE PRZETWARZANIA | RÓWNOWAŻNE ŚRODKI BEZPIECZEŃSTWA

[Włączone do CP-7].

(6) ZAPASOWE MIEJSCE PRZETWARZANIA | BRAK MOŻLIWOŚCI POWROTU DO LOKALIZACJI PODSTAWOWEJ

Organizacja planuje i przygotowuje się na okoliczności uniemożliwiające powrót do głównego miejsca przetwarzania.

Zabezpieczenia powiązane: Brak

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	CP-7 (opcjonalnie)	CP-7 (1) (2) (3)	CP-7 (1) (2) (3) (4)

CP-8 USŁUGI TELEKOMUNIKACYJNE

Zabezpieczenie: Organizacja ustanawia alternatywne usługi telekomunikacyjne, w tym niezbędne umowy zabezpieczające te usługi, celem umożliwienia wznowienia [*Realizacja: działania systemu teleinformatycznego zdefiniowanego przez organizację*] niezbędnych działań i funkcji biznesowych w czasie [*Realizacja: okres zdefiniowany przez organizację*], w przypadku niedostępności podstawowych możliwości telekomunikacyjne w głównym lub alternatywnym miejscu przetwarzania lub przechowywania.

Zabezpieczenia powiązane: CP-2, CP-6, CP-7.

Zabezpieczenia rozszerzone:

(1) USŁUGI TELEKOMUNIKACYJNE | PRIORYTETY ŚWIADCZENIA USŁUG

Organizacja:

(a) Opracowuje podstawowe i alternatywne umowy o świadczenie usług telekomunikacyjnych, które zawierają postanowienia dotyczące pierwszeństwa świadczenia usług zgodnie z wymogami dostępności określonymi przez organizację (w tym celami dotyczącymi czasu odzyskiwania - RTO);

(b) Żąda zapewnienia pierwszeństwa usługi telekomunikacyjnej dla wszystkich usług telekomunikacyjnych wykorzystywanych w celu zapewnienia, w przypadku wystąpienia awarii, wykonywania obowiązków na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego w sytuacji, gdy podstawowe i / lub alternatywne usługi telekomunikacyjne są świadczone przez wspólnego operatora.

(2) USŁUGI TELEKOMUNIKACYJNE | POJEDYNCZE PUNKTY AWARII

Organizacja ustanawia alternatywne usługi telekomunikacyjne w celu zmniejszenia prawdopodobieństwa wpływu jednostkowej awarii na świadczenie podstawowych usług telekomunikacyjnych.

(3) USŁUGI TELEKOMUNIKACYJNE | ROZDZIELENIE DOSTAWCÓW PODSTAWOWYCH / ALTERNATYWNYCH

Organizacja nabywa alternatywne usługi telekomunikacyjne od dostawców, którzy nie są powiązani z głównym dostawcą usług dla organizacji, celem zmniejszenia podatność na oddziaływanie tych samych zagrożeń w stosunku do usług telekomunikacyjnych.

(4) USŁUGI TELEKOMUNIKACYJNE | PLAN AWARYJNY DOSTAWCY

Organizacja:

(a) Wymaga, aby podstawowi i alternatywni dostawcy usług telekomunikacyjnych posiadali plany awaryjne;

(b) Dokonuje przeglądu planów awaryjnych dostawcy, aby upewnić się, że plany spełniają stawiane przez organizację wymogi dotyczące awaryjności;

(c) Uzyskuje dowody przeprowadzania przez dostawców testów / szkoleń planowania ciągłości działania na wypadek awarii z częstotliwością [*Realizacja: częstotliwość określona przez organizację*].

(5) USŁUGI TELEKOMUNIKACYJNE | ALTERNATYWNE TESTOWANIE USŁUG TELEKOMUNIKACYJNYCH

Organizacja testuje alternatywne usługi telekomunikacyjne z częstotliwością [*Realizacja: częstotliwość zdefiniowana przez organizację*].

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	CP-8 (opcjonalnie)	CP-8 (1) (2)	CP-8 (1) (2) (3) (4)

CP-9 KOPIA ZAPASOWA

Zabezpieczenie: Organizacja:

a. Wykonuje kopie zapasowe informacji na poziomie użytkownika, przetwarzanych w systemie teleinformatycznym z częstotliwością [*Realizacja: częstotliwość określona przez organizację zgodnie z czasem odzyskiwania i celami punktu odzyskiwania*];

b. Wykonuje kopie zapasowe informacji na poziomie systemu, przetwarzanych w systemie teleinformatycznym z częstotliwością [*Realizacja: częstotliwość określona przez organizację, zgodna z czasem odzyskiwania i celami punktu odzyskiwania*];

c. Wykonuje kopie zapasowe dokumentacji, w tym dokumentacji związanej z bezpieczeństwem z częstotliwością [*Realizacja: częstotliwość określona przez organizację zgodnie z czasem odzyskiwania i celami punktu odzyskiwania*];

d. Zapewnia poufność, integralność i dostępność kopii zapasowych w miejscach przechowywania.

Zabezpieczenia powiązane: CP-2, CP-6, MP-4, MP-5, SC-13.

Zabezpieczenia rozszerzone:

(1) KOPIA ZAPASOWA | BADANIE NIEZAWODNOŚCI NOŚNIKÓW / INTEGRALNOŚCI INFORMACJI

Organizacja testuje kopie zapasowe informacje z częstotliwością [*Realizacja: częstotliwość zdefiniowana przez organizację*], celem zweryfikowania niezawodność nośników danych i integralność informacji.

Zabezpieczenia powiązane: CP-4.

(2) KOPIA ZAPASOWA | TESTY ODTWORZENIOWE Z WYKORZYSTANIEM PRÓBEK DANYCH

Organizacja wykorzystuje próbkę informacji zapasowych w celu przywrócenia wybranych funkcji systemu teleinformatycznego w ramach testowania planu awaryjnego.

Zabezpieczenia powiązane: CP-4.

(3) KOPIA ZAPASOWA | SEPARACJA PRZECHOWYWANIA INFORMACJI KRYTYCZNYCH

Organizacja przechowuje kopie zapasowe [*Realizacja: zdefiniowane przez organizację oprogramowanie systemu informacji krytycznych i inne informacje związane z bezpieczeństwem*] w oddzielnym obiekcie lub w ognioodpornym kontenerze, który nie jest umieszczony razem z bieżącym systemem.

Zabezpieczenia powiązane: CM-2, CM-8.

(4) KOPIA ZAPASOWA | OCHRONA PRZED NIEAUTORYZOWANĄ MODYFIKACJĄ

[Włączono do CP-9].

(5) KOPIA ZAPASOWA | PRZEKAZANIE KOPII DO ALTERNATYWNEJ LOKALIZACJI

Organizacja przekazuje kopię zapasową systemu teleinformatycznego do alternatywnego miejsca przechowywania [*Realizacja: okres zdefiniowany przez organizację i szybkość transferu zgodna z czasem odzyskiwania i celami punktu odzyskiwania*].

(6) KOPIA ZAPASOWA | REDUNDANCJA (NADMIAROWOŚĆ) SYSTEMU

Organizacja wykonuje kopię zapasową systemu teleinformatycznego, utrzymując redundantny system wtórny, który nie jest kolokowany z systemem podstawowym i który można aktywować bez utraty informacji lub zakłócenia operacji.

Zabezpieczenia powiązane: CP-7, CP-10.

(7) KOPIA ZAPASOWA | PODWÓJNA AUTORYZACJA

Organizacja wymusza podwójną autoryzację w celu usunięcia lub zniszczenia [*Realizacja: informacje o kopii zapasowej zdefiniowane przez organizację*].

Podwójna autoryzacja zapewnia, że usunięcie lub zniszczenie danych kopii zapasowej nie będzie możliwe, chyba że dwie wykwalifikowane osoby wykonają zadanie. Osoby usuwające / niszczące informacje z kopii zapasowej posiadają wystarczające umiejętności / wiedzę specjalistyczną, aby ustalić, czy proponowane usunięcie / zniszczenie informacji o kopii zapasowej odzwierciedla zasady i procedury organizacyjne. Podwójna autoryzacja może być również znana jako kontrola dwuosobowa.

Zabezpieczenia powiązane: AC-3, MP-2.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	CP-9	CP-9 (1)	CP-9 (1) (2) (3) (5)

CP-10 ODZYSKIWANIE I ODTWARZANIE SYSTEMU

Zabezpieczenie: Organizacja zapewnia przywracanie i odtwarzanie systemu teleinformatycznego do znanego stanu przed zakłóceniem lub awarią.

Zabezpieczenia powiązane: CA-2, CA-6, CA-7, CP-2, CP-6, CP-7, CP-9, SC-24.

Zabezpieczenia rozszerzone:

(1) ODZYSKIWANIE I ODTWARZANIE SYSTEMU | TESTOWANIE PLANU AWARYJNEGO

[Włączone do CP-4].

(2) ODZYSKIWANIE I ODTWARZANIE SYSTEMU | ODTWARZANIE TRANSAKCJI

System teleinformatyczny posiada zdolność odtwarzania transakcji[28] w systemach opartych na transakcjach[29].

Systemy informacyjne oparte na transakcjach obejmują na przykład systemy zarządzania bazami danych i systemy przetwarzania transakcji. Mechanizmy wspierające odzyskiwanie transakcji obejmują na przykład wycofywanie transakcji i księgowanie transakcji.

(3) ODZYSKIWANIE I ODTWARZANIE SYSTEMU | KOMPENSACYJNE ŚRODKI BEZPIECZEŃSTWA

[Wycofane].

(4) ODZYSKIWANIE I ODTWARZANIE SYSTEMU | PRZYWRACANIE W OKREŚLONYM PRZEDZIALE CZASOWYM

Organizacja zapewnia możliwość przywracania komponentów systemu teleinformatycznego w przedziale czasowym [*Realizacja: okresy przywracania zdefiniowane przez organizację*] z informacji kontrolowanych przez konfigurację i chronionych pod kątem integralności, reprezentujących znany stan operacyjny komponentów.

Zabezpieczenia powiązane: CM-2.

(5) ODZYSKIWANIE I ODTWARZANIE SYSTEMU | PRACE AWARYJNE

[Włączono do SI-13].

(6) ODZYSKIWANIE I ODTWARZANIE SYSTEMU | OCHRONA KOMPONENTÓW

Organizacja chroni sprzęt do tworzenia kopii zapasowych i przywracania, oprogramowanie układowe (firmware) i oprogramowanie aplikacyjne (software).

Zabezpieczenia powiązane: AC-3, AC-6, PE-3.

[28] Systemy informacyjne oparte na transakcjach obejmują np. systemy zarządzania bazami danych i systemy przetwarzania transakcji.

[29] Mechanizmy wspierające odzyskiwanie transakcji obejmują np. wycofywanie transakcji i księgowanie transakcji.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	CP-10	CP-10 (2)	CP-10 (2) (4)

CP-11 ALTERNATYWNE PROTOKOŁY KOMUNIKACJI

Zabezpieczenie: W celu utrzymania ciągłości działania system teleinformatyczny umożliwia wykorzystanie [*Realizacja: zdefiniowane przez organizację alternatywne protokoły komunikacyjne*].

Zabezpieczenia rozszerzone: Brak.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P0	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	CP-11 (opcjonalnie)	CP-11 (opcjonalnie)	CP-11 (opcjonalnie)

CP-12 TRYB BEZPIECZNY

Zabezpieczenie: System teleinformatyczny po wykryciu [*Realizacja: warunki zdefiniowane przez organizację*] wchodzi w bezpieczny tryb pracy ograniczony do [*Realizacja: ograniczenia dotyczące bezpiecznego trybu działania określone przez organizację*].

Zabezpieczenia rozszerzone: Brak.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P0	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	CP-12 (opcjonalnie)	CP-12 (opcjonalnie)	CP-12 (opcjonalnie)

CP-13 ALTERNATYWNE MECHANIZMY BEZPIECZEŃSTWA

Zabezpieczenie: Organizacja stosuje [*Realizacja: zdefiniowane przez organizację alternatywne lub uzupełniające mechanizmy bezpieczeństwa*] w celu spełnienia [*Realizacja: funkcje bezpieczeństwa zdefiniowane przez organizację*], w przypadku gdy podstawowe środki implementacji funkcji bezpieczeństwa są niedostępne lub zagrożone.

Zabezpieczenia powiązane: CP-2.

Zabezpieczenia rozszerzone: Brak.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P0	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	CP-13 (opcjonalnie)	CP-13 (opcjonalnie)	CP-13 (opcjonalnie)

KATEGORIA: IDENTYFIKACJA I UWIERZYTELNIANIE

IA-1 IDENTYFIKACJA I UWIERZYTELNIANIE – POLITYKA I PROCEDURY

Zabezpieczenie: Organizacja:

a. Opracowuje, dokumentuje i rozpowszechnia w odniesieniu do [*Realizacja: personel lub role zdefiniowane przez organizację*]:

   1. Politykę identyfikacji i uwierzytelniania uwzględniającą cel, zakres, role, obowiązki, zaangażowanie kierownictwa, koordynację między jednostkami organizacyjnymi oraz ich podatności;

   2. Procedury ułatwiające wdrożenie polityki identyfikacji i uwierzytelniania oraz powiązane zabezpieczenia identyfikacji i uwierzytelnienia;

b. Przegląda i aktualizuje ustawienia aktualnej:

   1. Polityki identyfikacji i uwierzytelniania z częstotliwością *[Realizacja: częstotliwość określona przez organizację*];

   2. Procedury identyfikacji i uwierzytelnienia z częstotliwością [*Realizacja: częstotliwość określona przez organizację*].

Zabezpieczenia powiązane: PM-9.

Zabezpieczenia rozszerzone: Brak.

Zabezpieczenia powiązane: Brak

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	IA-1	IA-1	IA-1

IA-2 IDENTYFIKACJA I UWIERZYTELNIANIE (UŻYTKOWNICY ORGANIZACYJNI)

Zabezpieczenie: System teleinformatyczny jednoznacznie identyfikuje i uwierzytelnia użytkowników organizacji (lub procesy działające w imieniu użytkowników organizacji).

Zabezpieczenia powiązane: AC-2, AC-3, AC-14, AC-17, AC-18, IA-4, IA-5, IA-8.

Zabezpieczenia rozszerzone:

(1) IDENTYFIKACJA I UWIERZYTELNIENIE | DOSTĘP SIECIOWY Z KONT UPRZYWILEJOWANYCH

System teleinformatyczny implementuje uwierzytelnianie wieloskładnikowe w celu uzyskania dostępu sieciowego z kont uprzywilejowanych.

Zabezpieczenia powiązane: AC-6.

(2) IDENTYFIKACJA I UWIERZYTELNIENIE | DOSTĘP SIECIOWY Z KONT NIEUPRZYWILEJOWANYCH

System teleinformatyczny implementuje uwierzytelnianie wieloskładnikowe w celu uzyskania dostępu sieciowego z kont nieuprzywilejowanych.

(3) IDENTYFIKACJA I UWIERZYTELNIENIE | DOSTĘP LOKALNY Z KONT UPRZYWILEJOWANYCH

System teleinformatyczny implementuje uwierzytelnianie wieloskładnikowe celu uzyskania lokalnego dostępu z kont uprzywilejowanych.

Zabezpieczenia powiązane: AC-6.

(4) IDENTYFIKACJA I UWIERZYTELNIENIE | DOSTĘP LOKALNY Z KONT NIEUPRZYWILEJOWANYCH

System teleinformatyczny implementuje uwierzytelnianie wieloskładnikowe dla lokalnego dostępu z kont nieuprzywilejowanych.

(5) IDENTYFIKACJA I UWIERZYTELNIENIE | AUTORYZACJA GRUPY

Organizacja wymaga uwierzytelniania indywidualnych użytkowników logujących się do zasobów współużytkowanych przez grupę użytkowników, za pomocą indywidualnego identyfikatora przydzielonego tej osobie.

(6) IDENTYFIKACJA I UWIERZYTELNIENIE | DOSTĘP SIECIOWY Z KONT UPRZYWILEJOWANYCH – ODSEPAROWANE URZĄDZENIE

System teleinformatyczny implementuje uwierzytelnianie wieloskładnikowe w celu uzyskania dostępu sieciowego z kont uprzywilejowanych. Urządzenie uwierzytelniające dostęp do systemu jest odseparowane od systemu udzielającego dostępu i urządzenie to spełnia [*Realizacja: organizacja określa wymagania dotyczące mechanizmu uwierzytelniania*].

Zabezpieczenia powiązane: AC-6.

(7) IDENTYFIKACJA I UWIERZYTELNIENIE | DOSTĘP SIECIOWY Z KONT NIEUPRZYWILEJOWANYCH – ODSEPAROWANE URZĄDZENIE

System teleinformatyczny implementuje uwierzytelnianie wieloskładnikowe w celu uzyskania dostępu sieciowego z nieuprzywilejowanych kont. Urządzenie uwierzytelniające dostęp do systemu jest odseparowane od systemu i urządzenie to spełnia [*Realizacja: organizacja określa wymagania dotyczące mechanizmu uwierzytelniania*].

(8) IDENTYFIKACJA I UWIERZYTELNIENIE | DOSTĘP SIECIOWY Z KONT UPRZYWILEJOWANYCH – ODPORNOŚĆ NA POWTARZANIE

System teleinformatyczny implementuje odporne na powtarzanie mechanizmy uwierzytelniania dostępu sieciowego z uprzywilejowanych kont .

(9) IDENTYFIKACJA I UWIERZYTELNIENIE | DOSTĘP SIECIOWY Z KONT NIEUPRZYWILEJOWANYCH – ODPORNOŚĆ NA POWTARZANIE

System teleinformatyczny implementuje odporne na powtarzanie mechanizmy uwierzytelniania dostępu sieciowego z nieuprzywilejowanych kont.

(10) IDENTYFIKACJA I UWIERZYTELNIENIE | LOGOWANIE POJEDYNCZE (Single Sign-On)

System teleinformatyczny zapewnia możliwość pojedynczego logowania w celu uzyskania dostępu do *[Realizacja: konta i usługi systemu teleinformatycznego zdefiniowane przez organizację*].

(11) IDENTYFIKACJA I UWIERZYTELNIENIE | ZDALNY DOSTĘP - ODSEPAROWANE URZĄDZENIE

System teleinformatyczny implementuje uwierzytelnianie wieloskładnikowe na potrzeby zdalnego dostępu do kont uprzywilejowanych i nieuprzywilejowanych. Urządzenie uwierzytelniające dostęp do systemu jest odseparowane od systemu i urządzenie to spełnia [*Realizacja: organizacja określa wymagania dotyczące mechanizmu i siły uwierzytelniania*].

Zabezpieczenia powiązane: AC-6.

(12) IDENTYFIKACJA I UWIERZYTELNIENIE | AUTORYZACJA DANYCH DOSTĘPOWYCH

System teleinformatyczny akceptuje i elektronicznie weryfikuje dane identyfikacyjne karty dostępowej.

Zabezpieczenia powiązane: AU-2, PE-3, SA-4.

(13) IDENTYFIKACJA I UWIERZYTELNIENIE | UWIERZYTELNIANIE ”POZA PASMEM” (Z WYKORZYSTANIEM DWÓCH ODDZIELNYCH ŚCIEŻEK)

System teleinformatyczny implementuje [*Realizacja: uwierzytelnianie „poza pasmem” (OUT-OF-BAND)[30] zdefiniowane przez organizację*] w [*Realizacja: warunki zdefiniowane przez organizację*].

Zabezpieczenia powiązane: IA-10, IA-11, SC-37.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	IA-2 (1) (12)	IA-2 (1) (2) (3) (8) (11) (12)	IA-2 (1) (2) (3) (4) (8) (9) (11) (12)

[30] Uwierzytelnianie „poza pasmem” OUT-OF-BAND (OOBA) odnosi się do zastosowania dwóch oddzielnych ścieżek komunikacyjnych do identyfikacji i uwierzytelnienia użytkowników lub urządzeń w systemie teleinformatycznym.

IA-3 IDENTYFIKACJA I UWIERZYTELNIANIE URZĄDZENIA

Zabezpieczenie: System teleinformatyczny jednoznacznie identyfikuje i uwierzytelnia [*Realizacja: określone konfiguracje i / lub typy urządzeń zdefiniowane przez organizację*] przed ustanowieniem [*Wybór (jeden lub więcej): dostęp lokalny, zdalny, sieciowy*).

Zabezpieczenia powiązane: AC-17, AC-18, AC-19, CA-3, IA-4, IA-5.

Zabezpieczenia rozszerzone:

(1) IDENTYFIKACJA I UWIERZYTELNIENIE URZĄDZENIA | DWUKIERUNKOWE UWIERZYTELNIANIE KRYPTOGRAFICZNE

System teleinformatyczny uwierzytelnia [*Realizacja: określone urządzenia i / lub typy urządzeń zdefiniowane przez organizację*] przed ustanowieniem [*Wybór (jeden lub więcej): dostęp lokalny; zdalny; sieciowy*] połączenia przy użyciu uwierzytelniania dwukierunkowego[31] opartego na kryptografii.

Zabezpieczenia powiązane: SC-8, SC-12, SC-13.

(2) IDENTYFIKACJA I UWIERZYTELNIENIE URZĄDZENIA | DWUKIERUNKOWE SIECIOWE UWIERZYTELNIANIE KRYPTOGRAFICZNE

[Włączono do IA-3 (1)].

(3) IDENTYFIKACJA I AUTORYZACJA URZĄDZENIA | ALOKACJA ADRESU DYNAMICZNEGO

Organizacja:

(a) Standaryzuje informacje przydziału adresów dynamicznych i czas trwania dzierżawy przypisany do urządzeń zgodnie z [*Realizacja: informacje o dzierżawie zdefiniowane przez organizację oraz czas trwania dzierżawy*];

(b) Audytuje informacje o dzierżawie adresów dynamicznych, przypisanych do urządzenia.

Zabezpieczenia powiązane: AU-2, AU-3, AU-6, AU-12.

(4) IDENTYFIKACJA I UWIERZYTELNIENIE URZĄDZENIA | ATESTACJA URZĄDZENIA

Organizacja zapewnia, że atestowane urządzenia identyfikacji i uwierzytelniana są obsługiwane przez [*Realizacja: proces zarządzania konfiguracją zdefiniowany przez organizację*].

[31] Uwierzytelnianie dwukierunkowe – polega na kolejnym lub jednoczesnym uwierzytelnieniu obu podmiotów (które są wzajemnie i naprzemiennie uwierzytelnianym oraz uwierzytelniającym).

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	IA-3 (opcjonalnie)	IA-3	IA-3

IA-4 ZARZĄDZANIE IDENTYFIKATOREM

Zabezpieczenie: Organizacja zarządza identyfikatorami systemu teleinformatycznego poprzez:

a. Uzyskiwanie autoryzacji od [*Realizacja: personel lub role zdefiniowane przez organizację*] w celu przypisania unikalnego identyfikatora osobie, grupie, roli lub urządzeniu;

b. Wybieranie identyfikatora, który identyfikuje osobę, grupę, rolę lub urządzenie;

c. Przypisywanie identyfikatora do konkretnej osoby, grupy, roli lub urządzenia;

d. Zapobieganie ponownemu użyciu identyfikatorów przez okres [*Realizacja: okres zdefiniowany przez organizację*];

e. Wyłączenie identyfikatora po czasie [*Realizacja: okres nieaktywności zdefiniowany przez organizację*].

Zabezpieczenia powiązane: AC-2, IA-2, IA-3, IA-5, IA-8, SC-37.

Zabezpieczenia rozszerzone:

(1) ZARZĄDZANIE IDENTYFIKATOREM | ZAKAZ UŻYWANIA IDENTYFIKATORÓW KONT JAKO IDENTYFIKATORÓW PUBLICZNYCH

Organizacja zabrania używania identyfikatorów kont systemu teleinformatycznego, które są takie same jak identyfikatory publiczne stosowane w indywidualnych kontach poczty elektronicznej.

Zabezpieczenia powiązane: AT-2.

(2) ZARZĄDZANIE IDENTYFIKATOREM | AUTORYZACJA PRZEŁOŻONEGO

Organizacja wymaga, aby proces rejestracji w celu otrzymania indywidualnego identyfikatora podlegał autoryzacji przełożonego.

(3) ZARZĄDZANIE IDENTYFIKATOREM | WIELE FORM CERTYFIKACJI

Organizacja wymaga stosowania wielu form certyfikacji[32] indywidualnych znaków rozpoznawczych (identyfikatorów).

(4) ZARZĄDZANIE IDENTYFIKATOREM | IDENTYFIKACJA STATUSU UŻYTKOWNIKA

Organizacja zarządza indywidualnymi identyfikatorami, jednoznacznie weryfikując każdą osobę jako [*Realizacja: charakterystyka zdefiniowana przez organizację identyfikująca status indywidualny[33]*].

Zabezpieczenia powiązane: AT-2.

(5) ZARZĄDZANIE IDENTYFIKATOREM | ZARZĄDZANIE DYNAMICZNE

System teleinformatyczny dynamicznie zarządza identyfikatorami.

Zabezpieczenia powiązane: AC-16.

(6) ZARZĄDZANIE IDENTYFIKATOREM | ZARZĄDZANIE MIĘDZYORGANIZACYJNE

Organizacja koordynuje z [*Realizacja: instytucje zewnętrzne zdefiniowane przez organizację*] działania w zakresie zarządzania identyfikatorami między organizacjami.

(7) ZARZĄDZANIE IDENTYFIKATOREM | REJESTRACJA OSOBISTA

Organizacja wymaga, aby proces rejestracji w celu otrzymania indywidualnego identyfikatora został przeprowadzony osobiście przez wyznaczony organ rejestracyjny.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	IA-4	IA-4	IA-4

[32] Formy identyfikacji, np. dowody z dokumentów lub połączenie dokumentów i danych biometrycznych.

[33] Cechy identyfikujące status osób fizycznych obejmują np. kontrahentów i cudzoziemców.

IA-5 ZARZĄDZANIE METODAMI UWIERZYTELNIANIA

Zabezpieczenie: Organizacja zarządza metodami uwierzytelniania w systemie teleinformatycznym poprzez:

a. Weryfikację, w ramach początkowego procesu uwierzytelnienia, tożsamości osoby, grupy, roli lub urządzenia uczestniczącego w procesie uwierzytelnienia;

b. Ustanowienie wstępnej treści uwierzytelniającej odnoszącej się do osób uwierzytelnianych określonych przez organizację;

c. Zapewnienie, że mechanizmy uwierzytelnienia mają wystarczającą siłę, która umożliwia ich wykorzystanie;

d. Ustanowienie i wdrożenie procedur administracyjnych dotyczących wstępnej dystrybucji elementów uwierzytelniających, postępowania z zagubionymi / zagrożonymi lub uszkodzonymi elementami uwierzytelniania oraz odwoływania metod i elementów uwierzytelniających;

e. Zmianę domyślnej zawartości metod uwierzytelnienia przed instalacją systemu teleinformatycznego;

f. Ustanowienie minimalnych i maksymalnych ograniczeń w zakresie okresu używalności oraz warunków ponownego użycia metod uwierzytelniania;

g. Zmianę / odświeżenie metod uwierzytelnienia w czasie [*Realizacja: okres zdefiniowany przez organizację według typu wystawcy uwierzytelnienia*];

h. Ochronę treści uwierzytelniających przed nieuprawnionym ujawnieniem i modyfikacją;

i. Wymaganie od osób fizycznych wdrażania i stosowania określonych metod zabezpieczeń urządzeń w celu zapewnienia uwierzytelniania;

j. Zmianę metod uwierzytelnienia kont grupowych / ról w przypadku zmiany członkostwa w tych kontach.

Zabezpieczenia powiązane: AC-2, AC-3, AC-6, CM-6, IA-2, IA-4, IA-8, PL-4, PS-5, PS-6, SC-12, SC-13, SC-17, SC-28.

Zabezpieczenia rozszerzone:

(1) ZARZĄDZANIE METODAMI UWIERZYTELNIANIA | UWIERZYTELNIANIE OPARTE O HASŁA

System teleinformatyczny, dokonując uwierzytelniania opartego na hasłach:

(a) Wymusza minimalną złożoność hasła [*Realizacja: zdefiniowane przez organizację wymagania dotyczące rozróżniania wielkości liter, liczby znaków, kombinacji wielkich liter, małych liter, cyfr i znaków specjalnych, w tym minimalne wymagania dla każdego typu*];

(b) Wymusza przynajmniej następującą liczbę zmienionych znaków podczas tworzenia nowych haseł: [*Realizacja: liczba zdefiniowana przez organizację*];

(c) Przechowuje i przesyła wyłącznie hasła chronione kryptograficznie;

(d) Egzekwuje ograniczenia dotyczące minimalnego i maksymalnego okresu ważności hasła w okresie [*Realizacja: okres zdefiniowane przez organizację dla minimalnego okresu ważności, oraz maksymalnego okresu ważności*];

(e) Zabrania ponownego użycia hasła po [*Realizacja: liczba wystąpień zdefiniowana przez organizację*] wystąpieniach;

(f) Umożliwia użycie hasła tymczasowego do logowania do systemu z wymuszeniem natychmiastowej zmiany na hasło stałe.

Zabezpieczenia powiązane: IA-6.

(2) ZARZĄDZANIE METODAMI UWIERZYTELNIANIA | UWIERZYTELNIANIE OPARTE O INFRASTRUKTURĘ KLUCZA PUBLICZNEGO

System teleinformatyczny wykorzystujący uwierzytelnianie oparte o infrastrukturę klucza publicznego:

(a) Zatwierdza certyfikaty oraz sprawdza informacje o statusie certyfikatu, konstruując i weryfikując ścieżkę certyfikacji[34] do zaakceptowanej „Kotwicy zaufania" (Trust Anchor);

(b) Wymusza autoryzowany dostęp do odpowiedniego klucza prywatnego;

(c) Mapuje uwierzytelnioną tożsamość do konta indywidualnego lub grupy;

(d) Implementuje lokalną pamięć podręczną unieważnionych danych w celu obsługi ścieżki wykrywania i sprawdzania w przypadku niemożności sieciowego dostępu do tych unieważnionych danych.

Zabezpieczenia powiązane: IA-6.

(3) ZARZĄDZANIE METODAMI UWIERZYTELNIANIA | REJESTRACJA OSOBISTA LUB PRZEZ ZAUFANĄ TRZECIĄ STRONĘ

Organizacja wymaga, aby proces rejestracji w celu uzyskania [*Realizacja: organizacyjnie określone typy i / lub specyfikacje weryfikatorów*] został przeprowadzony [*Realizacja: osobiście; przez zaufaną stronę trzecią*] przed uzyskaniem autoryzacji [*Realizacja: określone przez organizację podmioty uwierzytelniające*], za zgodą i autoryzacją [*Realizacja: personelu lub roli zdefiniowanej przez organizację*].

(4) ZARZĄDZANIE METODAMI UWIERZYTELNIANIA | AUTOMATYCZNE WSPARCIE OKREŚLANIA SIŁY HASŁA

Organizacja wykorzystuje zautomatyzowane narzędzia do określania, czy hasło uwierzytelniające jest wystarczająco silne, aby spełnić [*Realizacja: wymagania zdefiniowane przez organizację*].

Zabezpieczenia powiązane: CA-2, CA-7, RA-5.

[34] Informacje o statusie ścieżek certyfikacji obejmują, np. listy odwołania certyfikatów lub odpowiedzi usługi weryfikacji ważności certyfikatu on-line (OCSP).

(5) ZARZĄDZANIE METODAMI UWIERZYTELNIANIA | ZMIANA METODY UWIERZYTELNIANIA PRZED DOSTAWĄ

Organizacja wymaga od twórców / instalatorów komponentów systemu teleinformatycznego dostarczenia unikatowych uwierzytelnień lub zmiany domyślnych uwierzytelnień przed dostawą / instalacją elementu systemu.

(6) ZARZĄDZANIE METODAMI UWIERZYTELNIANIA | OCHRONA METOD UWIERZYTELNIANIA

Organizacja chroni wystawców uwierzytelnień proporcjonalnie do kategorii bezpieczeństwa informacji, do których umożliwia dostęp wystawcy uwierzytelnienia.

(7) ZARZĄDZANIE METODAMI UWIERZYTELNIANIA | BRAK WBUDOWANYCH NIEZASZYFROWANYCH STATYCZNYCH ELEMENTÓW UWIERZYTELNIANIA

Organizacja zapewnia, że niezaszyfrowane statyczne elementy uwierzytelniania nie są osadzone w aplikacjach lub skryptach dostępu ani przechowywane pod klawiszami klawiatury.

(8) ZARZĄDZANIE METODAMI UWIERZYTELNIANIA | JEDNO KONTO W WIELU SYSTEMACH INFORMACYJNYCH

Organizacja wdraża [*Realizacja: środki bezpieczeństwa zdefiniowane przez organizację*] w celu zarządzania ryzykiem naruszenia bezpieczeństwa spowodowanego faktem używania przez personel tego samego konta w wielu systemach teleinformatycznych.

(9) ZARZĄDZANIE METODAMI UWIERZYTELNIANIA | ZARZĄDZANIE DANYMI UWIERZYTELNIAJĄCYMI MIĘDZY ORGANIZACJAMI

Organizacja koordynuje działania z *[Realizacja: instytucje zewnętrzne zdefiniowane przez organizację*] w zakresie zarządzania metodami uwierzytelniania między organizacjami.

(10) ZARZĄDZANIE METODAMI UWIERZYTELNIANIA | DYNAMICZNE KOJARZENIE DANYCH UWIERZYTELNIAJĄCYCH

System teleinformatyczny dynamicznie weryfikuje tożsamość.

(11) ZARZĄDZANIE METODAMI UWIERZYTELNIANIA | UWIERZYTELNIANIE PRZY UŻYCIU TOKENA

System teleinformatyczny do sprzętowego uwierzytelniania opartego na tokenach wykorzystuje mechanizmy, które spełniają [*Realizacja: wymagania jakościowe dotyczące tokenów zdefiniowane przez organizację*].

(12) ZARZĄDZANIE METODAMI UWIERZYTELNIANIA | UWIERZYTELNIANIE BIOMETRYCZNE

System teleinformatyczny do uwierzytelniania opartego na danych biometrycznych wykorzystuje mechanizmy, które spełniają [*Realizacja: określone przez organizację wymagania jakości identyfikacji biometrycznej*].

(13) ZARZĄDZANIE METODAMI UWIERZYTELNIANIA | PRZEDAWNIENIE BUFOROWANYCH ELEMENTÓW UWIERZYTELNIANIA

System teleinformatyczny zabrania używania buforowanych elementów uwierzytelniania po [*Realizacja: okres zdefiniowany przez organizację*].

(14) ZARZĄDZANIE METODAMI UWIERZYTELNIANIA | ZARZĄDZANIE ZAWARTOŚCIĄ ZAUFANYCH MAGAZYNÓW INFRASTRUKTURY KLUCZA PUBLICZNEGO

W przypadku uwierzytelniania opartego na infrastrukturze klucza publicznego, organizacja stosuje w całej organizacji metodologię zarządzania zawartością magazynów zaufania infrastruktury klucza publicznego zainstalowanych na wszystkich platformach, w tym w sieciach, systemach operacyjnych, przeglądarkach i aplikacjach.

Zabezpieczenia powiązane: Brak.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	IA-5 (1) (11)	IA-5 (1) (2) (3) (11)	IA-5 (1) (2) (3) (11)

IA-6 OCHRONA PROCESU UWIERZYTELNIANIA

Zabezpieczenie: System teleinformatyczny „ukrywa" informacje zwrotne dotyczące informacji uwierzytelniających podczas procesu uwierzytelniania, w celu ochrony informacji przed możliwym wykorzystaniem / użyciem przez nieupoważnione osoby.

Zabezpieczenia powiązane: PE-18.

Zabezpieczenia rozszerzone: Brak.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P2	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	IA-6	IA-6	IA-6

IA-7 UWIERZYTELNIANIE MODUŁU KRYPTOGRAFICZNEGO

Zabezpieczenie: System teleinformatyczny implementuje mechanizmy uwierzytelniania w module kryptograficznym, które spełniają wymagania obowiązujących przepisów, zarządzeń wykonawczych, dyrektyw, zasad, standardów i wskazówek dotyczących takiego uwierzytelnienia.

Zabezpieczenia powiązane: SC-12, SC-13.

Zabezpieczenia rozszerzone: Brak.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	IA-7	IA-7	IA-7

IA-8 IDENTYFIKACJA I UWIERZYTELNIANIE (UŻYTKOWNICY SPOZA ORGANIZACJI)

Zabezpieczenie: system teleinformatyczny jednoznacznie identyfikuje i uwierzytelnia użytkowników spoza struktur organizacji (lub procesy działające w imieniu tych użytkowników).

Zabezpieczenia powiązane: AC-2, AC-14, AC-17, AC-18, IA-2, IA-4, IA-5, MA-4, RA-3, SA-12, SC-8.

Zabezpieczenia rozszerzone:

(1) IDENTYFIKACJA I UWIERZYTELNIENIE | AKCEPTACJA POŚWIADCZEŃ TOŻSAMOŚCI WYDANYCH PRZEZ INNE ORGANIZACJE

System teleinformatyczny akceptuje i elektronicznie weryfikuje dane identyfikacyjne karty dostępowej przedstawicieli innych organizacji.

Zabezpieczenia powiązane: AU-2, PE-3, SA-4.

(2) IDENTYFIKACJA I UWIERZYTELNIENIE | AKCEPTACJA POŚWIADCZEŃ STRON TRZECICH

System teleinformatyczny akceptuje tylko poświadczenia osób trzecich akceptowane i zatwierdzone zgodnie z procedurami przyjętymi w organizacji.

Zabezpieczenia powiązane: AU-2.

(3) IDENTYFIKACJA I UWIERZYTELNIENIE | WYKORZYSTANIE CERTYFIKOWANYCH PRODUKTÓW

Organizacja stosuje tylko certyfikowane komponenty systemu teleinformatycznego w [*Realizacja: systemy teleinformatyczne zdefiniowane przez organizację*] do akceptowania poświadczeń stron trzecich.

Zabezpieczenia powiązane: SA-4.

(4) IDENTYFIKACJA I UWIERZYTELNIENIE | WYKORZYSTANIE PROFILI WYDAWANYCH PRZEZ STOSOWNE INSTYTUCJE

[Usunięto]

Zabezpieczenia powiązane: SA-4.

(5) IDENTYFIKACJA I UWIERZYTELNIENIE | AKCEPTACJA POŚWIADCZEŃ OSOBISTEJ WERYFIKACJI TOŻSAMOŚCI

[Usunięto]

Zabezpieczenia powiązane: AU-2.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	IA-8 (1) (2) (3)	IA-8 (1) (2) (3)	IA-8 (1) (2) (3)

IA-9 IDENTYFIKACJA I UWIERZYTELNIANIE USŁUGI

Zabezpieczenie: organizacja identyfikuje i uwierzytelnia [*Realizacja: usługi systemu teleinformatycznego zdefiniowane przez organizację*] przy użyciu [*Realizacja: środki bezpieczeństwa zdefiniowane przez organizację*].

Zabezpieczenia rozszerzone:

(1) IDENTYFIKACJA I UWIERZYTELNIANIE USŁUG | WYMIANA INFORMACJI

Organizacja zapewnia dostawcom usług odbieranie, sprawdzanie i przesyłanie informacji identyfikacyjnych i uwierzytelniających.

(2) IDENTYFIKACJA I UWIERZYTELNIANIE USŁUG | PRZEKAZYWANIE DECYZJI O POZYTYWNEJ IDENTYFIKACJI I UWIERZYTELNIENIU

Organizacja zapewnia, że decyzje dotyczące identyfikacji i uwierzytelnienia są przesyłane między [*Realizacja: usługi zdefiniowane przez organizację*] zgodnie z zasadami ustanowionymi przez organizację.

Zabezpieczenia powiązane: SC-8.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P0	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	IA-9 (opcjonalnie)	IA-9 (opcjonalnie)	IA-9 (opcjonalnie)

IA-10 IDENTYFIKACJA I UWIERZYTELNIANIE ADAPTACYJNE

Zabezpieczenie: organizacja wymaga, aby zatrudniane osoby uzyskiwały dostęp do systemu teleinformatycznego poprzez [*Realizacja: zdefiniowane przez organizację dodatkowe techniki lub mechanizmy uwierzytelniania*] w określonych [*Realizacja: okoliczności lub sytuacje zdefiniowane przez organizację*].

Zabezpieczenia powiązane: AU-6, SI-4.

Zabezpieczenia rozszerzone: Brak.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P0	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	IA-10 (opcjonalnie)	IA-10 (opcjonalnie)	IA-10 (opcjonalnie)

IA-11 PONOWNE UWIERZYTELNIANIE

Zabezpieczenie: organizacja wymaga od użytkowników i urządzeń ponownego uwierzytelnienia, w przypadku wystąpienia [*Realizacja: określone przez organizację okoliczności lub sytuacje wymagające ponownego uwierzytelnienia*].

Zabezpieczenia powiązane: AC-11.

Zabezpieczenia rozszerzone: Brak.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P0	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	IA-11 (opcjonalnie)	IA-11 (opcjonalnie)	IA-11 (opcjonalnie)

KATEGORIA: REAGOWANIE NA INCYDENTY

IR-1 POLITYKA I PROCEDURY REAGOWANIA NA INCYDENTY

Zabezpieczenie: Organizacja:

a. Opracowuje, dokumentuje i rozpowszechnia w odniesieniu do [*Realizacja: personel lub role zdefiniowane przez organizację*]:

   1. Politykę reagowania na incydenty, która dotyczy celu, zakresu, ról, obowiązków, zaangażowania kierownictwa, koordynacji między jednostkami organizacyjnymi i zachowania spójności działań;

   2. Procedury ułatwiające wdrażanie polityki reagowania na incydenty i związane z nimi środki reagowania na incydenty;

b. Przegląda i aktualizuje bieżącą:

   1. Politykę reagowania na incydenty z częstotliwością [*Realizacja: częstotliwość określona przez organizację*];

   2. Procedury reagowania na incydenty z częstotliwością [*Realizacja: częstotliwość określona przez organizację*].

Zabezpieczenia powiązane: PM-9.

Zabezpieczenia rozszerzone: Brak.

Zabezpieczenia powiązane: Brak

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	IR-1	IR-1	IR-1

IR-2 SZKOLENIE W ZAKRESIE REAGOWANIA NA INCYDENTY

Zabezpieczenie: Organizacja zapewnia szkolenie w zakresie reagowania na incydenty użytkownikom systemu teleinformatycznego zgodnie z przypisanymi rolami i obowiązkami:

a. W ciągu [*Realizacja: okres zdefiniowany przez organizację*] od podjęcia reakcji lub odpowiedzialności na incydent;

b. W przypadku wystąpienia zmian w systemie teleinformatycznym;

c. Cyklicznie [*Realizacja: częstotliwość określona przez organizację*].

Zabezpieczenia powiązane: AT-3, CP-3, IR-8.

Zabezpieczenia rozszerzone:

(1) SZKOLENIE W ZAKRESIE REAGOWANIA NA INCYDENTY | WYDARZENIA SYMULOWANE

Organizacja włącza symulowane zdarzenia do szkolenia w zakresie reagowania na incydenty, aby umożliwiać skuteczne reagowanie personelu w sytuacjach kryzysowych.

(2) SZKOLENIE W ZAKRESIE REAGOWANIA NA INCYDENTY | ZAUTOMATYZOWANE ŚRODOWISKA SZKOLENIOWE

Organizacja stosuje zautomatyzowane mechanizmy celem zapewnienia dokładniejszego i bardziej realistycznego środowisko szkolenia w zakresie reagowania na incydenty.

Zabezpieczenia powiązane: Brak

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P2	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	IR-2	IR-2	IR-2 (1) (2)

IR-3 TESTOWANIE REAGOWANIA NA INCYDENTY

Zabezpieczenie: Organizacja testuje zdolność reagowania na incydenty w systemie teleinformatycznym z częstotliwością [*Realizacja: częstotliwość określona przez organizację*] przy użyciu [*Realizacja: testy zdefiniowane przez organizację*] w celu ustalenia skuteczności reakcji na incydent i udokumentowania wyników testów.

Zabezpieczenia powiązane: CP-4, IR-8.

Zabezpieczenia rozszerzone:

(1) TESTOWANIE REAGOWANIA NA INCYDENTY | TESTOWANIE AUTOMATYCZNE

Organizacja stosuje zautomatyzowane mechanizmy w celu dokładniejszego i bardziej skutecznego testowania zdolności reagowania na incydenty.

Zabezpieczenia powiązane: AT-2.

(2) TESTOWANIE REAGOWANIA NA INCYDENTY | KOORDYNACJA Z POWIĄZANYMI PLANAMI

Organizacja koordynuje testowanie reakcji na incydenty z jednostkami organizacyjnymi odpowiedzialnymi za powiązane plany.

Zabezpieczenia powiązane: Brak

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P2	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	IR-3 (opcjonalnie)	IR-3 (2	IR-3 (2)

IR-4 OBSŁUGA INCYDENTÓW

Zabezpieczenie: Organizacja:

a. Wdraża funkcję obsługi incydentów mających wpływ na bezpieczeństwo, która obejmuje przygotowanie, wykrywanie i analizę, powstrzymywanie, eliminowanie i odzyskiwanie;

b. Koordynuje działania związane z obsługą incydentów z działaniami planowania awaryjnego;

c. Uwzględnia wnioski wyciągnięte z bieżących działań związanych z obsługą incydentów w procedurach reagowania na incydenty, szkoleniach i testach oraz odpowiednio wdraża wynikające z nich zmiany.

Zabezpieczenia powiązane: AU-6, CM-6, CP-2, CP-4, IR-2, IR-3, IR-8, PE-6, SC-5, SC-7, SI-3, SI-4 , SI-7.

Zabezpieczenia rozszerzone:

(1) OBSŁUGA INCYDENTÓW | AUTOMATYCZNE PROCESY OBSŁUGI ZDARZEŃ

Organizacja stosuje zautomatyzowane mechanizmy wspierające proces obsługi incydentów.

(2) OBSŁUGA INCYDENTÓW | DYNAMICZNA REKONFIGURACJA

Organizacja implementuje dynamiczną rekonfigurację [*Realizacja: elementy systemu teleinformatycznego zdefiniowane przez organizację*] w celu osiągnięcia zdolności do reagowania na incydent.

Zabezpieczenia powiązane: AC-2, AC-4, AC-16, CM-2, CM-3, CM-4.

(3) OBSŁUGA INCYDENTÓW | CIĄGŁOŚĆ OPERACJI

Organizacja identyfikuje [*Realizacja: zdefiniowane przez organizację klasy incydentów*] i wprowadza [*Realizacja: zdefiniowane przez organizację działania, które należy podjąć w odpowiedzi na klasy incydentów*] w celu zapewnienia kontynuacji zadań organizacyjnych i funkcji biznesowych.

(4) OBSŁUGA INCYDENTÓW | KORELACJA INFORMACJI

Organizacja koreluje informacje o incydentach i indywidualne reakcje na incydenty, w celu uzyskania szerokiej świadomości i możliwości reagowania na incydenty.

(5) OBSŁUGA INCYDENTÓW | AUTOMATYCZNE WYŁĄCZENIE SYSTEMU INFORMATYCZNEGO

Organizacja wdraża konfigurowalną funkcję automatycznego wyłączania systemu teleinformatycznego w przypadku wykrycia [*Realizacja: naruszenia bezpieczeństwa zdefiniowane przez organizację*] .

(6) OBSŁUGA INCYDENTÓW | ZAGROŻENIA WEWNĘTRZNE

Organizacja wdraża funkcję obsługi incydentów w przypadku zagrożeń wewnętrznych.

(7) OBSŁUGA INCYDENTÓW | ZAGROŻENIA WEWNĘTRZNE - KOORDYNACJA WEWNĄTRZ ORGANIZACJI

Organizacja koordynuje obsługę incydentów w zakresie zagrożeń wewnętrznych w [*Realizacja: zdefiniowane przez organizację komponenty lub elementy organizacji*].

(8) OBSŁUGA INCYDENTÓW | KOORDYNACJA Z ORGANIZACJAMI ZEWNĘTRZNYMI

Organizacja koordynuje działania z [*Realizacja: organizacje zewnętrzne zdefiniowane przez organizację*], aby skorelować i udostępnić [*Realizacja: informacje o zdarzeniach zdefiniowane przez organizację*], w celu zbudowania szerokiej międzyorganizacyjnej świadomości dotyczącej zdarzeń i podejmowania bardziej skutecznych reakcji na zdarzenia.

(9) OBSŁUGA INCYDENTÓW | ZDOLNOŚĆ UDZIELANIA DYNAMICZNEJ ODPOWIEDZI

Organizacja stosuje [*Realizacja: funkcje dynamicznego reagowania zdefiniowane przez organizację*], w celu podejmowania skutecznej reakcji na zdarzenia związane z bezpieczeństwem.

Zabezpieczenia powiązane: CP-10.

(10) OBSŁUGA INCYDENTÓW | KOORDYNACJA ŁAŃCUCHA DOSTAW

Organizacja koordynuje działania związane z obsługą incydentów obejmujące zdarzenia związane z łańcuchem dostaw z innymi organizacjami zaangażowanymi w łańcuch dostaw.

Zabezpieczenia powiązane: Brak.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	IR-4	IR-4 (1)	IR-4 (1) (4)

IR-5 MONITOROWANIE INCYDENTÓW

Zabezpieczenie: organizacja śledzi i dokumentuje incydenty związane z bezpieczeństwem systemu teleinformatycznego.

Zabezpieczenia powiązane: AU-6, IR-8, PE-6, SC-5, SC-7, SI-3, SI-4, SI-7.

Zabezpieczenia rozszerzone:

(1) MONITOROWANIE INCYDENTÓW | AUTOMATYCZNE ŚLEDZENIE / ZBIERANIE DANYCH / ANALIZA

Organizacja stosuje zautomatyzowane mechanizmy pomagające w śledzeniu incydentów bezpieczeństwa oraz w gromadzeniu i analizie informacji o incydentach.

Zabezpieczenia powiązane: AU-7, IR-4.

Zabezpieczenia powiązane: Brak

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	IR-5	IR-5	IR-5 (1)

IR-6 RAPORTOWANIE INCYDENTÓW

Zabezpieczenie: Organizacja:

a. Wymaga od personelu zgłaszania podejrzanych incydentów bezpieczeństwa do odpowiednich komórek zarządzania incydentami w ciągu [*Realizacja: okres zdefiniowany przez organizację*];

b. Zgłasza informacje o zdarzeniu naruszającym bezpieczeństwo do [*Realizacja: właściwy CSIRT zdefiniowany przez organizację*].

Zabezpieczenia powiązane: IR-4, IR- 5, IR-8.

Zabezpieczenia rozszerzone:

(1) RAPORTOWANIE INCYDENTÓW | AUTOMATYCZNE RAPORTOWANIE

Organizacja stosuje zautomatyzowane mechanizmy pomagające w zgłaszaniu incydentów bezpieczeństwa.

Zabezpieczenia powiązane: IR-7.

(2) RAPORTOWANIE INCYDENTÓW | PODATNOŚĆ NA INCYDENTY

Organizacja zgłasza luki w zabezpieczeniach systemu teleinformatycznego związane ze zgłoszonymi incydentami bezpieczeństwa do [*Realizacja: personel lub role zdefiniowane przez organizację*].

(3) RAPORTOWANIE INCYDENTÓW | KOORDYNACJA Z ŁAŃCUCHEM DOSTAW

Organizacja przekazuje informacje o zdarzeniu naruszającym bezpieczeństwo innym organizacjom zaangażowanym w łańcuch dostaw do systemów teleinformatycznych lub elementów systemu teleinformatycznego powiązanych z incydentem.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	IR-6	IR-6 (1)	IR-6 (1)

IR-7 WSPARCIE REAGOWANIA NA INCYDENTY

Zabezpieczenie: Organizacja zapewnia personel wsparcia do reagowania na incydenty, integralny z funkcją reagowania na incydenty organizacyjne, który oferuje porady i pomoc użytkownikom systemu teleinformatycznego w zakresie obsługi i zgłaszania incydentów związanych z bezpieczeństwem.

Zabezpieczenia powiązane: AT-2, IR-4, IR-6, IR-8, SA-9.

Zabezpieczenia rozszerzone:

(1) WSPARCIE REAGOWANIA NA INCYDENTY | AUTOMATYCZNE WSPARCIE DOSTĘPNOŚCI INFORMACJI / OBSŁUGI

Organizacja stosuje zautomatyzowane mechanizmy reakcji i wsparcia incydentów w celu zwiększenia dostępności informacji**.**

(2) WSPARCIE REAGOWANIA NA INCYDENTY | KOORDYNACJA Z DOSTAWCAMI ZEWNĘTRZNYMI

Organizacja:

(a) Ustanawia bezpośredni, oparty na współpracy związek między własną zdolnością reagowania na incydenty, a zewnętrznymi dostawcami środków ochrony systemu teleinformatycznego;

(b) Wskazuje zewnętrznym dostawcom członków zespołu reagowania na incydenty.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P2	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	IR-7	IR-7 (1)	IR-7 (1)

IR-8 PLAN REAGOWANIA NA INCYDENTY

Zabezpieczenie: Organizacja:

a. Opracowuje plan reagowania na incydenty, który:

1. Dostarcza organizacji strategię dotyczącą wdrażania zdolności reagowania na incydenty;
2. Opisuje strukturę i organizację zdolności reagowania na incydenty;
3. Zapewnia ogólne podejście do tego, jak zdolność reagowania na incydenty wpisuje się w ogólne ramy działalności organizacji;

4. Spełnia unikalne wymagania organizacji dotyczące działań biznesowych, wielkości, struktury i funkcji;
5. Definiuje zgłaszane zdarzenia;
6. Dostarcza metryki[35] do pomiaru zdolności reagowania na incydenty w organizacji;
7. Określa zasoby i wsparcie zarządzania potrzebne do skutecznego utrzymania zdolności reagowania na incydenty;
8. Jest weryfikowany i zatwierdzany przez [*Realizacja: personel lub role zdefiniowane przez organizację*];

b. Dystrybuuje kopie planu reagowania na incydenty do [*Realizacja: personel reagowania na incydenty zdefiniowany przez organizację (identyfikowany według nazwiska i / lub roli) oraz elementy organizacyjne*];

c. Przegląda i analizuje plan reagowania na incydenty co [*Realizacja: częstotliwość określona przez organizację*];

d. Aktualizuje plan reagowania na incydenty, aby uwzględnić zmiany systemowe / organizacyjne lub problemy napotkane podczas wdrażania, wykonywania lub testowania planu;

e. Informuje o zmianach planu reagowania na incydenty [*Realizacja: personel reagowania na incydenty zdefiniowany przez organizację (identyfikowany według nazwiska i / lub roli) oraz elementy organizacyjne*];

f. Chroni plan reagowania na incydenty przed nieuprawnionym ujawnieniem i modyfikacją.

Zabezpieczenia powiązane: MP-2, MP-4, MP-5.

Zabezpieczenia rozszerzone: Brak.

Zabezpieczenia powiązane: Brak

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	IR-8	IR-8	IR-8

[35] Możliwe metryki dotyczące danych związanych z incydentami obejmują: liczbę obsługiwanych incydentów; czas zaangażowania w incydent; obiektywną ocenę każdego incydentu; subiektywną ocenę każdego incydentu.

IR-9 REAKCJA NA WYCIEK / UJAWNIENIE INFORMACJI

Zabezpieczenie: Organizacja reaguje na wycieki informacji poprzez:

a. Identyfikację specyficznych informacji mających ujemny wpływ na system teleinformatyczny;

b. Ostrzeganie [*Realizacja: personel lub role zdefiniowane przez organizację*] o wycieku informacji przy użyciu metody komunikacji niezwiązanej z ujawnieniem;

c. Izolowanie „zakażonego" systemu teleinformatycznego lub elementu systemu;

d. Usunięcie informacji z „zakażonego" systemu teleinformatycznego lub elementu;

e. Identyfikację innych systemów teleinformatycznych lub elementów systemu, które mogą zostać „zakażone" w przyszłości;

f. Wykonywanie innych czynności [*Realizacja: działania zdefiniowane przez organizację*].

Zabezpieczenia rozszerzone:

(1) ODPOWIEDŹ NA WYCIEK / UJAWNIENIE INFORMACJI | ODPOWIEDZIALNY PERSONEL

Organizacja powołuje [*Realizacja: personel lub role zdefiniowane przez organizację*] odpowiedzialny za reagowanie na wycieki informacji.

(2) ODPOWIEDŹ NA WYCIEK / UJAWNIENIE INFORMACJI | SZKOLENIE

Organizacja zapewnia szkolenie w zakresie reagowania na wycieki informacji z częstotliwością [*Realizacja: częstotliwość określona przez organizację*].

(3) ODPOWIEDŹ NA WYCIEK / UJAWNIENIE INFORMACJI | DZIAŁANIA PO UJAWNIENIU

Organizacja wdraża [*Realizacja: procedury zdefiniowane przez organizację*], aby zapewnić personelowi organizacyjnemu, na który wpływ mają wycieki informacji, możliwość dalszego działania, podczas gdy „zakażone" systemy podejmują działania naprawcze.

(4) ODPOWIEDŹ NA WYCIEK / UJAWNIENIE INFORMACJI | WYSTAWIENIE NA DZIAŁANIA OSÓB NIEAUTORYZOWANYCH

Organizacja stosuje [*Realizacja: procedury ochrony bezpieczeństwa zdefiniowane przez organizację*] wobec personelu uzyskującego dostęp do informacji, zapoznanie się z którymi nie mieści się w przydzielonych im uprawnieniach dostępu.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P0	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	IR-9 (opcjonalnie)	IR-9 (opcjonalnie)	IR-9 (opcjonalnie)

IR-10 ZINTEGROWANY ZESPÓŁ REAGOWANIA NA INCYDENTY

Zabezpieczenie: Organizacja powołuje zintegrowany zespół reagowania na incydenty zawierający twórców narzędzi i personelu operacyjnego.

Zabezpieczenia rozszerzone: Brak.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P0	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	IR-10 (opcjonalnie)	IR-10 (opcjonalnie)	IR-10 (opcjonalnie)

KATEGORIA: UTRZYMANIE I WSPARCIE

MA-1 POLITYKA I PROCEDURY UTRZYMANIA SYSTEMU

Zabezpieczenie: Organizacja:

a. Opracowuje, dokumentuje i rozpowszechnia wśród [*Realizacja: personel lub role zdefiniowane przez organizację*]:

   1. Politykę utrzymania i wsparcia systemu, która dotyczy celu, zakresu, ról, obowiązków, zaangażowania kierownictwa, koordynacji między jednostkami organizacyjnymi i spójności działań;

   2. Procedury ułatwiające wdrożenie polityki utrzymania i wsparcia systemu i związanych z nimi kontroli utrzymania systemu;

b. Przegląda i aktualizuje bieżącą:

   1. Polityki utrzymania systemu z częstotliwością [*Realizacja: częstotliwość określona przez organizację*];

   2. Procedury utrzymania systemu z częstotliwością [*Realizacja: częstotliwość określona przez organizację*].

Zabezpieczenia powiązane: PM-9.

Zabezpieczenia rozszerzone: Brak.

Zabezpieczenia powiązane: Brak

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	MA-1	MA-1	MA-1

MA-2 NADZÓR NAD UTRZYMANIEM

Zabezpieczenie: Organizacja:

a. Planuje, wykonuje, dokumentuje i przegląda zapisy konserwacji i napraw komponentów systemu teleinformatycznego zgodnie ze specyfikacjami producenta lub dostawcy i / lub wymaganiami organizacyjnymi;

b. Zatwierdza i monitoruje wszystkie czynności konserwacyjne, zarówno wykonywane na miejscu, jak i zdalnie, oraz sprawdza czy sprzęt jest serwisowany na miejscu, czy przenoszony w inne miejsce;

c. Wymaga, aby [*Realizacja: personel lub role zdefiniowane przez organizację*] zatwierdzał usunięcie systemu teleinformatycznego lub komponentów systemu z obiektów organizacyjnych w celu konserwacji lub naprawy poza organizacją;

d. Usuwa wszystkie informacje z powiązanych mediów przed przeniesieniem z pomieszczeń organizacyjnych w celu dokonania konserwacji lub napraw poza siedzibą;

e. Sprawdza wszystkie potencjalnie naruszenia mechanizmów zabezpieczeń, celem określenia poprawności działania mechanizmów kontrolnych po przeprowadzonych czynnościach konserwacyjnych lub naprawczych;

f. Uwzględnia uzyskane informacje [*Realizacja: informacje związane z utrzymaniem zdefiniowane przez organizację*] w dokumentacja utrzymania.

Zabezpieczenia powiązane: CM-3, CM-4, MA-4, MP-6, PE-16, SA-12, SI-2.

Zabezpieczenia rozszerzone:

(1) NADZÓR NAD UTRZYMANIEM | ZAWARTOŚĆ REKORDU

[Włączono do MA-2]

(2) NADZÓR NAD UTRZYMANIEM | AUTOMATYCZNE DZIAŁANIA KONSERWACYJNE

Organizacja:

(a) Stosuje zautomatyzowane mechanizmy do planowania, przeprowadzania oraz dokumentowania konserwacji i napraw;

(b) Tworzy aktualne, dokładne i kompletne zapisy wszystkich żądanych, planowanych, przetwarzanych i zakończonych działań związanych z konserwacją i naprawą.

Zabezpieczenia powiązane: CA-7, MA-3.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P2	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	MA-2	MA-2	MA-2 (2)

MA-3 NARZĘDZIA UTRZYMANIOWE

Zabezpieczenie: Organizacja zatwierdza, kontroluje i monitoruje narzędzia do konserwacji systemu teleinformatycznego.

Zabezpieczenia powiązane: MA-2, MA-5, MP-6.

Zabezpieczenia rozszerzone:

(1) NARZĘDZIA UTRZYMANIOWE | NARZĘDZIA KONTROLNE

Organizacja sprawdza narzędzia serwisowe wnoszone do obiektu przez personel obsługi technicznej pod kątem niewłaściwych lub nieautoryzowanych modyfikacji.

Zabezpieczenia powiązane: SI-7.

(2) NARZĘDZIA UTRZYMANIOWE | MEDIA KONTROLNE

Organizacja sprawdza nośniki zawierające programy diagnostyczne i testowe pod kątem złośliwego kodu, zanim zostaną one użyte w systemie teleinformatycznym.

Zabezpieczenia powiązane: SI-3.

(3) NARZĘDZIA UTRZYMANIOWE | ZAPOBIEGANIE NIEAUTORYZOWANEMU USUWANIU

Organizacja zapobiega nieuprawnionemu usunięciu sprzętu utrzymaniowego zawierającego informacje organizacyjne poprzez:

(a) Sprawdzenie, czy w urządzeniu nie są przechowywane informacje organizacyjne;

(b) Zerowanie lub niszczenie sprzętu;

(c) Pozostawienie sprzętu w obiekcie;

(d) Uzyskanie zezwolenia wydanego przez [*Realizacja: personel lub role zdefiniowane przez organizację]* upoważniającego do usunięcia sprzętu z obiektu.

(4) NARZĘDZIA UTRZYMANIOWE | OGRANICZANIE UŻYWANIA NARZĘDZI

System teleinformatyczny ogranicza użycie narzędzi utrzymaniowych wyłącznie przez upoważniony personelu.

Zabezpieczenia powiązane: AC-2, AC-3, AC-5, AC-6.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P3	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	MA-3 (opcjonalnie)	MA-3 (1) (2)	MA-3 (1) (2) (3)

MA-4 UTRZYMANIE ZDALNE

Zabezpieczenie: Organizacja:

a. Zatwierdza i monitoruje zdalne działania utrzymaniowe i diagnostyczne;

b. Pozwala na korzystanie ze zdalnych narzędzi do utrzymania i diagnostyki zgodnie z ustanowioną polityką organizacyjną i udokumentowaniu w planie bezpieczeństwa systemu teleinformatycznego;

c. Korzysta z silnego uwierzytelniania przy ustanawianiu zdalnych sesji do obsługi technicznej i diagnostycznej;

d. Prowadzi dokumentację dotyczącą zdalnych czynności utrzymaniowych i diagnostycznych;

e. Zamyka sesje i połączenia sieciowe po zakończeniu czynności zdalnego utrzymania.

Zabezpieczenia powiązane: AC-2, AC-3, AC-6, AC-17, AU-2, AU-3, IA-2, IA-4, IA-5, IA-8, MA-2, MA-5 , MP-6, PL-2, SC-7, SC-10, SC-17.

Zabezpieczenia rozszerzone:

(1) UTRZYMANIE ZDALNE | AUDYT I PRZEGLĄD

Organizacja:

(a) Prowadzi audyty zdalnych sesji utrzymania i diagnostyki [*Realizacja: zdarzenia kontrolne zdefiniowane przez organizację*];

(b) Przegląda zapisy z konserwacji i sesji diagnostycznych.

Zabezpieczenia powiązane: AU-2, AU-6, AU-12.

(2) UTRZYMANIE ZDALNE | DOKUMENTY ZDALNEGO UTRZYMANIA

Organizacja umieszcza w planie bezpieczeństwa systemu teleinformatycznego zasady i procedury ustanawiania i korzystania ze zdalnych połączeń serwisowych i diagnostycznych.

(3) UTRZYMANIE ZDALNE | PORÓWNYWALNE POZIOMY BEZPIECZEŃSTWA / SANITYZACJA

Organizacja:

(a) wymaga, aby zdalne usługi serwisowe i diagnostyczne były świadczone z systemu teleinformatycznego, który realizuje funkcję bezpieczeństwa porównywalną z funkcją wdrożoną w obsługiwanym systemie;

(b) Usuwa serwisowany komponent z systemu teleinformatycznego przed podłączeniem ze zdalnymi usługami utrzymaniowymi lub diagnostycznymi, dokonuje sanityzacji komponentu (w odniesieniu do informacji organizacyjnych) przed przeniesieniem z pomieszczeń organizacyjnych, a po wykonaniu usługi sprawdza i sanityzuje komponent (w odniesieniu do potencjalnie złośliwego oprogramowania) przed ponownym podłączeniem tego komponentu do systemu teleinformatycznego.

Zabezpieczenia powiązane: MA-3, SA-12, SI-3, SI-7.

(4) UTRZYMANIE ZDALNE | UWIERZYTELNIANIE / SEPARACJA SESJI UTRZYMANIOWYCH

Organizacja chroni zdalne sesje serwisowe poprzez:

(a) Stosowanie uwierzytelnianie [*Realizacja: podmioty uwierzytelniające zdefiniowane w organizacji, które są odporne na odtwarzanie*];

(b) Oddzielenie sesji utrzymaniowych od innych połączeń sieciowych z systemem teleinformatycznym poprzez:

(1) Fizycznie oddzielone ścieżki komunikacyjne;

(2) Logicznie rozdzielone ścieżki komunikacyjne oparte na szyfrowaniu.

Zabezpieczenia powiązane: SC-13.

(5) UTRZYMANIE ZDALNE | ZGODY I POWIADOMIENIA

Organizacja:

(a) Wymaga zatwierdzenia przez [*Realizacja: personel lub role zdefiniowane przez organizację*] każdej zdalnej sesji wykorzystywanej do obsługi technicznej;

(b) Powiadamia [*Realizacja: personel lub role zdefiniowane przez organizację*] o dacie i godzinie planowanej zdalnej obsługi technicznej.

(6) UTRZYMANIE ZDALNE | OCHRONA KRYPTOGRAFICZNA

System teleinformatyczny implementuje mechanizmy kryptograficzne w celu ochrony integralności i poufności transmisji zdalnego utrzymania i diagnostyki.

Zabezpieczenia powiązane: SC-8, SC-13.

(7) UTRZYMANIE ZDALNE | ZDALNA WERYFIKACJA ZAKOŃCZENIA SESJI

System teleinformatyczny stosuje weryfikację zdalnego zakończenia zdalnych sesji utrzymania i diagnostyki.

Zdalna weryfikacja rozłączenia zapewnia, że zdalne połączenia z nielokalnych sesji serwisowych zostały zakończone i nie są już dostępne do użytku.

Zabezpieczenia powiązane: SC-13.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P2	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	MA-4	MA-4 (2)	MA-4 (2) (3)

MA-5 PERSONEL UTRZYMANIOWY

Zabezpieczenie: Organizacja:

a. Ustanawia proces autoryzacji personelu obsługi technicznej i prowadzi listę autoryzowanych organizacji obsługi technicznej lub personelu;

b. Zapewnia, aby personel wykonujący obsługę techniczną systemu teleinformatycznego, który nie jest bezpośrednio nadzorowany, posiadał autoryzację dostępu;

c. Wyznacza personel organizacyjny posiadający wymagane uprawnienia dostępu i kompetencje techniczne, do nadzorowania czynności utrzymaniowych wykonywanych przez personel nieposiadający wymaganych uprawnień dostępu.

Zabezpieczenia powiązane: AC-2, IA-8, MP-2, PE-2, PE-3, PE-4, RA-3.

Zabezpieczenia rozszerzone:

(1) PERSONEL UTRZYMANIOWY | OSOBY NIEPOSIADAJĄCE STOSOWNYCH PRAW DOSTĘPU

Organizacja:

(a) Wdraża procedury dotyczące korzystania z personelu obsługi technicznej, który nie posiada odpowiednich poświadczeń bezpieczeństwa lub nie jest obywatelem Polski i określa następujące wymagania:

(1) Personel obsługujący, który nie posiada autoryzacji dostępu, poświadczeń bezpieczeństwa lub formalnych zezwoleń na dostęp, jest eskortowany i nadzorowany podczas wykonywania czynności serwisowych i diagnostycznych w systemie teleinformatycznym, przez zatwierdzony personel organizacyjny, który posiada poświadczenia bezpieczeństwa, odpowiednie zezwolenia na dostęp, oraz posiada odpowiednie kwalifikacje techniczne;

(2) Przed rozpoczęciem czynności serwisowych lub diagnostycznych przez personel, który nie posiada autoryzacji dostępu, poświadczeń bezpieczeństwa lub formalnych zezwoleń na dostęp, wszystkie nietrwałe elementy przechowujące informacje w systemie teleinformatycznym są czyszczone, a wszystkie nieulotne nośniki pamięci są usuwane lub fizycznie odłączane od systemu i zabezpieczane;

(b) Opracowuje i wdraża alternatywne zabezpieczenia w przypadku, gdy element systemu teleinformatycznego nie może zostać wyczyszczony, usunięty lub odłączony od systemu.

Zabezpieczenia powiązane: MP-6, PL-2.

(2) PERSONEL UTRZYMANIOWY | POŚWIADCZENIA BEZPIECZEŃSTWA / SYSTEMY NIEJAWNE

Organizacja zapewnia, że personel wykonujący czynności serwisowe i diagnostyczne w systemie przetwarzania, przechowywania lub przesyłania informacji niejawnych posiada stosowne poświadczenia bezpieczeństwa i formalne zatwierdzenia dostępu do co najmniej najwyższego poziomu klasyfikacji informacji przetwarzanej w tym systemie.

Zabezpieczenia powiązane: PS-3.

(3) PERSONEL UTRZYMANIOWY | OBYWATELSTWO / SYSTEMY NIEJAWNE[36]

Zabezpieczenia powiązane: Brak.

(4) PERSONEL UTRZYMANIOWY | CUDZOZIEMCY[37]

Zabezpieczenia powiązane: Brak.

(5) PERSONEL UTRZYMANIOWY | OBSŁUGA NIEZWIĄZANA Z UTRZYMANIEM SYSTEMU

Organizacja zapewnia, że nienadzorowany personel wykonujący czynności niezwiązane bezpośrednio z systemem teleinformatycznym, ale w bezpośredniej odległości od systemu, będzie wymagał autoryzacji dostępu.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P2	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	MA-5	MA-5	MA-5 (1

MA-6 TERMINOWOŚĆ PRZEPROWADZANIA KONSERWACJI

Zabezpieczenie: Organizacja uzyskuje wsparcie serwisowe i / lub części zamienne do [*Realizacja: komponenty systemu teleinformatycznego zdefiniowane przez organizację*] w ciągu [*Realizacja: okres zdefiniowany przez organizację*] od wystąpienia awarii.

Zabezpieczenia powiązane: CM-8, CP-2, CP-7, SA-14, SA-15.

[36] Zastosowanie mają przepisy ustawy o ochronie informacji niejawnych.
[37] Zastosowanie mają przepisy ustawy o ochronie informacji niejawnych.

Zabezpieczenia rozszerzone:

(1) TERMINOWOŚĆ PRZEPROWADZANIA KONSERWACJI | KONSERWACJA ZAPOBIEGAWCZA

Organizacja wykonuje konserwację zapobiegawczą elementów systemu [*Realizacja: komponenty systemu teleinformatycznego zdefiniowane przez organizację*] w okresie *[Realizacja: przedziały czasowe zdefiniowane przez organizację*].

(2) TERMINOWOŚĆ PRZEPROWADZANIA KONSERWACJI | PLANOWANIE KONSERWACJA

Organizacja wykonuje konserwację planową systemu[*Realizacja: komponenty systemu teleinformatycznego zdefiniowane przez organizację*] w okresie [*Realizacja: przedziały czasowe zdefiniowane przez organizację*].

(3) TERMINOWOŚĆ PRZEPROWADZANIA KONSERWACJI | AUTOMATYCZNE WSPARCIE W ZAKRESIE KONSERWACJI PROGNOZOWANEJ

Organizacja wykorzystuje zautomatyzowane mechanizmy do przesyłania danych dotyczących konserwacji prognozowanej do komputerowego systemu zarządzania konserwacją.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P2	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	MA-6 (opcjonalnie)	MA-6	MA-6

KATEGORIA: OCHRONA NOŚNIKÓW DANYCH

MP-1 POLITYKA I PROCEDURY OCHRONY NOŚNIKÓW DANYCH

Zabezpieczenie: Organizacja:

a. Opracowuje, dokumentuje i rozpowszechnia w odniesieniu do [*Realizacja: personel lub role zdefiniowane przez organizację*]:

   1. Politykę ochrony nośników danych uwzględniającą cel, zakres, role, obowiązki, zaangażowanie kierownictwa, koordynację między jednostkami organizacyjnymi i spójności działań;

   2. Procedury ułatwiające wdrażanie polityki ochrony nośników danych i związane z tym środki ochrony nośników danych;

b. Przegląda i aktualizuje bieżącą:

   1. Politykę ochrony nośników danych z częstotliwością [*Realizacja: częstotliwość określona przez organizację*];

   2. Procedury ochrony nośników danych z częstotliwością [*Realizacja: częstotliwość określona przez organizację*].

Zabezpieczenia powiązane: PM-9.

Zabezpieczenia rozszerzone: Brak.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	MP-1	MP-1	MP-1

MP-2 DOSTĘP DO NOŚNIKÓW

Zabezpieczenie: organizacja zezwala na dostęp do [*Realizacja: zdefiniowane przez organizację typy mediów cyfrowych i / lub nie cyfrowych*] tylko przez [*Realizacja: personel lub role zdefiniowane przez organizację*].

Zabezpieczenia powiązane: AC-3, IA-2, MP-4, PE-2, PE-3, PL-2.

Zabezpieczenia rozszerzone:

(1) DOSTĘP DO NOŚNIKÓW | OGRANICZONY DOSTĘP AUTOMATYCZNY

[Włączony do MP-4 (2)].

(2) DOSTĘP DO NOŚNIKÓW | OCHRONA KRYPTOGRAFICZNA

[Włączony do SC-28 (1)].

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	MP-2	MP-2	MP-2

MP-3 OZNAKOWANIE NOŚNIKÓW

Zabezpieczenie: Organizacja:

a. Oznacza nośniki systemu teleinformatycznego, wskazując ograniczenia dystrybucji, uwagi dotyczące obsługi i odpowiednie oznaczenia poziomów bezpieczeństwa (jeśli istnieją) informacji;

b. Niw wymaga znakowania nośników [*Realizacja: określone przez organizację typy nośników systemu teleinformatycznego*], dopóki pozostają one w strefach kontrolowanych przez organizację [*Realizacja: kontrolowane przez organizację obszary]*.

Zabezpieczenia powiązane: AC-16, PL-2, RA-3.

Zabezpieczenia rozszerzone: Brak.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P2	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	MP-3 (opcjonalnie)	MP-3	MP-3

MP-4 PRZECHOWYWANIE NOŚNIKÓW

Zabezpieczenie: Organizacja:

a. Fizycznie kontroluje i bezpiecznie przechowuje nośniki [*Realizacja: zdefiniowane przez organizację typy mediów cyfrowych i / lub nie cyfrowych*] w strefach kontrolowanych przez organizację [*Realizacja: obszary kontrolowane zdefiniowane przez organizację*];

b. Chroni nośniki systemu teleinformatycznego, dopóki nie zostaną one zniszczone lub poddane sanityzacji przy użyciu zatwierdzonego sprzętu, technik i procedur.

Zabezpieczenia powiązane: CP-6, CP-9, MP-2, MP-7, PE-3.

Zabezpieczenia rozszerzone:

(1) PRZECHOWYWANIE NOŚNIKÓW | OCHRONA KRYPTOGRAFICZNA

[Włączony do SC-28 (1)].

(2) PRZECHOWYWANIE NOŚNIKÓW | OGRANICZONY DOSTĘP AUTOMATYCZNY

Organizacja stosuje zautomatyzowane mechanizmy ograniczające dostęp do obszarów przechowywania multimediów oraz kontrolujące próby dostępu i przyznany dostęp.

Zautomatyzowane mechanizmy mogą obejmować na przykład klawiatury na zewnętrznych wejściach do obszarów przechowywania multimediów.

Zabezpieczenia powiązane: AU-2, AU-9, AU-6, AU-12.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	MP-4 (opcjonalnie)	MP-4	MP-4

MP-5 TRANSPORT NOŚNIKÓW

Zabezpieczenie: Organizacja:

a. Chroni i kontroluje nośniki [*Realizacja: zdefiniowane przez organizację nośniki systemu teleinformatycznego*] podczas transportu poza strefy kontrolne organizacji przy użyciu [*Realizacja: zabezpieczenia bezpieczeństwa zdefiniowane przez organizację*];

b. Utrzymuje odpowiedzialność za media systemu teleinformatycznego podczas transportu poza strefy kontrolowane;

c. Dokumentuje działania związane z transportem mediów systemu teleinformatycznego;

d. Zezwala na wykonywanie czynności związanych z transportem nośników systemu teleinformatycznego tylko przez upoważniony personel.

Zabezpieczenia powiązane: AC-19, CP-9, MP-3, MP-4, RA-3, SC-8, SC-13, SC-28.

Zabezpieczenia rozszerzone:

(1) TRANSPORT NOŚNIKÓW DANYCH | OCHRONA POZA STREFAMI KONTROLNYMI

[Włączone do MP-5].

(2) TRANSPORT NOŚNIKÓW | DOKUMENTACJA DZIAŁAŃ

[Włączone do MP-5].

(3) TRANSPORT NOŚNIKÓW | KONWOJENCI

Organizacja zatrudnia konwojentów /nadzorujących transport nośników danych systemu teleinformatycznego poza obszary kontrolowane.

(4) TRANSPORT NOŚNIKÓW | OCHRONA KRYPTOGRAFICZNA

System teleinformatyczny implementuje mechanizmy kryptograficzne w celu ochrony poufności i integralności informacji przechowywanych na nośnikach danych podczas transportu poza kontrolowane obszary.

Zabezpieczenia powiązane: MP-2.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	MP-5 (opcjonalnie)	MP-5 (4)	MP-5 (4)

MP-6 SANITYZACJA NOŚNIKÓW

Zabezpieczenie: Organizacja:

a. Usuwa dane z nośników [*Realizacja: zdefiniowane przez organizację nośniki danych*] przed wyniesieniem poza strefę kontrolną organizacji lub ponownym użyciem przez zastosowanie [*Realizacja: zdefiniowane przez organizację techniki i procedury sanityzacji*] zgodnie z obowiązującymi przepisami, standardami i zasadami;

b. Stosuje mechanizmy usuwania danych o sile i integralności proporcjonalnej do kategorii bezpieczeństwa lub klasyfikacji przetwarzanej informacji.

Zabezpieczenia powiązane: MA-2, MA-4, RA-3, SC-4.

Zabezpieczenia rozszerzone:

(1) SANITYZACJA NOŚNIKÓW | PRZEGLĄD / ZATWIERDZANIE / ŚLEDZENIE / DOKUMENTOWANIE / WERYFIKACJA

Organizacja przegląda, zatwierdza, śledzi, dokumentuje i weryfikuje działania związane z sanityzacją nośników danych oraz ich niszczeniem.

Zabezpieczenia powiązane: SI-12.

(2) SANITYZACJA NOŚNIKÓW | TESTOWANIE SPRZĘTU

Organizacja testuje sprzęt i procedury sanityzacji z częstotliwością [*Realizacja: częstotliwość określona przez organizację*], celem sprawdzenia spełnienia wymagań w zakresie sanityzacji nośników danych.

(3) SANITYZACJA NOŚNIKÓW | TECHNIKI NIEDESTRUKCYJNE

Organizacja stosuje niedestrukcyjne techniki sanityzacji przenośnych urządzeń pamięci masowej przed podłączeniem takich urządzeń do systemu teleinformatycznego w następujących okolicznościach: [*Realizacja: określone przez organizację okoliczności wymagające sanityzacji przenośnych urządzeń pamięci masowej*].

Zabezpieczenia powiązane: SI-3.

(4) SANITYZACJA NOŚNIKÓW | KONTROLOWANE INFORMACJE JAWNE

[Włączone do MP-6].

(5) SANITYZACJA NOŚNIKÓW | INFORMACJE NIEJAWNE[38]

[Włączono do MP-6].

(6) SANITYZACJA NOŚNIKÓW | NISZCZENIE MEDIÓW

[Włączono do MP-6].

(7) SANITYZACJA NOŚNIKÓW | PODWÓJNA AUTORYZACJA

Organizacja wymusza podwójną autoryzację w celu przeprowadzenia sanityzacji nośników [*Realizacja: media systemu teleinformatycznego zdefiniowane przez organizację*].

Zabezpieczenia powiązane: AC-3, MP-2.

(8) SANITYZACJA NOŚNIKÓW | ZDALNE KASOWANIE / WYMAZYWANIE INFORMACJI

Organizacja zapewnia możliwość kasowania / wymazywania informacji z [*Realizacja: zdefiniowane przez organizację systemy informacyjne, komponenty systemu lub urządzenia*] zdalnie pod następującymi warunkami: [*Realizacja: warunki zdefiniowane przez organizację*].

[38] Zastosowanie mają przepisy ustawy o ochronie informacji niejawnych.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	MP-6	MP-6	MP-6 (1) (2) (3)

MP-7 UŻYWANIE NOŚNIKÓW

Zabezpieczenie: Organizacja [*Realizacja: ogranicza; zabrania*] korzystania z [*Realizacja: zdefiniowane przez organizację nośniki systemu teleinformatycznego*] w [*Realizacja: zdefiniowane przez organizację systemy informacyjne lub komponenty systemu*] przy użyciu [*Realizacja: zabezpieczenia bezpieczeństwa zdefiniowane przez organizację*].

Zabezpieczenia powiązane: AC-19, PL-4.

Zabezpieczenia rozszerzone:

(1) UŻYWANIE NOŚNIKÓW | ZABRONIONE WYKORZYSTANIE NIEZIDENTYFIKOWANEJ WŁASNOŚCI

Organizacja zabrania używania przenośnych urządzeń pamięci masowej w systemach teleinformatycznych, gdy takie urządzenia nie mają zidentyfikowanego właściciela.

Zabezpieczenia powiązane: PL-4.

(2) UŻYWANIE NOŚNIKÓW | ZABRONIONE WYKORZYSTANIE MEDIÓW ODPORNYCH NA SANITYZACJĘ

Organizacja zabrania używania w organizacyjnych systemach teleinformatycznych nośników danych odpornych na sanityzację.

Zabezpieczenia powiązane: MP-6.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	MP-7	MP-7 (1)	MP-7 (1)

MP-8 DEKLASYFIKACJA NOŚNIKÓW

Zabezpieczenie: Organizacja:

a. Ustanawia [*Realizacja: proces obniżenia klasyfikacji (deklasyfikację) nośników danych zdefiniowany przez organizację*], który obejmuje zastosowanie mechanizmów deklasyfikacji w [*Realizacja: siła i integralność zdefiniowana przez organizację*];

b. Zapewnia, że proces deklasyfikacji nośników danych jest współmierny do kategorii bezpieczeństwa i / lub poziomu klasyfikacji informacji, które mają zostać usunięte, oraz posiadanych upoważnień użytkowników do dostępu do zdeklasyfikowanych informacji;

c. Identyfikuje nośniki danych [*Realizacja: zdefiniowane przez organizację nośniki systemu teleinformatycznego wymagające deklasyfikacji*] do deklasyfikacji;

d. Deklasyfikuje zidentyfikowane nośniki danych za pomocą ustanowionego procesu.

Zabezpieczenia rozszerzone:

(1) DEKLASYFIKACJA NOŚNIKÓW | DOKUMENTACJA PROCESU

Organizacja dokumentuje działania związane z deklasyfikacją nośników danych**.**

(2) DEKLASYFIKACJA NOŚNIKÓW | TESTOWANIE SPRZĘTU

Organizacja stosuje testy [*Realizacja: testy zdefiniowane przez organizację*] deklasyfikacji sprzętu i procedur w celu weryfikacji prawidłowości wykonania tego procesu z częstotliwością [*Realizacja: częstotliwość zdefiniowana przez organizację*].

(3) DEKLASYFIKACJA NOŚNIKÓW | KONTROLOWANE INFORMACJE JAWNE

Organizacja deklasyfikuje nośniki danych zawierającego informacje [*Realizacja: zdefiniowane przez organizację kontrolowane informacje jawne*] przed ich publicznym udostępnieniem, zgodnie z obowiązującymi przepisami, normami i zasadami organizacyjnymi.

(4) DEKLASYFIKACJA NOŚNIKÓW | INFORMACJE NIEJAWNE

Organizacja dokonuje deklasyfikacji (obniżenia klauzuli informacji) nośników danych zawierających informacje niejawne przed ich udostępnieniem osobom nieposiadającym stosownych poświadczeń bezpieczeństwa.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P0	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	MP-8 (opcjonalnie)	MP-8 (opcjonalnie)	MP-8 (opcjonalnie)

KATEGORIA: OCHRONA FIZYCZNA I ŚRODOWISKOWA

PE-1 POLITYKA I PROCEDURY OCHRONY FIZYCZNEJ I ŚRODOWISKOWEJ

Zabezpieczenie: Organizacja:

a. Opracowuje, dokumentuje i rozpowszechnia w odniesieniu do [*Realizacja: personel lub role zdefiniowane przez organizację*]:

   1. Politykę ochrony fizycznej i środowiskowej, która dotyczy celu, zakresu, ról, obowiązków, zaangażowania kierownictwa, koordynacji między jednostkami organizacyjnymi oraz zgodności z ustalonymi normami;

   2. Procedury ułatwiające wdrażanie polityki ochrony fizycznej i środowiskowej oraz powiązane zabezpieczenia;

b. Przegląda i aktualizuje bieżące:

   1. Polityki ochrony fizycznej i środowiskowej z częstotliwością *[Realizacja: częstotliwość określona przez organizację*];

   2. Procedury ochrony fizycznej i środowiskowej z częstotliwością [*Realizacja: częstotliwość określona przez organizację*].

Zabezpieczenia powiązane: PM-9.

Zabezpieczenia rozszerzone: Brak.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	PE-1	PE-1	PE-1

PE-2 ZEZWOLENIA NA DOSTĘP FIZYCZNY

Zabezpieczenie: Organizacja:

a. Opracowuje, zatwierdza i utrzymuje listę osób z uprawnionym dostępem do obiektu, w którym znajduje się system teleinformatyczny;

b. Wystawia poświadczenia (przepustki) dostępu do obiektu;

c. Przegląda listę dostępu wyszczególniając osoby fizyczne posiadające autoryzowany dostęp do obiektu [*Realizacja: częstotliwość określona przez organizację*] ;

d. Dokonuje aktualizacji listy osób posiadających dostęp do obiektu.

Zabezpieczenia powiązane: PE-3, PE-4, PS-3.

Zabezpieczenia rozszerzone:

(1) ZEZWOLENIA NA DOSTĘP FIZYCZNY | DOSTĘP ZGODNIE Z POSIADANĄ POZYCJĄ / ROLĄ

Organizacja zezwala na fizyczny dostęp do obiektu, w którym znajduje się system teleinformatyczny, w zależności od posiadanego stanowiska lub roli.

Zabezpieczenia powiązane: AC-2, AC-3, AC-6.

(2) ZEZWOLENIA NA DOSTĘP FIZYCZNY | PODWÓJNA IDENTYFIKACJA

Organizacja wymaga dwóch form identyfikacji z [*Realizacja: zdefiniowana przez organizację lista dopuszczalnych form identyfikacji*] w celu uzyskania dostępu gości do obiektu, w którym znajduje się system teleinformatyczny.

Zabezpieczenia powiązane: IA-2, IA-4, IA-5.

(3) ZEZWOLENIA NA DOSTĘP FIZYCZNY | OGRANICZANIE DOSTĘPU BEZ ASYSTY

Organizacja ogranicza dostęp bez asysty do obiektu, w którym znajduje się system teleinformatyczny, do personelu z [*Wybór (jeden lub więcej): z poświadczeniami bezpieczeństwa do wszystkich informacji zawartych w systemie; z formalną autoryzacją dostępu do wszystkich informacji zawartych w systemie; z potrzebą dostępu do wszystkich informacji zawartych w systemie; [Realizacja: posiadającymi poświadczenia zdefiniowane przez organizację*]].

Zabezpieczenia powiązane: PS-2, PS-6.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	PE-2	PE-2	PE-2

PE-3 KONTROLA DOSTĘPU FIZYCZNEGO

Zabezpieczenie: Organizacja:

a. Wymusza autoryzację fizycznego dostępu w punktach *[Realizacja: zdefiniowane przez organizację punkty wejścia / wyjścia do obiektu, w którym znajduje się system teleinformatyczny*] poprzez:

1. Weryfikację indywidualnych zezwoleń na dostęp, przed udzieleniem dostępu do obiektu;

2. Kontrolowanie wejścia / wyjścia do obiektu za pomocą [*Wybór (jeden lub więcej): [Realizacja: zdefiniowane przez organizację fizyczne systemy / urządzenia kontroli dostępu]; ochrona*];

b. Prowadzenie dziennika kontroli dostępu fizycznego w [*Realizacja: punkty wejścia / wyjścia zdefiniowane przez organizację*];

c. Zapewnienie [*Realizacja: zapewnienie poziomu bezpieczeństwa określonego przez organizację*] w celu kontroli dostępu do obszarów obiektu oficjalnie wyznaczonych jako publicznie dostępne;

d. Doprowadzanie odwiedzających i monitorowanie aktywności odwiedzających w okolicznościach [*Realizacja: określone przez organizację okoliczności wymagające eskorty i monitorowania gości*];

e. Zabezpieczanie kluczy, zestawów kontroli i innych fizycznych urządzeń dostępowych;

f. Sprawdzanie / inwentaryzacje urządzeń dostępowych [39][*Realizacja: fizyczne urządzenia dostępu zdefiniowane przez organizację*] z częstotliwością [*Realizacja: częstotliwość zdefiniowana przez organizację*];

g. Zmienia kombinacje i klucze z częstotliwością [*Realizacja: częstotliwość zdefiniowana przez organizację*] i / lub gdy klucze zostaną zagubione, kombinacje zostaną naruszone lub poszczególne osoby zostaną przeniesione lub zwolnione z organizacji.

Zabezpieczenia powiązane: AU-2, AU-6, MP-2, MP-4, PE-2, PE-4, PE-5, PS-3, RA-3.

Zabezpieczenia rozszerzone:

(1) KONTROLA DOSTĘPU FIZYCZNEGO | DOSTĘP DO SYSTEMU TELEINFORMATYCZNEGO

Organizacja wymusza, oprócz fizycznej kontroli dostępu do obiektu, uwierzytelnianie dostępu fizycznego do systemu teleinformatycznego w [*Realizacja: zdefiniowane przez organizację przestrzenie fizyczne zawierające jeden lub więcej elementów systemu teleinformatycznego*].

Zabezpieczenia powiązane: PS-2.

(2) KONTROLA DOSTĘPU FIZYCZNEGO | OBIEKT / OBSZAR SYSTEMU TELEINFORMATYCZNEGO

Organizacja przeprowadza kontrole bezpieczeństwa z częstotliwością [*Realizacja: częstotliwość zdefiniowana przez organizację*] w zakresie dostępu do fizycznej strefy obiektu lub dostępu do systemu teleinformatycznego w celu uniemożliwienia nieautoryzowanego upublicznienia informacji lub usunięcia elementów systemu teleinformatycznego**.**

Zabezpieczenia powiązane: AC-4, SC-7.

(3) KONTROLA DOSTĘPU FIZYCZNEGO | CIĄGŁOŚĆ OCHRONY / ALARMY / MONITOROWANIE

Organizacja zatrudnia ochronę i / lub wprowadza system kontroli dostępu w celu monitorowania każdego fizycznego punktu dostępu do obiektu, w którym znajduje się system teleinformatyczny. Ochrona funkcjonuje w trybie 24 godziny na dobę, 7 dni w tygodniu przez cały rok.

[39] Urządzenia dostępu fizycznego obejmują np. klucze, zamki, kombinacje i czytniki kart. Zabezpieczenia ogólnodostępnych obszarów w obiektach organizacyjnych obejmują np. kamery, monitorowanie przez ochronę i izolowanie wybranych systemów teleinformatycznych i / lub elementów systemu w zabezpieczonych obszarach.

Zabezpieczenia powiązane: CP-6, CP-7.

(4) KONTROLA DOSTĘPU FIZYCZNEGO | ZAMYKANE OBUDOWY

Organizacja wykorzystuje zamykane obudowy fizyczne w celu ochrony [*Realizacja: komponenty systemu teleinformatycznego zdefiniowane przez organizację*] przed nieuprawnionym dostępem fizycznym.

(5) KONTROLA DOSTĘPU FIZYCZNEGO | OCHRONA PRZED MANIPULACJĄ

Organizacja stosuje [*Realizacja: środki bezpieczeństwa zdefiniowane przez organizację*[40]] do [*Wybór (jeden lub więcej): wykrycie; zapobieganie*] fizycznym manipulacjom lub zmianom [*Realizacja: komponenty sprzętowe zdefiniowane przez organizację] w systemie teleinformatycznym*].

Zabezpieczenia powiązane: SA-12.

(6) KONTROLA DOSTĘPU FIZYCZNEGO | TESTY PENETRACYJNE OBIEKTU

Organizacja stosuje testy penetracyjne z częstotliwością [*Realizacja: częstotliwości zdefiniowana przez organizację*], który obejmują niezapowiedziane próby ominięcia lub obejścia środków bezpieczeństwa związanych z fizycznymi punktami dostępu do obiektu.

Zabezpieczenia powiązane: CA-2, CA-7.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	PE-3	PE-3	PE-3 (1)

PE-4 KONTROLA DOSTĘPU DO MEDIUM TRANSMISYJNEGO

Zabezpieczenie: Organizacja kontroluje fizyczny dostęp do [*Realizacja: zdefiniowane przez organizację linie dystrybucji i transmisji*] w obrębie obiektów organizacyjnych, poprzez stosowanie [*Realizacja: wymagań bezpieczeństwa zdefiniowane przez organizację*[41]].

Zabezpieczenia powiązane: MP-2, MP-4, PE-2, PE-3, PE-5, SC-7, SC-8.

Zabezpieczenia rozszerzone: Brak.

Zabezpieczenia powiązane: Brak

[40] Np. uszczelki wykrywające manipulacje, powłoki zapobiegające manipulacjom.

[41] Wymagania bezpieczeństwa w zakresie kontroli dostępu fizycznego do linii dystrybucyjnych i transmisyjnych systemu obejmują na przykład: (i) zamknięte szafy na okablowanie; (ii) odłączone lub zablokowane zapasowe gniazda; i / lub (iii) ochrona okablowania w kanałach kablowych lub korytka kablowe.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	PE-4 (opcjonalnie)	PE-4	PE-4

PE-5 KONTROLA DOSTĘPU DO URZĄDZEŃ WEJŚCIA - WYJŚCIA

Zabezpieczenie: Organizacja kontroluje fizyczny dostęp do urządzeń wejścia - wyjścia systemu teleinformatycznego w celu uniemożliwienia osobom nieupoważnionym uzyskania dostępu do wyników przetwarzania informacji.

Zabezpieczenia powiązane: PE-2, PE-3, PE-4, PE-18.

Zabezpieczenia rozszerzone:

(1) KONTROLA DOSTĘPU DO URZĄDZEŃ WEJŚCIA - WYJŚCIA | DOSTĘP UPOWAŻNIONYCH OSÓB DO URZĄDZEŃ

Organizacja:

(a) Kontroluje fizyczny dostęp do danych wyjściowych z [*Realizacja: urządzenia wejścia - wyjścia zdefiniowane przez organizację*];

(b) Zapewnia, że tylko upoważnione osoby mają dostęp do danych wyjściowych z urządzenia.

(2) KONTROLA DOSTĘPU DO URZĄDZEŃ WEJŚCIA - WYJŚCIA | DOSTĘP DO DANYCH NA PODSTAWIE INDYWIDUALNEJ TOŻSAMOŚCI

System teleinformatyczny:

(a) Kontroluje dostęp fizyczny do danych wyjściowych[42] z [*Realizacja: urządzenia wejścia - wyjścia zdefiniowane przez organizację*];

(b) Łączy indywidualną tożsamość z udzielaniem dostępu do danych wyjściowych z urządzenia.

(3) KONTROLA DOSTĘPU DO URZĄDZEŃ WEJŚCIA - WYJŚCIA | OZNACZANIE URZĄDZEŃ WEJŚCIA - WYJŚCIA

Odpowiednie oznaczenia urządzeń użytkowanych w organizacji [*Realizacja: urządzenia wejścia - wyjścia systemu teleinformatycznego zdefiniowane przez organizację*] wskazują jakie informacje mogą być wysyłane z urządzenia (klasyfikacja informacji).

[42] Np. kod PIN, token sprzętowy implementowany na urządzeniach wyjściowych.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P2	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	PE-5 (opcjonalnie)	PE-5	PE-5

PE-6 MONITOROWANIE DOSTĘPU FIZYCZNEGO

Zabezpieczenie: Organizacja:

(1) Monitoruje dostęp fizyczny do obiektu, w którym znajduje się system teleinformatyczny, w celu wykrywania i reagowania na incydenty związane z bezpieczeństwem fizycznym;

(2) Przegląda dzienniki dostępu fizycznego z częstotliwością [*Realizacja: częstotliwość zdefiniowana przez organizację*] i po wystąpieniu [*Realizacja: zdarzenia zdefiniowane przez organizację lub potencjalne wskazania zdarzeń*];

(3) Koordynuje wyniki przeprowadzanych przeglądów i dochodzeń z możliwością reagowania na incydenty organizacyjne.

Zabezpieczenia powiązane: CA-7, IR-4, IR-8.

Zabezpieczenia rozszerzone:

(1) MONITOROWANIE DOSTĘPU FIZYCZNEGO | ALARMY WŁAMANIOWE / URZĄDZENIA NADZORUJĄCE

Organizacja monitoruje alarmy włamaniowe i sprzęt nadzorujący fizyczną kontrolę dostępu.

(2) MONITOROWANIE DOSTĘPU FIZYCZNEGO | AUTOMATYCZNE ROZPOZNAWANIE WŁAMANIA / INFORMOWANIE

Organizacja wykorzystuje zautomatyzowane mechanizmy do rozpoznawania [*Realizacja: rodzaje włamań zdefiniowane przez organizację*] i inicjowania działań [*Realizacja: działania reagowania zdefiniowane przez organizację*].

Zabezpieczenia powiązane: SI-4.

(3) MONITOROWANIE DOSTĘPU FIZYCZNEGO | MONITORING WIZYJNY

Organizacja stosuje monitoring wideo w strefach [*Realizacja: obszary operacyjne zdefiniowane przez organizację*] i zachowuje nagrania wideo przez okres [*Realizacja: okres zdefiniowany przez organizację*].

(4) MONITOROWANIE DOSTĘPU FIZYCZNEGO | MONITOROWANIE DOSTĘPU FIZYCZNEGO DO SYSTEMÓW TELEINFORMATYCZNYCH

Oprócz monitorowania dostępu fizycznego do obiektu, organizacja monitoruje dostęp fizyczny do systemu teleinformatycznego eksploatowanego w [*Realizacja: zdefiniowane przez organizację przestrzenie fizyczne*[43] *zawierające jeden lub więcej elementów systemu teleinformatycznego*].

Zabezpieczenia powiązane: PS-2, PS-3.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	PE-6	PE-6 (1)	PE-6 (1) (4)

PE-7 KONTROLA GOŚCI

[Włączony do PE-2 i PE-3].

PE-8 REJESTRACJA DOSTĘPU GOŚCI

Zabezpieczenie: Organizacja:

a. Prowadzi zapisy dotyczące dostępu osób odwiedzających do obiektu, w którym znajduje się system teleinformatyczny i przechowuje je przez okres [*Realizacja: okres zdefiniowany przez organizację*];

b. Przegląda ewidencję osób odwiedzających z częstotliwością [*Realizacja: częstotliwość zdefiniowana przez organizację]*.

Zabezpieczenia rozszerzone:

(1) REJESTRACJA DOSTĘPU GOŚCI | AUTOMATYCZNA REJESTRACJA / PRZEGLĄD

Organizacja stosuje zautomatyzowane mechanizmy ułatwiające utrzymanie i przegląd zapisów dotyczących dostępu osób odwiedzających.

(2) REJESTRACJA DOSTĘPU GOŚCI | EWIDENCJA DOSTĘPU FIZYCZNEGO

[Włączone do PE-2].

[43] Np. serwerownie, obszary przechowywania mediów, centra komunikacyjne, centra przetwarzania danych.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P3	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	PE-8	PE-8	PE-8 (1)

PE-9 WYPOSAŻENIE ENERGETYCZNE I OKABLOWANIE

Zabezpieczenie: Organizacja chroni sprzęt zasilający i okablowanie energetyczne systemu teleinformatycznego przed uszkodzeniem i zniszczeniem.

Zabezpieczenia powiązane: PE-4.

Zabezpieczenia rozszerzone:

(1) WYPOSAŻENIE ENERGETYCZNE I OKABLOWANIE | REDUNDANCJA OKABLOWANIA

Organizacja stosuje nadmiarowe tory zasilania energetycznego, które są fizycznie rozdzielone i poprowadzone odrębnymi trasami kablowymi.

(2) WYPOSAŻENIE ENERGETYCZNE I OKABLOWANIE | AUTOMATYCZNA KONTROLA NAPIĘCIA

Organizacja stosuje automatyczne kontrole napięcia w elementach [*Realizacja: zdefiniowane przez organizację elementy systemu informacji krytycznej*].

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	PE-9 (opcjonalnie)	PE-9	PE-9

PE-10 WYŁĄCZENIE AWARYJNE

Zabezpieczenie: Organizacja:

a. Zapewnia możliwość odcięcia zasilania systemu teleinformatycznego lub poszczególnych elementów systemu w sytuacjach awaryjnych;

b. Umieszcza wyłączniki lub urządzenia wyłączania awaryjnego w [*Realizacja: lokalizacja zdefiniowana przez organizację w której znajduje się system teleinformatyczny lub elementu systemu*], w sposób umożliwiający personelowi bezpieczny i łatwy dostęp;

c. Zabezpiecza wyłączniki / urządzenia wyłączania awaryjnego przed nieuprawnioną aktywacją.

Zabezpieczenia powiązane: PE-15.

Zabezpieczenia rozszerzone:

(1) WYŁĄCZENIE AWARYJNE | PRZYPADKOWA / NIEAUTORYZOWANA AKTYWACJA

[Włączono do PE-10].

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	PE-10 (opcjonalnie)	PE-10	PE-10

PE-11 ZASILANIE AWARYJNE

Zabezpieczenie: Organizacja zapewnia krótkoterminowe źródła podtrzymania zasilania (UPS) w celu zapewnienia [*Wybór (jeden lub więcej): wyłączenia systemu teleinformatycznego; przejście systemu teleinformatycznego na długoterminowe źródło zapasowe*] w przypadku utraty podstawowego źródła zasilania.

Zabezpieczenia powiązane: AT-3, CP-2, CP-7.

Zabezpieczenia rozszerzone:

(1) ZASILANIE AWARYJNE | DŁUGOTERMINOWE ALTERNATYWNE ZASILANIE - MINIMALNA ZDOLNOŚĆ OPERACYJNA

Organizacja zapewnia długoterminowe alternatywne źródło zasilania systemu teleinformatycznego, które jest w stanie utrzymać minimalną wymaganą zdolność operacyjną w przypadku przedłużonej niedostępności podstawowego źródła zasilania.

(2) ZASILANIE AWARYJNE | DŁUGOTERMINOWE ALTERNATYWNE SAMOOBSŁUGOWE ŹRÓDŁO ZASILANIA

Organizacja zapewnia długoterminowe alternatywne źródło zasilania systemu teleinformatycznego, które:

(a) Jest samoobsługowe (autostart);

(b) Niezależne od zewnętrznego przyłącza energetycznego;

(c) Zdolne do utrzymania [*Realizacja: Wybór: minimalnie wymagana zdolność operacyjna; pełna zdolność operacyjna*] w przypadku przedłużonej utraty dostępności podstawowego źródła zasilania.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	PE-11 (opcjonalnie)	PE-11	PE-11 (1)

PE-12 OŚWIETLENIE AWARYJNE

Zabezpieczenie: Organizacja stosuje i serwisuje automatyczne oświetlenie awaryjne, które aktywuje się w przypadku przerwy w dostawie energii elektrycznej lub zakłócenia jej dostawy i które obejmuje wyjścia ewakuacyjne i drogi ewakuacyjne w obiekcie.

Zabezpieczenia powiązane: CP-2, CP-7.

Zabezpieczenia rozszerzone:

(1) OŚWIETLENIE AWARYJNE | ZASADNICZE DZIAŁANIA / FUNKCJE BIZNESOWE

Organizacja zapewnia oświetlenie awaryjne we wszystkich obszarach w obiekcie, wspierając niezbędne działania i funkcje biznesowe.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	PE-12	PE-12	PE-12

PE-13 OCHRONA PRZECIWPOŻAROWA

Zabezpieczenie: Organizacja stosuje i utrzymuje urządzenia / systemy wykrywania i gaszenia pożaru w pomieszczeniach koncentrujących system teleinformatyczny, które są zasilane przez niezależne źródło energetyczne.

Zabezpieczenia rozszerzone:

(1) OCHRONA PRZECIWPOŻAROWA | URZĄDZENIA / SYSTEMY WYKRYWANIA

Organizacja stosuje urządzenia / systemy wykrywania pożaru w obiektach systemu teleinformatycznego, które, w przypadku pożaru automatycznie aktywują się i powiadamiają [*Realizacja: personel lub role zdefiniowane przez organizację*] oraz [*Realizacja: osoby reagujące na sytuacje kryzysowe określone przez organizację*].

(2) OCHRONA PRZECIWPOŻAROWA | URZĄDZENIA / SYSTEMY GASZENIA

Organizacja stosuje urządzenia / systemy gaszenia pożaru w obiektach systemu teleinformatycznego, zapewniające automatyczne powiadamianie o każdej aktywacji systemu ppoż. personel[*Realizacja: personel lub role zdefiniowane przez organizację*] i [*Realizacja: zdefiniowane przez organizację osoby udzielające pomocy*].

(3) OCHRONA PRZECIWPOŻAROWA | AUTOMATYCZNE GASZENIE POŻARU

Organizacja stosuje funkcję automatycznego gaszenia pożaru w obiekcie systemu teleinformatycznego, gdy w obiekcie nie jest wykonywana praca zmianowa (ciągła).

(4) OCHRONA PRZECIWPOŻAROWA | INSPEKCJE

Organizacja zapewnia, że obiekt przechodzi z częstotliwością [*Realizacja: częstotliwość określona przez organizację*] inspekcje przez upoważnionych i wykwalifikowanych inspektorów i usuwane są zidentyfikowane podczas inspekcji niedociągnięcia w ciągu [*Realizacja: czas określony przez organizację*].

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	PE-13	PE-13 (3)	PE-13 (1) (2) (3)

PE-14 KONTROLA TEMPERATURY I WILGOTNOŚCI

Zabezpieczenie: Organizacja:

a. Utrzymuje poziomy temperatury i wilgotności w obiekcie, w którym znajduje się system teleinformatyczny w granicach [*Realizacja: dopuszczalne poziomy zdefiniowane przez organizację*];

b. Monitoruje poziomy temperatury i wilgotności z częstotliwością [*Realizacja: częstotliwość określona przez organizację*].

Zabezpieczenia powiązane: AT-3.

Zabezpieczenia rozszerzone:

(1) KONTROLA TEMPERATURY I WILGOTNOŚCI | STEROWANIE AUTOMATYCZNE

Organizacja stosuje automatyczną kontrolę temperatury i wilgotności w obiekcie w celu zapobiegania wahaniom zadanych wartości, potencjalnie szkodliwych dla systemu teleinformatycznego.

(2) KONTROLA TEMPERATURY I WILGOTNOŚCI | MONITOROWANIE, ALARMOWANIE / POWIADOMIENIA

Organizacja stosuje systemy monitorowania temperatury i wilgotności, które zapewniają generowanie alarmów lub powiadomień o zmianach zadanych wartości, potencjalnie szkodliwych dla personelu lub sprzętu.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	PE-14	PE-14	PE-14

PE-15 OCHRONA PRZED ZALANIEM

Zabezpieczenie: Organizacja chroni system teleinformatyczny przed uszkodzeniami wynikającymi z wycieku wody, zapewniając główne zawory odcinające, które są dostępne, działają prawidłowo i rozmieszczenie których znane jest kluczowemu personelowi.

Zabezpieczenia powiązane: AT-3.

Zabezpieczenia rozszerzone:

(1) OCHRONA PRZED ZALANIEM | AUTOMATYCZNE WYKRYWANIE

Organizacja stosuje zautomatyzowane mechanizmy wykrywania obecności wody w pobliżu systemu teleinformatycznego i ostrzega [*Realizacja: personel lub role zdefiniowane przez organizację*].

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	PE-15	PE-15	PE-15 (1)

PE-16 DOSTAWA I USUWANIE

Zabezpieczenie: Organizacja dopuszcza, monitoruje i kontroluje [*Realizacja: typy komponentów systemu teleinformatycznego zdefiniowane przez organizację*] instalowany i deinstalowany w obiekcie oraz prowadzi rejestr tych pozycji.

Zabezpieczenia powiązane: CM-3, MA-2, MA-3, MP-5, SA-12.

Zabezpieczenia rozszerzone: Brak.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P2	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	PE-16	PE-16	PE-16

PE-17 ZAPASOWE MIEJSCE PRACY

Zabezpieczenie: Organizacja:

a. Wprowadza [*Realizacja: środki bezpieczeństwa zdefiniowane przez organizację*] w zapasowych miejscach pracy;

b. Ocenia skuteczność środków bezpieczeństwa stosowanych w zapasowych miejscach pracy;

c. Zapewnia pracownikom środki komunikacji z personelem ds. bezpieczeństwa informacji w przypadku wystąpienia incydentów lub problemów związanych z bezpieczeństwem.

Zabezpieczenia powiązane: AC-17, CP-7.

Zabezpieczenia rozszerzone: Brak.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P2	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	PE-17 (opcjonalnie)	PE-17	PE-17

PE-18 LOKALIZACJA ELEMENTÓW SYSTEMU TELEINFORMATYCZNEGO

Zabezpieczenie: Organizacja umieszcza komponenty systemu teleinformatycznego w stosownym obiekcie, celem zminimalizowania potencjalnych szkód wynikających z [*Realizacja: zdefiniowane przez organizację zagrożenia fizyczne i środowiskowe*] oraz zminimalizowania możliwość nieautoryzowanego dostępu.

Zabezpieczenia powiązane: CP-2, PE-19, RA-3.

Zabezpieczenia rozszerzone:

(1) LOKALIZACJA KOMPONENTÓW SYSTEMU INFORMATYCZNEGO | LOKALIZACJA OBIEKTU

Organizacja planuje lokalizację obiektu, w którym rezyduje system teleinformatyczny, uwzględniając zagrożenia fizyczne i środowiskowe, a w przypadku istniejących obiektów uwzględnia zagrożenia fizyczne i środowiskowe w swojej strategii ograniczania ryzyka.

Zabezpieczenia powiązane: PM-8.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P3	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	PE-18 (opcjonalnie)	PE-18 (opcjonalnie)	PE-18 (opcjonalnie)

PE-19 ULOT INFORMACJI / ELEKTROMAGNETYCZNA EMISJA UJAWNIAJĄCA

Zabezpieczenie: Organizacja chroni system teleinformatyczny przed ulotem informacji spowodowanym emisją sygnałów elektromagnetycznych.

Zabezpieczenia rozszerzone:

(1) ULOT INFORMACJI | / POLITYKI I PROCEDURY (TEMPEST)

Organizacja zapewnia ochronę komponentów systemu teleinformatycznego, powiązanej transmisji danych i sieci zgodnie z krajowymi politykami i procedurami dotyczącymi emisji i rozwiązania TEMPEST w oparciu o kategorię bezpieczeństwa lub klasyfikację informacji.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P0	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	PE-19 (opcjonalnie)	PE-19 (opcjonalnie)	PE-19 (opcjonalnie)

PE-20 MONITOROWANIE I ŚLEDZENIE ZASOBÓW

Zabezpieczenie: Organizacja:

a. Wykorzystuje *[Realizacja: technologie lokalizacji zasobów zdefiniowane przez organizację*] do śledzenia i monitorowania lokalizacji i przemieszczania się [*Realizacja: zasoby zdefiniowane przez organizację*] w obrębie [*Realizacja: obszary kontrolowane przez organizację*];

b. Zapewnia, że technologie lokalizacji zasobów są stosowane zgodnie z obowiązującymi przepisami prawnymi, zarządzeniami wykonawczymi, dyrektywami, politykami, standardami i wytycznymi.

Zabezpieczenia powiązane: CM-8.

Zabezpieczenia rozszerzone: Brak.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P0	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	PE-20 (opcjonalnie)	PE-20 (opcjonalnie)	PE-20 (opcjonalnie)

KATEGORIA: PLANOWANIE

PL-1 POLITYKA I PROCEDURY PLANOWANIA BEZPIECZEŃSTWA

Zabezpieczenie: Organizacja:

a. Opracowuje, dokumentuje i rozpowszechnia w odniesieniu do [*Realizacja: personel lub role zdefiniowane przez organizację*]:

   1. Politykę planowania bezpieczeństwa, która dotyczy celu, zakresu, ról, obowiązków, zaangażowania kierownictwa, koordynacji między jednostkami organizacyjnymi i spójności działania;

   2. Procedury ułatwiające wdrożenie polityki planowania bezpieczeństwa i powiązanych planowanych środków bezpieczeństwa;

b. Recenzuje i aktualizuje aktualną:

   1. Politykę planowania bezpieczeństwa z częstotliwością [*Realizacja: częstotliwość określona przez organizację*];

   2. Procedury planowania bezpieczeństwa z częstotliwością [*Realizacja: częstotliwość określona przez organizację*].

Zabezpieczenia powiązane: PM-9.

Zabezpieczenia rozszerzone: Brak.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	PL-1	PL-1	PL-1

PL-2 PLAN BEZPIECZEŃSTWA SYSTEMU

Zabezpieczenie: Organizacja:

a. Opracowuje plan bezpieczeństwa systemu teleinformatycznego, który:

   1. Jest zgodny ze strukturą organizacji;

   2. Definiuje obszary autoryzacji systemu;

   3. Opisuje środowisko operacyjne systemu teleinformatycznego w kontekście misji i procesów biznesowych;

   4. Zapewnia kategoryzację bezpieczeństwa systemu teleinformatycznego, w tym uzasadnienie;

5. Opisuje środowisko operacyjne systemu teleinformatycznego oraz relacje z innymi systemami teleinformatycznymi lub połączenia z nimi;
6. Zawiera przegląd wymagań bezpieczeństwa odnoszących się do systemu;
7. W stosownych przypadkach określa wszelkie odpowiednie poprawki (patche) bezpieczeństwa;
8. Opisuje środki bezpieczeństwa stosowane lub planowane w celu spełnienia wymagań, w tym uzasadnienie decyzji dostosowawczych;
9. Jest sprawdzany i zatwierdzany przed realizacją planu, przez kierownika jednostki organizacyjnej lub osobę przez niego upoważnioną;

b. Dystrybuuje kopie planu bezpieczeństwa i informuje o kolejnych zmianach w planie personelowi [*Realizacja: personel lub role zdefiniowane przez organizację*];

c. Przegląda plan bezpieczeństwa systemu teleinformatycznego pod względem aktualności z częstotliwością [*Realizacja: częstotliwość określona przez organizację*];

d. Aktualizuje plan bezpieczeństwa w celu uwzględnienia zmian w systemie teleinformatycznym / środowisku działania lub problemów zidentyfikowanych podczas wdrażania planu lub ocen kontroli bezpieczeństwa;

e. Chroni plan bezpieczeństwa przed nieuprawnionym ujawnieniem i modyfikacją.

Zabezpieczenia powiązane: AC-2, AC-6, AC-14, AC-17, AC-20, CA-2, CA-3, CA-7, CM-9, CP-2, IR-8, MA-4 , MA-5, MP-2, MP-4, MP-5, PL-7, PM-1, PM-7, PM-8, PM-9, PM-11, SA-5, SA-17.

Zabezpieczenia rozszerzone:

(1) PLAN BEZPIECZEŃSTWA SYSTEMU | KONCEPCJA DZIAŁANIA

[Włączone do PL-7].

(2) PLAN BEZPIECZEŃSTWA SYSTEMU | ARCHITEKTURA FUNKCJONALNA

[Włączone do PL-8].

(3) PLAN BEZPIECZEŃSTWA SYSTEMU | PLANOWANIE / KOORDYNACJA Z INNYMI PODMIOTAMI ORGANIZACYJNYMI

Organizacja planuje i koordynuje działania związane z bezpieczeństwem mające wpływ na system teleinformatyczny z [*Realizacja: określone osoby lub grupy zdefiniowane przez organizację*] przed przeprowadzeniem takich działań, w celu zmniejszenia wpływu na inne jednostki organizacyjne.

Zabezpieczenia powiązane: CP-4, IR-4.

Zabezpieczenia powiązane: Brak.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	PL-2	PL-2 (3	PL-2 (3)

PL-3 AKTUALIZACJA PLANU BEZPIECZEŃSTWA SYSTEMU

[Włączony do PL-2].

PL-4 ZASADY POSTĘPOWANIA

Zabezpieczenie: Organizacja:

a. Ustanawia i udostępnia osobom, które wymagają dostępu do systemu teleinformatycznego, zasady opisujące ich obowiązki i oczekiwane zachowanie w odniesieniu do korzystania z systemu teleinformatycznego i informacji w nich przetwarzanych;

b. Egzekwuje podpisanie przez te osoby potwierdzenia wskazującego, że przeczytały, zrozumiały i wyrażają zgodę na przestrzeganie zasad zachowania przed udzieleniem zgody na dostęp do informacji i systemu teleinformatycznego;

c. Przegląda i aktualizuje zasady zachowania z częstotliwością [*Realizacja: częstotliwość określona przez organizację*];

d. Wymaga od osób, które podpisały poprzednią wersję reguł zachowania, przeczytania i ponownego podpisania tych reguł, w przypadku ich zmiany / zaktualizowania.

Zabezpieczenia powiązane: AC-2, AC-6, AC-8, AC-9, AC-17, AC-18, AC-19, AC-20, AT-2, AT-3, CM-11, IA-2 , IA-4, IA-5, MP-7, PS-6, PS-8, SA-5.

Zabezpieczenia rozszerzone:

(1) ZASADY POSTĘPOWANIA | MEDIA SPOŁECZNE I OGRANICZENIA SIECIOWE

Organizacja zawiera w regulaminie postępowania wyraźne ograniczenia w korzystaniu z mediów społecznościowych / serwisów sieciowych oraz publikowanie informacji organizacyjnych w publicznych stronach internetowych.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P2	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	PL-4	PL-4 (1)	PL-4 (1)

PL-5 OCENA WPŁYWU NA PRYWATNOŚĆ

[Zgodnie z Ogólnym Rozporządzeniem o Ochronie Danych Osobowych 2016/679 (RODO)].

PL-6 PLANOWANIE DZIAŁALNOŚCI ZWIĄZANEJ Z BEZPIECZEŃSTWEM

[Włączony do PL-2].

PL-7 KONCEPCJA BEZPIECZEŃSTWA DZIAŁAŃ OPERACYJNYCH

Zabezpieczenie: Organizacja:

a. Opracowuje koncepcję bezpieczeństwa działań operacyjnych systemu teleinformatycznego określającą sposób, w jaki organizacja zamierza obsługiwać system z punktu widzenia bezpieczeństwa informacji;

b. Przegląda i aktualizuje koncepcję bezpieczeństwa działań operacyjnych z częstotliwością [*Realizacja: częstotliwość zdefiniowana przez organizację*].

Zabezpieczenia powiązane: PL-2.

Zabezpieczenia rozszerzone: Brak.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P0	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	PL-7 (opcjonalnie)	PL-7 (opcjonalnie)	PL-7 (opcjonalnie)

PL-8 ARCHITEKTURA BEZPIECZEŃSTWA INFORMACJI

Zabezpieczenie: Organizacja:

a. Opracowuje architekturę bezpieczeństwa informacji systemu teleinformatycznego, która opisuje:

   1. Ogólną filozofię, wymagania i podejście, które należy zastosować w odniesieniu do ochrony poufności, integralności i dostępności informacji organizacyjnych;

   2. Sposób, w jaki architektura bezpieczeństwa informacji jest zintegrowana z architekturą korporacyjną;

   3. Wszelkie założenia dotyczące bezpieczeństwa informacji i usług zewnętrznych;

b. Przegląda i aktualizuje architekturę bezpieczeństwa informacji z częstotliwością [*Realizacja: zdefiniowane przez organizację częstotliwość*] w celu odzwierciedlenia aktualizacji w architekturze korporacyjnej;

c. Zapewnia, że planowane zmiany architektury bezpieczeństwa informacji znajdują odzwierciedlenie w planie bezpieczeństwa, koncepcji bezpieczeństwa operacji oraz zamówieniach / zakupach organizacyjnych.

Zabezpieczenia powiązane: CM-2, CM-6, PL-2, PM-7, SA-5, SA-17.

Zabezpieczenia rozszerzone:

(1) ARCHITEKTURA BEZPIECZEŃSTWA INFORMACJI | ZABEZPIECZENIE WIELOSTOPNIOWE (OCHRONA WARSTWOWA)

Organizacja projektuje swoją architekturę bezpieczeństwa, stosując podejście do jej ochrony które:

(a) Przydziela [*Realizacja: środki bezpieczeństwa zdefiniowane przez organizację*] do [*Realizacja: lokalizacje zdefiniowane przez organizację i warstwy architektoniczne*];

(b) Zapewnia, że stosowane środki bezpieczeństwa działają w sposób skoordynowany i wzajemnie się uzupełniający.

Zabezpieczenia powiązane: SC-29, SC- 36.

(2) ARCHITEKTURA BEZPIECZEŃSTWA INFORMACJI | DYWERSYFIKACJA DOSTAWCY

Organizacja wymaga, aby *[Realizacja: środki bezpieczeństwa zdefiniowane przez organizację*] przydzielone do [*Realizacja: lokalizacje zdefiniowane przez organizację i warstwy architektoniczne*] nabywane były od różnych dostawców.

Zabezpieczenia powiązane: SA-12.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	PL-8 (opcjonalnie)	PL-8	PL-8

PL-9 ZARZĄDZANIE CENTRALNE

Zabezpieczenie: organizacja centralnie zarządza zabezpieczeniami[*Realizacja: zdefiniowane przez organizację środki bezpieczeństwa i powiązane procesy*].

Zabezpieczenia powiązane: AC-2 (1) (2) (3) (4); AC-17 (1) (2) (3) (9); AC-18 (1) (3) (4) (5); AC-19 (4); AC-22; AC-23; AT-2 (1) (2); AT-3 (1) (2) (3); AT-4; AU-6 (1) (3) (5) (6) (9); AU-7 (1) (2); AU-11, AU-13, AU-16, CA-2 (1) (2) (3); CA-3 (1) (2) (3); CA-7 (1); CA-9; CM-2 (1) (2); CM-3 (1) (4); CM-4; CM-6 (1); CM-7 (4) (5); CM-8 (wszystkie); CM-9 (1); CM-10; CM-11; CP-7 (wszystkie); CP-8 (wszystkie); SC-43; SI-2; SI-3; SI-7; i SI-8.

Zabezpieczenia rozszerzone: Brak.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P0	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	PL-9 (opcjonalnie)	PL-9 (opcjonalnie)	PL-9 (opcjonalnie)

KATEGORIA: PROGRAMY BEZPIECZEŃSTWA INFORMACJI

PM-1 PLAN PROGRAMU BEZPIECZEŃSTWA INFORMACJI

Zabezpieczenie: Organizacja:

c. Opracowuje, dokumentuje i rozpowszechnia plan programu bezpieczeństwa informacji organizacji, który:

   1. Zawiera przegląd wymagań dotyczących programu bezpieczeństwa oraz opis zarządzania tym programem, a także ogólnej koncepcji zabezpieczeń, które są stosowane lub planowane w celu spełnienia tych wymagań;

   2. Obejmuje identyfikację i przypisanie ról, obowiązków, zaangażowania kierownictwa, koordynację między jednostkami organizacyjnymi i ich spójność;

   3. Odzwierciedla koordynację między jednostkami organizacyjnymi odpowiedzialnymi za różne aspekty bezpieczeństwa informacji (tj. techniczne, fizyczne, osobowe, teleinformatyczne);

   4. Jest zatwierdzony przez kierownika jednostki organizacyjnej lub osobę przez niego upoważnioną;

d. Dokonuje przeglądów planu bezpieczeństwa informacji w całej organizacji z częstotliwością [*Realizacja: częstotliwość zdefiniowana przez organizację*];

e. Aktualizuje plan w celu uwzględnienia zmian organizacyjnych i problemów zidentyfikowanych podczas realizacji planu lub oceny środków bezpieczeństwa dokonanych w ramach przeglądu;

f. Chroni plan programu bezpieczeństwa informacji przed nieautoryzowanym ujawnieniem i modyfikacją.

Zabezpieczenia powiązane: PM-8.
Referencje: ISO 27001 [4, 5, Załącznik A (A.5, A.6)].
Zabezpieczenia rozszerzone: Brak.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	PM-1	PM-1	PM-1

PM-2 OSOBA ODPOWIEDZIALNA ZA BEZPIECZEŃSTWO INFORMACJI (CSO)

Zabezpieczenie: Organizacja wyznacza osobę odpowiedzialną za bezpieczeństwo informacji z misją i zadaniami w zakresie koordynowania, opracowywania, wdrażania i utrzymywania programu bezpieczeństwa informacji obejmującego całą organizację.

Zabezpieczenia powiązane: Brak.
Referencje: Brak.
Zabezpieczenia rozszerzone: Brak.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	PM-2	PM-2	PM-2

PM-3 ŚRODKI BEZPIECZEŃSTWA INFORMACJI

Zabezpieczenie: Organizacja:

a. Zapewnia środki i zasoby niezbędne do wdrożenia programu bezpieczeństwa informacji i dokumentuje wszystkie wyjątki od tego wymogu;
b. Wykorzystuje uzasadnienie biznesowe w celu określenia niezbędnych zasobów;
c. Zapewnia, że zasoby niezbędne do zapewnienia bezpieczeństwa informacji wykonują swoje zadania zgodnie z planem programu bezpieczeństwa informacji.

Zabezpieczenia powiązane: PM-4, SA-2.
Referencje: ISO 27001 [8.1].
Zabezpieczenia rozszerzone: Brak.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	PM-3	PM-3	PM-3

PM-4 PLAN DZIAŁANIA I ETAPY WPROWADZANIA ZABEZPIECZEŃ

Zabezpieczenie: Organizacja:

a. Wdraża proces zapewnienia, że plany działania i etapy wprowadzania programu bezpieczeństwa i powiązanych systemów teleinformatycznych:

1. Są opracowywane i utrzymywane;

2. Dokumentują działania zaradcze w zakresie bezpieczeństwa informacji, mające na celu odpowiednią reakcję na wystąpienie ryzyka związanego z operacjami organizacyjnymi i aktywami, osobami fizycznymi, innymi organizacjami i organami władzy państwowej.

3. Są zgłaszane zgodnie z wymogami sprawozdawczości.

b. Aktualizuje plany działania i etapy wprowadzania zabezpieczeń w celu zapewnienia spójności ze strategią zarządzania ryzykiem organizacyjnym i priorytetami całej organizacji w zakresie reagowania na ryzyko.

Zabezpieczenia powiązane: CA-5.
Referencje: ISO 27001 [8.1]
Zabezpieczenia rozszerzone: Brak.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	PM-4	PM-4	PM-4

PM-5 INWENTARYZACJA SYSTEMU INFORMACYJNEGO

Zabezpieczenie: Organizacja opracowuje i utrzymuje spis swoich aktywów.

Zabezpieczenia powiązane: Brak.
Referencje: ISO 27001 [8.1.1].
Zabezpieczenia rozszerzone: Brak.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	PM-5	PM-5	PM-5

PM-6 SKUTECZNOŚĆ ŚRODKÓW BEZPIECZEŃSTWA INFORMACJI

Zabezpieczenie: Organizacja opracowuje, monitoruje i raportuje wyniki pomiaru skuteczności (wydajności) zabezpieczeń.

Zabezpieczenia powiązane: Brak.
Referencje: ISO 27001 [9.1].
Zabezpieczenia rozszerzone: Brak.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	PM-6	PM-6	PM-6

PM-7 STRUKTURA ORGANIZACYJNA

Zabezpieczenie: Organizacja opracowuje strukturę organizacyjną z uwzględnieniem aspektów bezpieczeństwa informacji i odniesieniem do ryzyka operacji biznesowych, zasobów organizacyjnych, osób, innych organizacji i organów władzy państwowej.

Zabezpieczenia powiązane: PL-2, PL-8, PM-11, RA-2, SA-3.
Referencje: ISO 27001 [8.1].
Zabezpieczenia rozszerzone: Brak.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	PM-7	PM-7	PM-7

PM-8 PLAN INFRASTRUKTURY KRYTYCZNEJ

Zabezpieczenie: Organizacja opracowuje i aktualizuje plan ochrony infrastruktury krytycznej / plan ochrony zasobów kluczowych zawierający stosowne środki bezpieczeństwa informacji.

Zabezpieczenia powiązane: PM-1, PM-9, PM-11, RA-3.

Referencje: Ustawa z dnia 26 kwietnia 2007 roku o zarządzaniu kryzysowym (Dz.U. 2007 Nr 89 poz. 590) i Narodowy Program Ochrony Infrastruktury Krytycznej.

Zabezpieczenia rozszerzone: Brak.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	PM-8	PM-8	PM-8

PM-9 STRATEGIA ZARZĄDZANIA RYZYKIEM

Zabezpieczenie: Organizacja:

a. Opracowuje kompleksową strategię zarządzania ryzykiem dla operacji i zasobów organizacyjnych, osób fizycznych, innych organizacji oraz organów władzy państwowej związanych z obsługą i wykorzystaniem systemów informatycznych;
b. Konsekwentnie wdraża strategię zarządzania ryzykiem w całej organizacji;
c. Przegląda i aktualizuje strategię zarządzania ryzykiem z częstotliwością [*Realizacja: częstotliwość określona przez organizację*] lub zgodnie z wymaganiami przepisów prawa, uwzględniając zmiany organizacyjne.

Zabezpieczenia powiązane: RA-3.
Referencje: ISO 27001 [8.2].
Zabezpieczenia rozszerzone: Brak.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	PM-9	PM-9	PM-9

PM-10 PROCES AUTORYZACJI ZABEZPIECZEŃ

Zabezpieczenie: Organizacja:

a. Zarządza stanem zabezpieczeń systemów informatycznych organizacji oraz środowiskami, w których systemy te działają, poprzez procesy autoryzacji zabezpieczeń;
b. Wyznacza osoby do pełnienia określonych ról i obowiązków w ramach procesu zarządzania ryzykiem organizacyjnym;
c. W pełni integruje procesy autoryzacji zabezpieczeń z programem zarządzania ryzykiem w całej organizacji.

Zabezpieczenia powiązane: CA-6.
Referencje: ISO 27001 [6.1.3].
Zabezpieczenia rozszerzone: Brak.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	PM-10	PM-10	PM-10

PM-11 DEFINICJA MISJI / PROCESU BIZNESOWEGO

Zabezpieczenie: Organizacja:

a. Definiuje misje / procesy biznesowe z uwzględnieniem bezpieczeństwa informacji i wynikającego z tego ryzyka dla operacji biznesowych, zasobów organizacyjnych, osób fizycznych, innych organizacji i organów władzy państwowej;

b. Określa potrzeby w zakresie ochrony informacji wynikające z określonych misji / procesów biznesowych i w razie potrzeby koryguje procesy, aż do osiągnięcia akceptowalnego stanu w zakresie bezpieczeństwa.

Zabezpieczenia powiązane: PM-7, PM-8, RA-2.

Referencje: ISO 27001 [6.2].

Zabezpieczenia rozszerzone: Brak.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	PM-11	PM-11	PM-11

PM-12 ZAGROŻENIA WEWNĘTRZNE

Zabezpieczenie: Organizacja wdraża program dotyczący zagrożeń wewnętrznych, który obejmuje interdyscyplinarny zespół zajmujący się incydentami związanymi z zagrożeniami wewnętrznymi.

Zabezpieczenia powiązane: AC-6, AT-2, AU-6, AU-7, AU-10, AU-12, AU-13, CA-7, IA-4, IR-4, MP-7, PE-2, PS-3, PS-4, PS-5, PS-8, SC-7, SC-38, SI-4, PM-1, PM-14.

Referencje: Brak.

Zabezpieczenia rozszerzone: Brak.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	PM-12	PM-12	PM-12

PM-13 PERSONEL BEZPIECZEŃSTWA INFORMACJI

Zabezpieczenie: Organizacja ustanawia program rozwoju i doskonalenia personelu ds. bezpieczeństwa informacji.

Zabezpieczenia powiązane: AT-2, AT-3.
Referencje: Brak.
Zabezpieczenia rozszerzone: Brak.
Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	PM-13	PM-13	PM-13

PM-14 TESTOWANIE, SZKOLENIA I MONITOROWANIE

Zabezpieczenie: Organizacja:

a. Wdraża proces zapewniający, że plany organizacyjne dotyczące przeprowadzania testów bezpieczeństwa, szkoleń i monitorowania działań związanych z systemami informacyjnymi organizacji są:
   1. Opracowywane i utrzymywane;
   2. Wykonywane w odpowiednim czasie;

b. Przegląda plany testowania, szkolenia i monitorowania pod kątem zgodności ze strategią zarządzania ryzykiem organizacji i ogólnymi priorytetami organizacji w zakresie działań związanych z reagowaniem na ryzyko.

Zabezpieczenia powiązane: AT-3, CA-7, CP-4, IR-3, SI-4.
Referencje: Brak.
Zabezpieczenia rozszerzone: Brak.
Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	PM-14	PM-14	PM-14

PM-15 KONTAKTY Z GRUPAMI I STOWARZYSZENIAMI ZAJMUJĄCYMI SIĘ BEZPIECZEŃSTWEM INFORMACJI

Zabezpieczenie: Organizacja nawiązuje i instytucjonalizuje kontakt z wybranymi grupami i stowarzyszeniami w społeczności bezpieczeństwa w celu:

a. Ułatwienia ciągłej edukacji i szkolenia w zakresie bezpieczeństwa personelu organizacyjnego;
b. Utrzymywania bieżącej pomocy w zakresie zalecanych praktyk, technik i technologii bezpieczeństwa;
c. Udostępniania bieżących informacji związanych z bezpieczeństwem, w tym informacji o zagrożeniach, podatnościach i incydentach.

Zabezpieczenia powiązane: SI-5.
Referencje: Brak.
Zabezpieczenia rozszerzone: Brak.
Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P3	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	PM-15	PM-15	PM-15

PM-16 OSTRZEGANIE O ZAGROŻENIACH

Zabezpieczenie: Organizacja wdraża program zapewniający informowanie o zagrożeniach, który obejmuje wymianę informacji między organizacjami.

Zabezpieczenia powiązane: PM-12, PM-16.
Referencje: Brak.
Zabezpieczenia rozszerzone: Brak.
Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	PM-16	PM-16	PM-16

KATEGORIA: BEZPIECZEŃSTWO OSOBOWE

PS-1 BEZPIECZEŃSTWO OSOBOWE – POLITYKA I PROCEDURY

Zabezpieczenie: Organizacja:

a. Opracowuje, dokumentuje i rozpowszechnia w odniesieniu do *[Realizacja: personel lub role zdefiniowane przez organizację*]:

   1. Politykę bezpieczeństwa osobowego, która dotyczy celu, zakresu, ról, obowiązków, zaangażowania kierownictwa, koordynacji między jednostkami organizacyjnymi i spójności działania;

   2. Procedury ułatwiające wdrożenie polityki bezpieczeństwa osobowego i powiązanych środków bezpieczeństwa;

b. Przegląda i aktualizuje na bieżąco:

   1. Politykę bezpieczeństwa osobowego z częstotliwością [*Realizacja: częstotliwość określona przez organizację*];

   2. Procedury bezpieczeństwa osobowego z częstotliwością [*Realizacja: częstotliwość określona przez organizację*].

Zabezpieczenia powiązane: PM-9.

Zabezpieczenia rozszerzone: Brak.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	PS-1	PS-1	PS-1

PS-2 OKREŚLANIE RYZYKA DLA STANOWISKA PRACY

Zabezpieczenie: Organizacja:

a. Szacuje ryzyko utraty bezpieczeństwa informacji w odniesieniu do wszystkich stanowisk do w organizacji;

b. Ustanawia kryteria selekcji osób zajmujących te stanowiska;

c. Przegląda i aktualizuje oszacowane ryzyko danego stanowiska z częstotliwością [*Realizacja: częstotliwość określona przez organizację*].

Zabezpieczenia powiązane: AT-3, PL-2, PS-3.

Zabezpieczenia rozszerzone: Brak.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	PS-2	PS-2	PS-2

PS-3 DOBÓR PERSONELU

Zabezpieczenie: Organizacja:

a. Sprawdza osoby przed udzieleniem autoryzacji dostępu do systemu teleinformatycznego;

b. Ponownie sprawdza osoby zgodnie z warunkami [*Realizacja: warunki zdefiniowane przez organizację wymagające ponownego przeglądu, a tam gdzie jest to wskazane, częstotliwość takiego przeglądu*].

Zabezpieczenia powiązane: AC-2, LA-4, PE-2, PS-2.

Zabezpieczenia rozszerzone:

(1) DOBÓR PERSONELU | INFORMACJE NIEJAWNE

Organizacja zapewnia, ażeby osoby uzyskujące dostęp do systemu teleinformatycznego przetwarzającego, przechowującego lub przesyłającego informacje niejawne posiadały poświadczenia bezpieczeństwa do najwyższego poziomu klasyfikacji informacji, do których mają dostęp w systemie.

Zabezpieczenia powiązane: AC-3, AC-4.

(2) DOBÓR PERSONELU | POSTĘPOWANIA SPRAWDZAJĄCE

Organizacja zapewnia, ażeby osoby uzyskujące dostęp do systemu teleinformatycznego przetwarzającego, przechowującego lub przekazującego informacje niejawne, podlegały, zgodnie z ustawą o ochronie informacji niejawnych, stosownemu postępowaniu sprawdzającemu.

Zabezpieczenia powiązane: AC-3, AC-4.

(3) DOBÓR PERSONELU | INFORMACJE WYMAGAJĄCE SZCZEGÓLNEJ OCHRONY

Organizacja zapewnia, aby osoby uzyskujące dostęp do systemu teleinformatycznego przetwarzającego, przechowującego lub przekazującego informacje wymagające specjalnej ochrony:

(a) Posiadały ważne poświadczenia bezpieczeństwa zezwalające na dostęp do informacji;

(b) Spełniały dodatkowe kryteria [*Realizacja: zdefiniowane przez organizację dodatkowe kryteria selekcji personelu*].

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	PS-3	PS-3	PS-3

PS-4 ZAKOŃCZENIE ZATRUDNIENIA

Zabezpieczenie: Po zakończeniu zatrudnienia organizacja:

a. Wyłącza dostęp do systemu teleinformatycznego w ciągu [*Realizacja: okres zdefiniowany przez organizację*];

b. Kończy / odwołuje wszelkie pełnomocnictwa / poświadczenia powiązane z osobą;

c. Prowadzi rozmowy końcowe, które obejmują omówienie tematów bezpieczeństwa [*Realizacja: tematy bezpieczeństwa informacji zdefiniowane przez organizację*];

d. Odbiera wszystkie aktywa związane z bezpieczeństwem systemu teleinformatycznego wykorzystywane, przydzielone oraz wytworzone przez pracownika na danym stanowisku;

e. Zachowuje dostęp do informacji organizacyjnych i systemów teleinformatycznych nadzorowanych (użytkowanych) przez zwalnianą osobę;

f. Powiadamia [*Realizacja: personel lub role zdefiniowane przez organizację*] w ciągu [*Realizacja: okres zdefiniowany przez organizację*] o rozwiązaniu umowy świadczenia stosunku pracy (innej umowy cywilnoprawnej) ze zwalnianą osobą.

Zabezpieczenia powiązane: AC-2, IA-4, PE-2, PS-5, PS-6.

Zabezpieczenia rozszerzone:

(1) ZAKOŃCZENIE ZATRUDNIENIA | ZOBOWIĄZANIA PO ZAKOŃCZENIU ZATRUDNIENIU

Organizacja**:**

(a) Powiadamia zwalniane osoby o obowiązujących w zakresie ochrony informacji organizacyjnych prawnie wiążących wymaganiach po okresie zatrudnienia;

(b) Wymaga podpisania przez zwalniane osoby oświadczenie w zakresie zachowania tajemnicy organizacji po okresie zatrudnienia.

Organizacje konsultują się z biurem radcy prawnego w sprawach dotyczących wymagań po okresie zatrudnienia.

(2) ZAKOŃCZENIE ZATRUDNIENIA | AUTOMATYCZNE POWIADAMIANIE

Organizacja stosuje zautomatyzowane mechanizmy powiadamiania [*Realizacja: personel lub role zdefiniowane przez organizację*] o zwolnieniu danej osoby.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	PS-4	PS-4	PS-4 (2)

PS-5 OBSADZENIE LUB PRZENIESIENIE STANOWISKA

Zabezpieczenie: Organizacja:

a. Dokonuje przeglądu i potwierdza bieżącą potrzebę operacyjną logicznych i fizycznych zezwoleń na dostęp do systemów / urządzeń teleinformatycznych, gdy osoby zostaną ponownie obsadzone / przeniesione na inne stanowiska w organizacji;

b. Inicjuje [*Realizacja: zdefiniowane przez organizację działania przeniesienia lub ponownego obsadzenia stanowiska*] w ciągu [*Realizacja: zdefiniowane przez organizację okres po formalnym przeniesieniu / ponownym obsadzeniu*];

c. W razie potrzeby modyfikuje autoryzację dostępu, aby odpowiadała wszelkim zmianom potrzeb operacyjnych spowodowanych zmianą stanowiska lub przeniesienia;

d. Powiadamia [*Realizacja: personel lub role zdefiniowane przez organizację*] w ciągu [*Realizacja: okres zdefiniowany przez organizację*].

Zabezpieczenia powiązane: AC-2, IA-4, PE-2, PS-4.

Zabezpieczenia rozszerzone: Brak.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P2	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	PS-5	PS-5	PS-5

PS-6 UMOWY DOSTĘPU / WSPÓŁPRACY

Zabezpieczenie: Organizacja:

a. Opracowuje i dokumentuje umowy dostępu / współpracy do systemów teleinformatycznych organizacji;

b. Przegląda i aktualizuje umowy o dostępie / współpracy z częstotliwością [*Realizacja: częstotliwość określona przez organizację*];

c. Zapewnia, aby osoby wymagające dostępu do informacji organizacyjnych i systemów teleinformatycznych:

   1. Podpisały odpowiednie umowy o dostęp / współpracę przed udzieleniem im dostępu;

   2. Ponownie podpisywały umowy o dostępie / współpracy, celem zachowania dostępu do systemów teleinformatycznych organizacji, gdy umowy o dostęp zostały zaktualizowane lub z częstotliwością [*Realizacja: częstotliwość określona przez organizację*].

Zabezpieczenia powiązane: PL-4, PS-2, PS-3, PS-4, PS-8.

Zabezpieczenia rozszerzone:

(1) UMOWY DOSTĘPU / WSPÓŁPRACY| INFORMACJE WYMAGAJĄCE SPECJALNEJ OCHRONY

[Włączone do PS-3].

(2) UMOWY DOSTĘPU / WSPÓŁPRACY | INFORMACJE NIEJAWNE WYMAGAJĄCE OCHRONY SPECJALNEJ

Organizacja zapewnia, że dostęp do informacji niejawnych wymagających szczególnej ochrony mają tylko osoby, które:

(a) Posiadają ważne poświadczenia bezpieczeństwa, wydane przez krajową władzę bezpieczeństwa;

(b) Spełniają kryteria bezpieczeństwa osobowego;

(c) Przeczytały, zrozumiały i podpisały umowę o zachowaniu poufności.

(3) UMOWY DOSTĘPU / WSPÓŁPRACY | WYMOGI PO ZAKOŃCZENIU ZATRUDNIENIA

Organizacja:

(a) Powiadamia osoby o obowiązujących po okresie zatrudnienia, prawnie wiążących wymaganiach zachowania tajemnicy informacji organizacyjnych;

(b) Wymaga od osób podpisania oświadczeniu o zachowaniu tajemnicy informacji organizacyjnych.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P3	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	PS-6	PS-6	PS-6

PS-7 BEZPIECZEŃSTWO OSOBOWE STRON TRZECICH

Zabezpieczenie: Organizacja:

a. Ustanawia wymagania dotyczące bezpieczeństwa osobowego, w tym role bezpieczeństwa i obowiązki dostawców zewnętrznych;

b. Wymaga od zewnętrznych dostawców przestrzegania zasad i procedur bezpieczeństwa osobowego ustanowionych przez organizację;

c. Dokumentuje wymagania bezpieczeństwa osobowego;

d. Wymaga od zewnętrznych dostawców powiadamiania [*Realizacja: personel lub role zdefiniowane przez organizację*] o każdym przeniesieniu lub zakończeniu pracy personelu zewnętrznego, który posiada poświadczenia i / lub identyfikatory organizacyjne lub posiada uprawnienia systemowe nie później niż do [*Realizacja: okres zdefiniowany przez organizację*];

e. Monitoruje stosowanie przez dostawcę zasad i procedur bezpieczeństwa.

Zabezpieczenia powiązane: PS-2, PS-3, PS-4, PS-5, PS-6, SA-9, SA-21.

Zabezpieczenia rozszerzone: Brak.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	PS-7	PS-7	PS-7

PS-8 SANKCJE PERSONALNE

Zabezpieczenie: Organizacja:

a. Stosuje formalny proces sankcji[44] wobec osób, które nie przestrzegają ustalonych zasad i procedur bezpieczeństwa informacji;

b. Powiadamia [*Realizacja: personel lub role zdefiniowane przez organizację*] w ciągu [*Realizacja: okres zdefiniowany przez organizację*] o rozpoczęciu formalnego procesu nakładania sankcji na pracownika, określając osobę objętą sankcją i powód nałożenia sankcji.

Zabezpieczenia powiązane: PL-4, PS-6.

Zabezpieczenia rozszerzone: Brak.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P3	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	PS-8	PS-8	PS-8

[44] Procesy sankcji organizacyjnych odzwierciedlają obowiązujące przepisy prawne.

KATEGORIA: OCENA RYZYKA

RA-1 POLITYKA I PROCEDURY SZACOWANIA RYZYKA

Zabezpieczenie: Organizacja:

a. Opracowuje, dokumentuje i rozpowszechnia w odniesieniu do [*Realizacja: personel lub role zdefiniowane przez organizację*]:

   1. Politykę oceny ryzyka uwzględniającą cel, zakres, role, obowiązki, zaangażowanie kierownictwa, koordynację między jednostkami organizacyjnymi i spójności działania;

   2. Procedury ułatwiające wdrażanie polityki oceny ryzyka i powiązane kontrole oceny ryzyka;

b. Przegląda i aktualizuje bieżącą:

   1. Politykę oceny ryzyka z częstotliwością [*Realizacja: częstotliwość określona przez organizację*];

   2. Procedury oceny ryzyka z częstotliwością [*Realizacja: częstotliwość określona przez organizację*].

Zabezpieczenia powiązane: PM-9.

Zabezpieczenia rozszerzone: Brak.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	RA-1	RA-1	RA-1

RA-2 KATEGORYZACJA BEZPIECZEŃSTWA

Zabezpieczenie: Organizacja:

a. Klasyfikuje informacje i system teleinformatyczny zgodnie z obowiązującymi przepisami, zarządzeniami wykonawczymi, dyrektywami, politykami, przepisami, standardami i wytycznymi;

b. Dokumentuje wyniki kategoryzacji bezpieczeństwa (w tym uzasadnienie) w planie bezpieczeństwa systemu teleinformatycznego;

c. Zapewnia, że osoba upoważniona przez kierownika jednostki organizacyjnej dokonuje przeglądu i zatwierdza decyzję w sprawie kategoryzacji bezpieczeństwa.

Zabezpieczenia powiązane: CM-8, MP-4, RA-3, SC-7.

Zabezpieczenia rozszerzone: Brak.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	RA-2	RA-2	RA-2

RA-3 SZACOWANIE RYZYKA

Zabezpieczenie: Organizacja:

a. Przeprowadza ocenę ryzyka, w tym prawdopodobieństwa wystąpienia i wielkość szkody, wynikającej z nieuprawnionego dostępu, użytkowania, ujawnienia, zakłócenia, modyfikacji lub zniszczenia systemu teleinformatycznego oraz informacji, które ta organizacja przetwarza, przechowuje lub przesyła;

b. Dokumentuje ocenę ryzyka w [*Wybór: plan bezpieczeństwa; raport z oceny ryzyka; [Realizacja: dokument zdefiniowany przez organizację*]];

c. Przegląda wyniki oceny ryzyka z częstotliwością [*Realizacja: częstotliwość określona przez organizację*];

d. Rozpowszechnia wyniki oceny ryzyka w odniesieniu [*Realizacja: personel lub role zdefiniowane przez organizację*];

e. Aktualizuje ocenę ryzyka z częstotliwością [*Realizacja: częstotliwość zdefiniowana przez organizację*] lub za każdym razem, gdy nastąpią znaczące zmiany w systemie teleinformatycznym lub środowisku działania (w tym zidentyfikowania nowych zagrożeń i podatności) lub inne warunki, które mogą mieć wpływ na stan bezpieczeństwa systemu.

Zabezpieczenia powiązane: RA-2, PM-9.

Zabezpieczenia rozszerzone: Brak.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	RA-3	RA-3	RA-3

RA-4 AKTUALIZACJA SZACOWANIA RYZYKA

[Włączony do RA-3].

RA-5 SKANOWANIE PODATNOŚCI

Zabezpieczenie: Organizacja:

a. Skanuje system teleinformatyczny w poszukiwaniu luk w tym systemie i aplikacjach hostowanych z częstotliwością [*Realizacja: częstotliwość zdefiniowana przez organizację i / lub losowo zgodnie z procesem zdefiniowanym przez organizację*] oraz w przypadku identyfikacji i zgłoszenia nowych podatności mogących mieć potencjalny wpływ na pracę systemu;

b. Wykorzystuje narzędzia i techniki skanowania, które ułatwiają interoperacyjność między narzędziami i automatyzują części procesu zarządzania podatnością, wykorzystując standardy dla:

   1. Wyliczania platform, wad oprogramowania i niewłaściwych konfiguracji;
   2. Formatowania list kontrolnych i procedur testowych;
   3. Pomiaru wpływu podatności na zagrożenia;

c. Analizuje raporty skanowania narażenia na atak i wyniki oceny środków bezpieczeństwa;

d. Usuwa uzasadnione luki w zabezpieczeniach w czasie [*Realizacja: czasy reakcji określone przez organizację*] od wykrycia, zgodnie z oceną ryzyka przeprowadzoną przez organizację;

e. Udostępnia informacje uzyskane z procesu skanowania w poszukiwaniu luk i oceny środków bezpieczeństwa personelowi [*Realizacja: personel lub role zdefiniowane przez organizację*], aby pomóc wyeliminować podobne podatności w innych systemach teleinformatycznych (tj. słabości lub braki systemowe).

Zabezpieczenia powiązane: CA-2, CA-7, CM-4, CM-6, RA-2, RA-3, SA-11, SI-2.

Zabezpieczenia rozszerzone:

(1) SKANOWANIE PODATNOŚCI | AKTUALIZACJA NARZĘDZI

Organizacja stosuje narzędzia do skanowania podatności, które umożliwiają ich aktualizacje o zdiagnozowane nowe podatności systemu teleinformatycznego.

Zabezpieczenia powiązane: SI-3, SI-7.

(2) SKANOWANIE PODATNOŚCI | AKTUALIZACJA CZĘSTOTLIWOŚCI PRZEPROWADZANIA / AKTUALIZACJA PRZED NOWYM SKANOWANIEM / AKTUALIZACJA PO ZIDENTYFIKOWANIU ZAGROŻENIA

Organizacja aktualizuje narzędzia do skanowania podatności w systemie teleinformatycznym [*Wybór (jeden lub więcej*; *przed nowym skanowaniem; po zidentyfikowaniu / zgłoszeniu nowych luk*] z częstotliwością *[Realizacja: częstotliwość określona przez organizację*]

Zabezpieczenia powiązane: SI-3, SI-5.

(3) SKANOWANIE PODATNOŚCI | ZAKRES PODATNOŚCI

Organizacja stosuje procedury skanowania w poszukiwaniu luk w zabezpieczeniach, które mogą określić zakres występowania podatności (tj. skanowane są komponenty systemu teleinformatycznego i sprawdzane ich podatności).

(4) SKANOWANIE WRAŻLIWOŚCI | WYKRYWANIE SKANOWANIA

Organizacja określa, jakie informacje o systemie teleinformatycznym są wykrywalne przez przeciwników, a następnie podejmuje [*Realizacja: działania naprawcze zdefiniowane przez organizację*].

Zabezpieczenia powiązane: AU-13.

(5) SKANOWANIE PODATNOŚCI | DOSTĘP UPRZYWILEJOWANY

System teleinformatyczny wprowadza autoryzację dostępu uprzywilejowanego do [*Realizacja: komponenty systemu teleinformatycznego zidentyfikowane przez organizację*] dla wybranych działań [*Realizacja: działania skanowania narażenia zdefiniowane przez organizację*].

(6) SKANOWANIE PODATNOŚCI | AUTOMATYCZNE ANALIZY TRENDÓW

W celu określenia trendów w podatnościach systemów teleinformatycznych organizacja stosuje zautomatyzowane mechanizmy do porównywania wyników skanów podatności w czasie.

Zabezpieczenia powiązane: IR-4, IR-5, SI-4.

(7) SKANOWANIE PODATNOŚCI | AUTOMATYCZNE WYKRYWANIE I POWIADAMIANIE O NIEAUTORYZOWANYCH KOMPONENTACH

[Włączono do CM-8].

(8) SKANOWANIE PODATNOŚCI | PRZEGLĄD HISTORYCZNYCH LOGÓW AUDYTU

Organizacja dokonuje przeglądu historycznych dzienników logów w celu ustalenia, czy luka zidentyfikowana w systemie teleinformatycznym nie została wcześniej wykorzystana.

Zabezpieczenia powiązane: AU-6.

(9) SKANOWANIE PODATNOŚCI | TESTY PENETRACYJNE I ANALIZY

[Włączono do CA-8].

(10) SKANOWANIE PODATNOŚCI | KORELACJA SKANOWANYCH DANYCH

Organizacja koreluje dane wyjściowe z narzędzi do skanowania w poszukiwaniu luk w celu ustalenia obecności wektorów ataku z wieloma podatnościami / wektorami ataku.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	RA-5	RA-5 (1) (2) (5)	RA-5 (1) (2) (4) (5)

RA-6 TECHNICZNE ZABEZPIECZENIE PRZED PODGLĄDEM I PODSŁUCHEM

Zabezpieczenie: Organizacja stosuje techniczne zabezpieczenia przed podglądem i podsłuchem w firmie [*Realizacja: lokalizacje zdefiniowane przez organizację*] [*Wybór (jeden lub więcej): [Realizacja: częstotliwość zdefiniowana przez organizację]; [Realizacja: występują zdarzenia lub wskaźniki zdefiniowane przez organizację*[45]*]*].

Zabezpieczenia rozszerzone: Brak.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P0	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	RA-6 (opcjonalnie)	RA-6 (opcjonalnie)	RA-6 (opcjonalnie)

[45] Wykrywanie obecności urządzeń / zagrożeń podglądu i podsłuchu oraz identyfikowanie technicznych niedociągnięć w zakresie bezpieczeństwa, które mogłyby ułatwić przeprowadzanie penetracji technicznych zdefiniowanych przez organizację obiektów / lokalizacji. Zabezpieczenie to zazwyczaj obejmuje dokładne badania wizualne, elektroniczne i fizyczne badanych obiektów / lokalizacji.

KATEGORIA: NABYWANIE SYSTEMU I USŁUG

SA-1 POLITYKA I PROCEDURY NABYWANIA SYSTEMU I USŁUG

Zabezpieczenie: Organizacja:

a. Opracowuje, dokumentuje i rozpowszechnia w odniesieniu do [*Realizacja: personel lub role zdefiniowane przez organizację*]:

   1. Politykę pozyskiwania systemów i usług, która dotyczy celu, zakresu, ról, obowiązków, zaangażowania kierownictwa, koordynacji między jednostkami organizacyjnymi i spójności działania;

   2. Procedury ułatwiające wdrażanie polityki nabywania systemu i usług oraz powiązane kontrole nabywania systemu i usług;

b. Przegląda i aktualizuje bieżącą:

   1. Politykę nabywania systemów i usług z częstotliwością [*Realizacja: częstotliwość określona przez organizację*];

   2. Procedury pozyskiwania systemów i usług z częstotliwością [*Realizacja: częstotliwość określona przez organizację*].

Zabezpieczenia powiązane: PM-9.

Zabezpieczenia rozszerzone: Brak.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	SA-1	SA-1	SA-1

SA-2 PRZYDZIAŁ ZASOBÓW

Zabezpieczenie: Organizacja:

a. Określa wymagania bezpieczeństwa informacji w systemie teleinformatycznym lub usługi systemu teleinformatycznego w planowaniu misji / procesów biznesowych;

b. Określa, dokumentuje i przydziela zasoby wymagane do ochrony systemu teleinformatycznego lub usługi systemu teleinformatycznego w ramach procesu planowania i kontroli inwestycji;

c. Ustanawia oddzielne pozycje zamówień dotyczące bezpieczeństwa informacji w dokumentacji programowej i budżetowej organizacji.

Zabezpieczenia powiązane: PM-3, PM-11.

Zabezpieczenia rozszerzone: Brak.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	SA-2	SA-2	SA-2

SA-3 CYKL ŻYCIA SYSTEMU

Zabezpieczenie: Organizacja:

a. Zarządza systemem teleinformatycznym przy użyciu [*Realizacja: cykl rozwoju systemu zdefiniowany przez organizację*], który uwzględnia aspekty bezpieczeństwa informacji;

b. Definiuje i dokumentuje role i obowiązki w zakresie bezpieczeństwa informacji w całym cyklu życia systemu;

c. Identyfikuje osoby pełniące role i obowiązki związane z bezpieczeństwem informacji;

d. Integruje proces zarządzania ryzykiem związanym z bezpieczeństwem informacji w organizacji z cyklem życia systemu.

Zabezpieczenia powiązane: AT-3, PM-7, SA-8.

Zabezpieczenia rozszerzone: Brak.

Zabezpieczenia powiązane: Brak

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	SA-3	SA-3	SA-3

SA-4 PROCES NABYCIA

Zabezpieczenie: Organizacja zawiera następujące wymagania, opisy i kryteria, wprost lub przez odniesienie, w umowie nabycia systemu teleinformatycznego, komponentu systemu lub usługi systemu teleinformatycznego zgodnie z obowiązującymi przepisami prawnymi, zarządzeniami wykonawczymi, dyrektywami, politykami, przepisami , standardami, oraz wytycznymi:

a. Wymagania funkcjonalne w zakresie bezpieczeństwa;

b. Wymagania dotyczące poziomów bezpieczeństwa;

c. Wymogi zapewnienia bezpieczeństwa;

d. Wymagania dotyczące dokumentacji związanej z bezpieczeństwem;

e. Wymagania dotyczące ochrony dokumentacji związanej z bezpieczeństwem;

f. Opis środowiska programistycznego i środowiska funkcjonowania systemu;

g. Kryteria komisyjnego odbioru.

Zabezpieczenia powiązane: CM-6, PL-2, PS-7, SA-3, SA-5, SA-8, SA-11, SA-12.

Zabezpieczenia rozszerzone:

(1) PROCES NABYCIA | WŁAŚCIWOŚCI FUNKCJONALNE ZABEZPIECZEŃ

Organizacja wymaga od twórcy systemu teleinformatycznego, komponentu systemu lub usługi systemu teleinformatycznego przedstawienia opisu funkcjonalnych właściwości stosowanych zabezpieczeń.

Zabezpieczenia powiązane: SA-5.

(2) PROCES NABYCIA | PROJEKTOWANIE / IMPLEMENTACJA ZABEZPIECZEŃ

Organizacja wymaga od twórcy systemu teleinformatycznego, komponentu systemu lub usługi systemu teleinformatycznego dostarczenia informacji projektowych i wdrożeniowych dotyczących stosowanych zabezpieczeń, które obejmują: [*Wybór (jeden lub więcej): interfejsy systemu zewnętrznego istotne z punktu widzenia bezpieczeństwa; projekt wysokopoziomowy; konstrukcja niskopoziomowa; kod źródłowy lub schematy sprzętowe; [Realizacja: informacje dotyczące projektu / wdrożenia zdefiniowane przez organizację*]] na poziomie [*Realizacja: poziom szczegółowości zdefiniowany przez organizację*].

Zabezpieczenia powiązane: SA-5.

(3) PROCES NABYCIA | METODY ROZWOJU / TECHNIKI / PRAKTYKI

Organizacja wymaga od twórcy systemu teleinformatycznego, komponentu systemu lub usługi systemu teleinformatycznego wykazania cyklu życia systemu, który obejmuje [*Realizacja: system zdefiniowany przez organizację / metody inżynierii bezpieczeństwa, metody opracowywania oprogramowania , techniki testowania / oceny / certyfikacji oraz procesy kontroli jakości*].

Zabezpieczenia powiązane: SA-12.

(4) PROCES NABYCIA | PRZYPISANIE KOMPONENTÓW DO SYSTEMÓW

[Włączono do CM-8 (9)].

(5) PROCES NABYCIA | KONFIGURACJA SYSTEMU / KOMPONENTÓW / USŁUG

Organizacja wymaga od twórcy systemu teleinformatycznego, komponentu systemu lub usługi systemu teleinformatycznego:

(a) Dostarczenia systemu, komponentu lub usługi z zaimplementowanymi [*Realizacja: konfiguracje bezpieczeństwa zdefiniowane przez organizację*];

(b) Zastosowania konfiguracji domyślnej dla każdej kolejnej ponownej instalacji lub aktualizacji systemu, komponentu lub usługi.

Zabezpieczenia powiązane: CM-8.

(6) PROCES NABYCIA | UŻYWANIE PRODUKTÓW ZAPEWNIAJĄCYCH BEZPIECZEŃSTWO INFORMACJI

Organizacja zapewnia, że produkty bezpieczeństwa informacji zostały ocenione i / lub zatwierdzone przez krajową władzę bezpieczeństwa zgodnie z obowiązującymi przepisami.

Zabezpieczenia powiązane: SC-8, SC-12, SC-13.

(7) PROCES NABYCIA | ZATWIERDZONE PROFILE OCHRONY

Organizacja:

(a) Korzysta z komercyjnych produktów technologii teleinformatycznych, które zostały pomyślnie ocenione przez krajową władzę bezpieczeństwa zgodnie z obowiązującymi przepisami.

(b) Wymaga, aby moduł kryptograficzny stosowany w systemie teleinformatycznym został zatwierdzony przez krajową władzę bezpieczeństwa zgodnie z obowiązującymi przepisami.

Zabezpieczenia powiązane: SC-12, SC-13.

(8) PROCES NABYCIA | PLAN CIĄGŁOŚCI MONITOROWANIA

Organizacja wymaga od twórcy systemu teleinformatycznego, komponentu systemu lub usługi systemu teleinformatycznego opracowania planu ciągłego monitorowania skuteczności zastosowanych środków bezpieczeństwa, który zawiera [*Realizacja: poziom szczegółowości zdefiniowany przez organizację*].

Zabezpieczenia powiązane: CA-7.

(9) PROCES NABYCIA | FUNKCJE / PORTY / PROTOKOŁY / USŁUGI

Organizacja wymaga od twórcy systemu teleinformatycznego, komponentu lub usługi systemu teleinformatycznego identyfikacji początkowym etapie cyklu życia systemu funkcji, portów, protokołów i usług przeznaczonych do użycia przez organizację.

Zabezpieczenia powiązane: CM-7, SA-9.

(10) PROCES NABYCIA | WYKORZYSTANIE ZATWIERDZONYCH PRODUKTÓW

Organizacja stosuje wyłącznie produkty teleinformatyczne z listy produktów zatwierdzonych przez [*Realizacja: zgodnie z wewnętrznymi regulacjami organizacji lub wymaganiami ustalonymi przepisem prawa*] do celów weryfikacji tożsamości osobistej zaimplementowanych w organizacyjnych systemach teleinformatycznych.

Zabezpieczenia powiązane: IA-2, IA-8.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	SA-4 (10)	SA-4 (1) (2) (9) (10)	SA-4 (1) (2) (9) (10)

SA-5 DOKUMENTACJA SYSTEMU TELEINFORMATYCZNEGO

Zabezpieczenie: Organizacja:

a. Tworzy dokumentację administratora systemu teleinformatycznego, komponentu systemu lub usługi systemu teleinformatycznego, która opisuje:
   1. Bezpieczną konfigurację, instalację i działanie systemu, komponentu lub usługi;
   2. Efektywne wykorzystanie i utrzymanie funkcji / mechanizmów bezpieczeństwa;
   3. Znane luki w zabezpieczeniach dotyczące konfiguracji i korzystania z funkcji administracyjnych (tj. uprzywilejowanych);
b. Uzyskuje dokumentację użytkownika systemu teleinformatycznego, komponentu systemu lub usługi systemu teleinformatycznego, która opisuje:
   1. Funkcje / mechanizmy bezpieczeństwa dostępne dla użytkownika i sposoby skutecznego korzystania z tych funkcji / mechanizmów bezpieczeństwa;
   2. Metody interakcji użytkownika, które umożliwiają użytkownikom korzystanie z systemu, komponentu lub usługi w bezpieczny sposób;
   3. Odpowiedzialność użytkownika za utrzymanie bezpieczeństwa systemu, komponentu lub usługi;
c. Dokumentuje próby uzyskania dostępu do systemu teleinformatycznego, komponentu systemu lub usługi systemu teleinformatycznego, a gdy taka dokumentacja jest niedostępna lub nie istnieje, podejmuje [*Realizacja: działania zdefiniowane przez organizację*];
d. Chroni dokumentację zgodnie ze strategią zarządzania ryzykiem;
e. Dystrybuuje dokumentację do [*Realizacja: personel lub role zdefiniowane przez organizację*].

Zabezpieczenia powiązane: CM-6, CM-8, PL-2, PL-4, PS-2, SA-3, SA-4.

Zabezpieczenia rozszerzone:

(1) DOKUMENTACJA SYSTEMU INFORMATYCZNEGO | FUNKCJONALNE WŁAŚCIWOŚCI ŚRODKÓW BEZPIECZEŃSTWA

[Włączone do SA-4 (1)].

(2) DOKUMENTACJA SYSTEMU INFORMATYCZNEGO | BEZPIECZEŃSTWO INTERFEJSÓW SYSTEMU ZEWNĘTRZNEGO

[Włączone do SA-4 (2)].

(3) DOKUMENTACJA SYSTEMU INFORMATYCZNEGO | PROJEKTOWANIE WYSOKOPOZIOMOWE

[Włączone do SA-4 (2)].

(4) DOKUMENTACJA SYSTEMU INFORMATYCZNEGO | PROJEKTOWANIE NISKOPOZIOMOWE

[Włączony do SA-4 (2)].

(5) DOKUMENTACJA SYSTEMU INFORMATYCZNEGO | KOD ŹRÓDŁOWY

[Włączone do SA-4 (2)].

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P2	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	SA-5	SA-5	SA-5

SA-6 OGRANICZENIA W UŻYCIU OPROGRAMOWANIA

[Włączony do CM-10 i SI-7].

SA-7 OPROGRAMOWANIE INSTALOWANE PRZEZ UŻYTKOWNIKA

[Włączony do CM-11 i SI-7].

SA-8 ZARZĄDZANIE BEZPIECZEŃSTWEM INFORMACJI

Zabezpieczenie: Organizacja określa zasady zarządzania bezpieczeństwem informacji w specyfikacji, projekcie, oraz podczas rozwoju, wdrażaniu i modyfikacji systemu teleinformatycznego.

Zabezpieczenia powiązane: PM-7, SA-3, SA-4, SA-17, SC-2, SC-3.

Zabezpieczenia rozszerzone: Brak.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	SA-8 (opcjonalnie)	SA-8	SA-8

SA-9 USŁUGI ZEWNĘTRZNEGO SYSTEMU INFORMATYCZNEGO

Zabezpieczenie: Organizacja:

a. Wymaga, aby dostawcy usług zewnętrznego systemu teleinformatycznego przestrzegali wymagań bezpieczeństwa informacji organizacyjnych i stosowali [*Realizacja: środki bezpieczeństwa określone przez organizację*] zgodnie z obowiązującymi przepisami, zarządzeniami wykonawczymi, dyrektywami, politykami, przepisami, standardami i wytycznymi;

b. Definiuje i dokumentuje nadzór oraz role i obowiązki użytkowników w odniesieniu do usług zewnętrznego systemu teleinformatycznego;

c. Wykorzystuje [*Realizacja: procesy, metody i techniki zdefiniowane przez organizację*] do bieżącego monitorowania zgodności środków bezpieczeństwa stosowanych przez zewnętrznych dostawców usług.

Zabezpieczenia powiązane: CA-3, IR-7, PS-7.

Zabezpieczenia rozszerzone:

(1) USŁUGI ZEWNĘTRZNEGO SYSTEMU INFORMATYCZNEGO | OCENA RYZYKA / ZATWIERDZENIA ORGANIZACYJNE

Organizacja:

(a) przeprowadza ocenę ryzyka organizacyjnego przed nabyciem lub zleceniem wykonania dedykowanych usług bezpieczeństwa informacji;

(b) Zapewnia, że nabycie lub zlecenie wykonania dedykowanych usług bezpieczeństwa informacji jest zatwierdzone przez [*Realizacja: personel lub role zdefiniowane przez organizację*].

Zabezpieczenia powiązane: CA-6, RA-3.

(2) USŁUGI ZEWNĘTRZNEGO SYSTEMU INFORMATYCZNEGO | IDENTYFIKACJA FUNKCJI / PORTÓW / PROTOKOŁÓW / USŁUG

Organizacja wymaga od dostawców zapewnienia *[Przypisania: zdefiniowane przez organizację usługi zewnętrznego systemu teleinformatycznego*] do zidentyfikowania funkcji, portów, protokołów i innych usług wymaganych do korzystania z takich usług.

Zabezpieczenia powiązane: CM-7.

(3) USŁUGI ZEWNĘTRZNEGO SYSTEMU INFORMATYCZNEGO | TWORZENIE / UTRZYMANIE RELACJI ZAUFANIA Z DOSTAWCAMI

Organizacja ustanawia, dokumentuje i utrzymuje relacje zaufania z zewnętrznymi dostawcami usług w oparciu o [*Realizacja: zdefiniowane przez organizację wymagania bezpieczeństwa, właściwości, czynniki lub warunki określające dopuszczalne relacje zaufania*].

(4) USŁUGI ZEWNĘTRZNEGO SYSTEMU INFORMATYCZNEGO | ZGODNOŚĆ INTERESÓW KONSUMENTÓW I DOSTAWCÓW

Organizacja stosuje [*Realizacja: środki bezpieczeństwa zdefiniowane przez organizację*], w celu zapewnienia zgodności oraz odzwierciedlenia interesów [*Realizacja: zewnętrzni dostawcy usług zdefiniowani przez organizację*] z interesami organizacyjnymi.

(5) USŁUGI ZEWNĘTRZNEGO SYSTEMU INFORMATYCZNEGO | OBSZAR PROCESOWANIA, PRZECHOWYWANIA, I OBSŁUGI TECHNICZNEJ

Organizacja ogranicza (zawężą) lokalizację [*Wybór (jeden lub więcej): przetwarzanie informacji; informacje / dane; usługi systemu teleinformatycznego*] do obszaru [*Realizacja: lokalizacje (obszary) zdefiniowane przez organizację*] na podstawie [*Realizacja: wymagania lub warunki zdefiniowane przez organizację*].

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	SA-9	SA-9 (2)	SA-9 (2)

SA-10 ZARZĄDZANIE KONFIGURACJĄ DEWELOPERA

Zabezpieczenie: organizacja wymaga od twórców systemu teleinformatycznego, komponentu systemu lub usługi systemu teleinformatycznego, aby:

a) Zarządzali konfiguracją podczas pracy systemu, komponentu lub usługi w fazie [*Wybór (jeden lub więcej): projekt; rozwój; realizacja; operacja*];

b) Dokumentowali, zarządzali i kontrolowali integralność zmian w [*Realizacja: elementy konfiguracji zdefiniowane przez organizację w ramach zarządzania konfiguracją*];

c) Wprowadzali w życie tylko zatwierdzone przez organizację zmiany w systemie, komponencie lub usłudze;

d) Dokumentowali zatwierdzone zmiany w systemie, komponencie lub usłudze oraz potencjalny wpływ takich zmian na bezpieczeństwo;

e) Śledzili naruszenia bezpieczeństwa i usuwali te naruszenia w systemie, komponencie lub usłudze i zgłaszali ustalenia do [*Realizacja: personel zdefiniowany przez organizację*].

Zabezpieczenia powiązane: CM-3, CM-4, CM-9, SA-12, SI-2.

Zabezpieczenia rozszerzone:

(1) ZARZĄDZANIE KONFIGURACJĄ DEWELOPERA | WERYFIKACJA INTEGRALNOŚCI PROGRAMÓW / OPROGRAMOWANIA UKŁADOWEGO

Organizacja wymaga od twórcy systemu teleinformatycznego, komponentu systemu lub usługi systemu teleinformatycznego, aby umożliwiał weryfikację integralności oprogramowania i komponentów oprogramowania układowego.

Zabezpieczenia powiązane: SI-7.

(2) ZARZĄDZANIE KONFIGURACJĄ DEWELOPERA | ALTERNATYWNE PROCESY ZARZĄDZANIA KONFIGURACJĄ

Organizacja zapewnia alternatywny proces zarządzania konfiguracją przy użyciu personelu organizacyjnego w przypadku braku dedykowanego zespołu programistów zarządzającego konfiguracją.

(3) ZARZĄDZANIE KONFIGURACJĄ DEWELOPERA | WERYFIKACJA INTEGRALNOŚCI SPRZĘTU

Organizacja wymaga od twórcy systemu teleinformatycznego, komponentu systemowego lub usługi systemu teleinformatycznego, aby umożliwiał weryfikację integralności komponentów sprzętowych.

Zabezpieczenia powiązane: SI-7.

(4) ZARZĄDZANIE KONFIGURACJĄ DEWELOPERA | ZAUFANA GENERACJA

Organizacja wymaga od twórcy systemu teleinformatycznego, komponentu systemowego lub usługi systemu teleinformatycznego zastosowania narzędzi do porównywania nowo wygenerowanych wersji opisów sprzętu związanego z bezpieczeństwem, programów, oprogramowania układowego i kodu obiektowego z poprzednimi wersjami.

(5) ZARZĄDZANIE KONFIGURACJĄ DEWELOPERA | INTEGRALNOŚĆ MAPOWANIA KONTROLI WERSJI

Organizacja wymaga od twórcy systemu teleinformatycznego, komponentu systemu lub usługi systemu teleinformatycznego utrzymania integralności mapowania między danymi kompilacji głównej (sprzęt i programy/ oprogramowanie układowe) opisującymi aktualną wersję istotnego dla bezpieczeństwa sprzętu, aplikacji i oprogramowania układowego oraz zaktualizowaną kopią głównej wersji danych.

(6) ZARZĄDZANIE KONFIGURACJĄ DEWELOPERA | ZAUFANA DYSTRYBUCJA

Organizacja wymaga od twórcy systemu teleinformatycznego, komponentu systemowego lub usługi systemu teleinformatycznego wykonania procedur zapewniających, że istotne dla bezpieczeństwa sprzętu, oprogramowania i oprogramowania układowego aktualizacje dystrybuowane do organizacji są dokładnie takie, jak podano we wzorcach tych aktualizacji.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	SA-10 (opcjonalnie)	SA-10	SA-10

SA-11 TESTOWANIE I OCENA BEZPIECZEŃSTWA PRZEZ DEWELOPERA

Zabezpieczenie: Organizacja wymaga od dewelopera systemu teleinformatycznego, komponentu systemu lub usługi systemu teleinformatycznego, aby:

a) Utworzył i wdrożył plan oceny bezpieczeństwa;

b) Wykonał [*Wybór (jeden lub więcej): jednostkowe; konsolidacyjne; systemowe; zredukowane] testowanie / ocenę w [Realizacja: wielostopniowość i zakres zdefiniowane przez organizację*[46]];

c) Przedstawił dowody wykonania planu oceny bezpieczeństwa oraz wyniki testów / oceny bezpieczeństwa;

d) Wdrożył weryfikowalny proces usuwania zagrożeń;

e) Poprawił wady wykryte podczas testowania / oceny bezpieczeństwa.

Zabezpieczenia powiązane: CA-2, CM-4, SA-3, SA-4, SA-5, SI-2.

Zabezpieczenia rozszerzone:

[46] Wielostopniowość testowania/oceny zabezpieczeń odnosi się do rygoru i poziomu szczegółowości związanego z procesem oceny (np. czarna skrzynka, szara skrzynka lub testowanie białej skrzynki). Zakres testowania/oceny zabezpieczeń odnosi się do zakresu (tj. liczby i typu) artefaktów uwzględnionych w procesie oceny.

(1) TESTOWANIE I OCENA BEZPIECZEŃSTWA PRZEZ DEWELOPERA | ANALIZA KODU STATYCZNEGO

Organizacja wymaga od twórcy systemu teleinformatycznego, komponentu systemu lub usługi systemu teleinformatycznego zastosowania narzędzi do analizy kodu statycznego w celu zidentyfikowania typowych błędów i udokumentowania wyników analizy.

(2) TESTOWANIE I OCENA BEZPIECZEŃSTWA PRZEZ DEWELOPERA | ANALIZA ZAGROŻENIA I WRAŻLIWOŚCI

Organizacja wymaga od twórcy systemu teleinformatycznego, komponentu systemu lub usługi systemu teleinformatycznego przeprowadzenia analiz zagrożeń i podatności, a następnie testowania / oceny wykonanego systemu, komponentu lub usługi.

Zabezpieczenia powiązane: PM-15, RA-5.

(3) TESTOWANIE I OCENA BEZPIECZEŃSTWA PRZEZ DEWELOPERA | NIEZALEŻNA WERYFIKACJA PLANÓW OCENY / EWIDENCJA

Organizacja:

(a) Wymaga niezależnego organu spełniającego [Realizacja: kryteria niezależności zdefiniowane przez organizację] do zweryfikowania prawidłowego wdrożenia przez dewelopera planu oceny bezpieczeństwa i dowodów uzyskanych podczas testowania / oceny bezpieczeństwa;

(b) Zapewnia, że niezależny organ albo otrzymuje wystarczające informacje, aby ukończyć proces weryfikacji, albo udzielane jest mu upoważnienia do uzyskania takich informacji.

Zabezpieczenia powiązane: AT-3, CA-7, RA-5, SA-12.

(4) TESTOWANIE I OCENA BEZPIECZEŃSTWA PRZEZ DEWELOPERA | MANUALNY PRZEGLĄD KODU

Organizacja wymaga od dostawcy systemu teleinformatycznego, komponentu systemu lub usługi systemu teleinformatycznego ręcznego przeglądu kodu [*Przypisanie; kod zdefiniowany przez organizację*] przy użyciu [*Przypisanie; procesy, procedury i / lub techniki zdefiniowane przez organizację*].

(5) TESTOWANIE I OCENA BEZPIECZEŃSTWA PRZEZ DEWELOPERA | TESTOWANIE PENETRACYJNE

Organizacja wymaga od dostawcy systemu teleinformatycznego, komponentu systemu lub usługi systemu teleinformatycznego przeprowadzania testów penetracyjnych w [*Realizacja: zakres zdefiniowany przez organizację*] oraz z [*Realizacja: ograniczenia zdefiniowane przez organizację*].

(6) TESTOWANIE I OCENA BEZPIECZEŃSTWA PRZEZ DEWELOPERA | PRZEGLĄD PŁASZCZYZNY ATAKU

Organizacja wymaga od twórcy systemu teleinformatycznego, komponentu systemu lub usługi systemu teleinformatycznego przeprowadzenia przeglądów płaszczyzny ataku.

(7) TESTOWANIE I OCENA BEZPIECZEŃSTWA PRZEZ DEWELOPERA | WERYFIKACJA ZAKRESU TESTU / OCENA

Organizacja wymaga od twórcy systemu teleinformatycznego, komponentu systemu lub usługi systemu teleinformatycznego sprawdzenia, czy zakres testów / oceny bezpieczeństwa zapewnia pełne pokrycie wymaganych środków bezpieczeństwa w [*Realizacja: zdefiniowana przez organizację wielostopniowość testowania / oceny*].

(8) TESTOWANIE I OCENA BEZPIECZEŃSTWA PRZEZ DEWELOPERA | DYNAMICZNA ANALIZA KODU

Organizacja wymaga od twórcy systemu teleinformatycznego, komponentu systemu lub usługi systemu teleinformatycznego zastosowania narzędzi do dynamicznej analizy kodu w celu zidentyfikowania typowych błędów i udokumentowania wyników analizy.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	SA-11 (opcjonalnie)	SA-11	SA-11

SA-12 BEZPIECZEŃSTWO ŁAŃCUCHA DOSTAW

Zabezpieczenie: Organizacja chroni przed zagrożeniami łańcuch dostaw systemu teleinformatycznego, komponentu systemu lub usługi systemu teleinformatycznego, stosując [*Realizacja: środki bezpieczeństwa zdefiniowane przez organizację*] jako część kompleksowej, wielostopniowej strategii bezpieczeństwa informacji.

Zabezpieczenia powiązane: AT-3, CM-8, IR-4, PE-16, PL-8, SA-3, SA-4, SA-8, SA-10, SA-14, SA-15, SA-18 , SA-19, SC-29, SC-30, SC-38, SI-7.

Zabezpieczenia rozszerzone:

(1) OCHRONA ŁAŃCUCHA DOSTAW | STRATEGIE ZAKUPÓW / NARZĘDZIA / METODY

Organizacja stosuje [*Realizacja: zdefiniowane przez organizację dostosowane strategie akwizycji, narzędzia kontraktowe i metody zaopatrzenia*] do zakupu systemu teleinformatycznego, komponentu systemu lub usługi systemu teleinformatycznego od dostawców.

Zabezpieczenia powiązane: SA-19.

(2) OCHRONA ŁAŃCUCHA DOSTAW | PRZEGLĄD DOSTAWCÓW

Organizacja przeprowadza przegląd dostawców przed zawarciem umowy nabycia systemu teleinformatycznego, komponentu systemu lub usługi systemu teleinformatycznego.

(3) OCHRONA ŁAŃCUCHA DOSTAW | ZAUFANA WYSYŁKA I MAGAZYNOWANIE

[Włączone do SA-12 (1)].

(4) OCHRONA ŁAŃCUCHA DOSTAW | DYWERSYFIKACJA DOSTAWCÓW

[Włączone do SA-12 (13)].

(5) OCHRONA ŁAŃCUCHA DOSTAW | OGRANICZENIE SZKODY

Organizacja stosuje [*Realizacja: środki bezpieczeństwa zdefiniowane przez organizację*] w celu ograniczenia szkód ze strony potencjalnych przeciwników rozpoznających i atakujących organizacyjny łańcuch dostaw.

(6) OCHRONA ŁAŃCUCHA DOSTAW | MINIMALIZACJA CZASU ZAMÓWIENIA

[Włączone do SA-12 (1)].

(7) OCHRONA ŁAŃCUCHA DOSTAW | OCENY PRZED WYBOREM / ODBIOREM / AKTUALIZACJĄ

Organizacja dokonuje oceny systemu teleinformatycznego, komponentu systemu lub usługi systemu teleinformatycznego przed wyborem, akceptacją lub aktualizacją systemu.

Zabezpieczenia powiązane: CA-2, SA-11.

(8) OCHRONA ŁAŃCUCHA DOSTAW | WYKORZYSTANIE DOSTĘPNYCH ANALIZ WYWIADOWCZYCH

Organizacja wykorzystuje analizy wywiadowcze odnoszące się do wszystkich potencjalnych dostawców systemu teleinformatycznego, komponentu systemu lub usługi systemu teleinformatycznego.

Zabezpieczenia powiązane: SA-15.

(9) OCHRONA ŁAŃCUCHA DOSTAW | BEZPIECZEŃSTWO OPERACYJNE

Organizacja stosuje [*Realizacja: zabezpieczenia operacyjne zdefiniowane przez organizację)*] zgodnie z rekomendacjami wydawanymi na podstawie przepisów prawa w celu ochrony informacji związanych z łańcuchem dostaw systemu teleinformatycznego, komponentu systemu lub usługi systemu teleinformatycznego.

(10) OCHRONA ŁAŃCUCHA DOSTAW | OCENA ORYGINALNOŚCI I NIEZMIENNOŚCI

Organizacja stosuje [*Realizacja: środki bezpieczeństwa zdefiniowane przez organizację*], aby potwierdzić, że otrzymany system teleinformatyczny lub składnik systemu jest oryginalny i nie został zmieniony.

(11) OCHRONA ŁAŃCUCHA DOSTAW | TESTOWANIE PENETRACYJNE / ANALIZA ELEMENTÓW, PROCESÓW I WYKONAWCÓW

Organizacja stosuje [*Wybór (jeden lub więcej) analiza organizacyjna, niezależne analizy strony trzeciej, testy penetracyjne prowadzone przez organizację, testy penetracyjne wykonywane przez niezależnych podmiot*] procesów [*Realizacja: elementy, procesy i podmioty łańcucha dostaw zdefiniowane przez organizację,*] powiązanych z system teleinformatycznym, komponentem systemu lub usługą systemu teleinformatycznego.

Zabezpieczenia powiązane: RA-5.

(12) OCHRONA ŁAŃCUCHA DOSTAW | UMOWY MIĘDZYORGANIZACYJNE

Organizacja zawiera porozumienia i określa procedury współpracy z podmiotami zaangażowanymi w łańcuch dostaw systemu teleinformatycznego, komponentu systemu lub usługi systemu teleinformatycznego.

(13) OCHRONA ŁAŃCUCHA DOSTAW | KOMPONENTY KRYTYCZNE SYSTEMU INFORMATYCZNEGO

Organizacja stosuje [*Realizacja: środki bezpieczeństwa zdefiniowane przez organizację*], w celu zapewnienia dostawy odpowiednich elementów *[Realizacja: zdefiniowane przez organizację elementy systemu informacji krytycznej*].

(14) OCHRONA ŁAŃCUCHA DOSTAW | IDENTYFIKACJA I ŚLEDZENIE

Organizacja ustanawia i zachowuje unikalną identyfikację [*Realizacja: zdefiniowane przez organizację elementy łańcucha dostaw, procesy i podmioty*] systemu teleinformatycznego, komponentu systemu lub usługi systemu teleinformatycznego.

(15) OCHRONA ŁAŃCUCHA DOSTAW | MECHANIZMY ADRESOWANIA SŁABYCH STRON LUB WAD

Organizacja ustanawia procesy zaradcze w celu wyeliminowania słabości lub niedociągnięć elementów łańcucha dostaw zidentyfikowanych podczas niezależnych lub organizacyjnych ocen takich elementów.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	SA-12 (opcjonalnie)	SA-12 (opcjonalnie)	SA-12

SA-13 WIARYGODNOŚĆ

Zabezpieczenie: Organizacja:

a. Opisuje wiarygodność[47] wymaganą w [*Realizacja: system teleinformatyczny zdefiniowany przez organizację, komponent systemu teleinformatycznego lub usługę systemu teleinformatycznego*] wspierającą jego kluczowe działania / funkcje biznesowe;

b. Implementuje [*Realizacja: nakładki zabezpieczeń zdefiniowana przez organizację*], w celu osiągnięcia zamierzonej wiarygodności.

Zabezpieczenia powiązane: RA-2, SA-4, SA-8, SA-14, SC-3.

Zabezpieczenia rozszerzone: Brak.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P0	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	SA-13 (opcjonalnie)	SA-13 (opcjonalnie)	SA-13 (opcjonalnie)

[47] Czynniki wpływające na wiarygodność systemów informatycznych obejmują: (i) funkcjonalność zabezpieczeń (tj. funkcje zabezpieczeń, funkcje i/lub mechanizmy stosowane w systemie i jego środowisku działania); oraz (ii) zapewnienie bezpieczeństwa (tj. pewność, że zastosowane funkcje bezpieczeństwa są skuteczne)

SA-14 ANALIZA KRYTYCZNOŚCI

Zabezpieczenie: Organizacja identyfikuje krytyczne komponenty i funkcje systemu teleinformacyjnego, przeprowadzając analizę krytyczności [*Realizacja: systemy informacyjne zdefiniowane przez organizację, składniki systemu teleinformatycznego lub usługi systemu teleinformatycznego*] w [*Realizacja: punkty decyzyjne zdefiniowane przez organizację w cyklu życia systemu*].

Zabezpieczenia powiązane: CP-2, PL-2, PL-8, PM-1, SA-8, SA-12, SA-13, SA-15, SA-20.

Zabezpieczenia rozszerzone: Brak.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P0	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	SA-14 (opcjonalnie)	SA-14 (opcjonalnie)	SA-14 (opcjonalnie)

SA-15 PROCES ROZWOJU, STANDARDY I NARZĘDZIA

Zabezpieczenie: Organizacja:

a. Wymaga od dostawcy systemu teleinformatycznego, komponentu systemu lub usługi systemu teleinformatycznego, aby postępował zgodnie z udokumentowanym procesem rozwoju, który:
   1. Jednoznacznie odnosi się do wymagań bezpieczeństwa;
   2. Identyfikuje standardy i narzędzia stosowane w procesie rozwoju;
   3. Dokumentuje konkretne opcje narzędzi i konfiguracje narzędzi stosowane w procesie rozwoju;
   4. Dokumentuje, zarządza i zapewnia integralność zmian w procesie i / lub narzędziach wykorzystywanych w rozwoju;
b. Przegląda proces rozwoju, standardy, narzędzia i opcje / konfiguracje narzędzi z częstotliwością [*Realizacja: częstotliwość zdefiniowana przez organizację*] celem ustalenia, czy wybrany i zastosowany proces, standard, narzędzia i opcje / konfiguracje spełniają [*Realizacja: wymagania bezpieczeństwa zdefiniowane przez organizację*].

Zabezpieczenia powiązane: SA-3, SA-8.

Zabezpieczenia rozszerzone:

(1) PROCES ROZWOJU, STANDARDY I NARZĘDZIA | METRYKI JAKOŚCI

Organizacja wymaga od twórcy systemu teleinformatycznego, komponentu systemu lub usługi systemu teleinformatycznego, aby:

(a) Zdefiniował wskaźniki jakości na początku procesu rozwoju;

(b) Udostępnił świadectwo spełnienia wskaźników jakości [*Wybór (jeden lub więcej): [Realizacja: częstotliwość określona przez organizację] ; [Realizacja: etapy przeglądu programu zdefiniowane przez organizację] ; przy dostawie*].

(2) PROCES ROZWOJU, STANDARDY I NARZĘDZIA | NARZĘDZIA ŚLEDZENIA BEZPIECZEŃSTWA

Organizacja wymaga od twórcy systemu teleinformatycznego, komponentu systemu lub usługi systemu teleinformatycznego wybrania i zastosowania narzędzia do śledzenia bezpieczeństwa używanego podczas procesu programowania.

(3) PROCES ROZWOJU, STANDARDY I NARZĘDZIA | ANALIZA KRYTYCZNOŚCI

Organizacja wymaga od twórcy systemu teleinformatycznego, komponentu systemu lub usługi systemu teleinformatycznego przeprowadzenia analizy krytyczności w *[Realizacja: wielopoziomowość zdefiniowana przez organizację*] oraz w *[Realizacja: zdefiniowane przez organizację punkty decyzyjne w cyklu życia systemu*].

Zabezpieczenia powiązane: SA-4, SA-14.

(4) PROCES ROZWOJU, STANDARDY I NARZĘDZIA | MODELOWANIE ZAGROŻEŃ / ANALIZA WRAŻLIWOŚCI

Organizacja wymaga, aby deweloperzy wykonali modelowanie zagrożeń i analizę podatności na zagrożenia systemu teleinformatycznego w [*Realizacja: wielopoziomowość zdefiniowana przez organizację*], która:

(a) Wykorzystuje [*Realizacja: informacje zdefiniowane przez organizację dotyczące wpływu środowiska działania, znanych lub zakładanych zagrożeń oraz dopuszczalnych poziomów ryzyka*];

(b) Stosuje [*Realizacja: narzędzia i metody zdefiniowane przez organizację*];

(c) Przedstawia dowody, które spełniają [*Realizacja: kryteria akceptacji zdefiniowane przez organizację*].

Zabezpieczenia powiązane: SA-4.

(5) PROCES ROZWOJU, STANDARDY I NARZĘDZIA | OGRANICZENIE PŁASZCZYZNY ATAKU

Organizacja wymaga od twórcy systemu teleinformatycznego, komponentu systemu lub usługi systemu teleinformatycznego ograniczenia powierzchni ataku do *[Realizacja: progi zdefiniowane przez organizację*].

Zabezpieczenia powiązane: CM-7.

(6) PROCES ROZWOJU, STANDARDY I NARZĘDZIA | CIĄGŁE DOSKONALENIE

Organizacja wymaga od twórcy systemu teleinformatycznego, komponentu systemu lub usługi systemu teleinformatycznego wdrożenia jasno sprecyzowanego mechanizmu ciągłego doskonalenia procesu programowania.

(7) PROCES ROZWOJU, STANDARDY I NARZĘDZIA | AUTOMATYCZNA ANALIZA WRAŻLIWOŚCI

Organizacja wymaga od twórców systemu teleinformatycznego, komponentu systemu lub usługi systemu teleinformatycznego, aby:

(a) Wykonali automatyczną analizę podatności za pomocą [*Realizacja: narzędzia zdefiniowane przez organizację]*;

(b) Określili ewentualne wykorzystanie wykrytych luk;

(c) Określili potencjalne ograniczenie ryzyka dostarczonych słabych punktów systemu;

(d) Dostarczyli uzyskane dane wyjściowe i wyniki analizy do [*Realizacja: personel lub role zdefiniowane przez organizację*].

Zabezpieczenia powiązane: RA-5.

(8) PROCES ROZWOJU, STANDARDY I NARZĘDZIA | PONOWNIE UŻYCIE INFORMACJI O ZAGROŻENIACH / WRAŻLIWOŚCI

Organizacja wymaga od twórcy systemu teleinformatycznego, komponentu systemu lub usługi systemu teleinformatycznego, aby korzystał z modelowania zagrożeń i analiz podatności z adekwatnych systemów, komponentów lub usług w celu informowania o bieżącym procesie rozwoju zagrożeń.

(9) PROCES ROZWOJU, STANDARDY I NARZĘDZIA | KREATYWNE WYKORZYSTANIE DANYCH

Organizacja zatwierdza, dokumentuje i kontroluje kreatywne wykorzystanie danych w środowiskach programistycznych i testowych systemu teleinformatycznego, komponentu systemu lub usługi systemu teleinformatycznego.

(10) PROCES ROZWOJU, STANDARDY I NARZĘDZIA | PLAN ODPOWIEDZI NA INCYDENTY

Organizacja wymaga od twórcy systemu teleinformatycznego, komponentu systemu lub usługi systemu teleinformatycznego opracowania planu reagowania na incydenty.

Zabezpieczenia powiązane: IR-8.

(11) PROCES ROZWOJU, STANDARDY I NARZĘDZIA | SYSTEM ARCHIWIZACJI INFORMACJI / KOMPONENTY

Organizacja wymaga, aby twórca systemu teleinformatycznego lub komponentu systemu dokonał archiwizacji wydanego / dostarczonego systemu lub komponentu wraz z odpowiednimi dowodami wskazującymi na przeprowadzenie końcowego przeglądu bezpieczeństwa.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P2	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	SA-15 (opcjonalnie)	SA-15 (opcjonalnie)	SA-15

SA-16 SZKOLENIA PROWADZONE PRZEZ DEWELOPERA

Zabezpieczenie: organizacja wymaga od twórcy systemu teleinformatycznego, komponentu systemu lub usługi systemu teleinformatycznego zapewnienia szkolenia [*Realizacja: szkolenie zdefiniowane przez organizację*] na temat prawidłowego wykorzystania i działania zaimplementowanych funkcji bezpieczeństwa, kontroli i / lub mechanizmów.

Zabezpieczenia powiązane: AT-2, AT-3, SA-5.

Zabezpieczenia rozszerzone: Brak.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P2	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	SA-16 (opcjonalnie)	SA-16 (opcjonalnie)	SA-16

SA-17 ARCHITEKTURA I PROJEKT BEZPIECZEŃSTWA DEWELOPERA

Zabezpieczenie: organizacja wymaga od twórcy systemu teleinformatycznego, komponentu systemu lub usługi systemu teleinformatycznego opracowania specyfikacji projektowej i architektury bezpieczeństwa, która:

a. Jest spójna i wspiera architekturę bezpieczeństwa organizacji, która jest ustanowiona w ramach i jest integralną częścią architektury korporacyjnej organizacji;

b. Dokładnie i kompleksowo opisuje wymaganą funkcjonalność bezpieczeństwa oraz podział środków bezpieczeństwa pomiędzy komponenty fizyczne i logiczne;

c. Wskazuje, w jaki sposób poszczególne funkcje, mechanizmy i usługi bezpieczeństwa współpracują ze sobą, aby zapewnić wymagane możliwości bezpieczeństwa i jednolite podejście do ochrony.

Zabezpieczenia powiązane: PL-8, PM-7, SA-3, SA-8.

Zabezpieczenia rozszerzone:

(1) ARCHITEKTURA I PROJEKT BEZPIECZEŃSTWA DEWELOPERA | MODEL POLITYKI

Organizacja wymaga od twórcy systemu teleinformatycznego, komponentu systemu lub usługi systemu teleinformatycznego, aby:

(a) Opracował, jako integralną część procesu rozwoju, formalny model polityki opisujący [*Realizacja: zdefiniowane przez organizację elementy polityki bezpieczeństwa organizacji*], które należy egzekwować;

(b) Wykazał, że formalny model polityki jest wewnętrznie spójny i wystarczający do egzekwowania określonych elementów polityki bezpieczeństwa organizacji po zakończeniu wdrożenia.

(2) ARCHITEKTURA I PROJEKT BEZPIECZEŃSTWA DEWELOPERA | BAZOWE ELEMENTY BEZPIECZEŃSTWA

Organizacja wymaga od twórcy systemu teleinformatycznego, komponentu systemu lub usługi systemu teleinformatycznego, aby:

(a) Zdefiniował istotny dla bezpieczeństwa sprzęt, aplikacje i oprogramowanie sprzętowe;

(b) Przedstawił uzasadnienie, że definicja sprzętu, aplikacji i oprogramowania układowego dotyczącego bezpieczeństwa jest kompletna.

Zabezpieczenia powiązane: SA-5.

(3) ARCHITEKTURA I PROJEKT BEZPIECZEŃSTWA DEWELOPERA | FORMALNA SPECYFIKACJA

Organizacja wymaga od twórcy systemu teleinformatycznego, komponentu systemu lub usługi systemu teleinformatycznego, aby:

(a) Opracował, jako integralną część procesu rozwoju, formalną specyfikację najwyższego poziomu, która określa interfejsy sprzętowe istotne z punktu widzenia bezpieczeństwa, aplikacje oraz oprogramowanie układowe powiązane merytorycznie z wyjątkami, komunikatami o błędach i skutkami;

(b) Wykazał za pomocą możliwego do przeprowadzenia dowodu, a w razie potrzeby dodatkowo z nieformalną prezentacją, że istniejąca specyfikacja najwyższego poziomu jest zgodna z formalnym modelem polityki;

(c) Wykazał poprzez nieformalną prezentację, że formalna specyfikacja najwyższego poziomu obejmuje interfejsy z istotnym dla bezpieczeństwa sprzętem, aplikacjami i oprogramowaniem układowym;

(d) Wykazał, że formalna specyfikacja najwyższego poziomu jest dokładnym opisem zaimplementowanego, związanego z bezpieczeństwem sprzętu, aplikacji i oprogramowania układowego;

(e) Opisał mechanizmy związane z bezpieczeństwem sprzętu, aplikacji i oprogramowania układowego, które nie zostały uwzględnione w formalnej specyfikacji najwyższego poziomu, ale ściśle dotyczą sprzętu, oprogramowania i oprogramowania układowego związanego z bezpieczeństwem.

Zabezpieczenia powiązane: SA- 5.

(4) ARCHITEKTURA I PROJEKT BEZPIECZEŃSTWA DEWELOPERA | NIEFORMALNE SPECYFIKACJE

Organizacja wymaga od twórcy systemu teleinformatycznego, komponentu systemu lub usługi systemu teleinformatycznego, aby:

(a) Opracował, jako integralną część procesu rozwoju, nieformalną opisową specyfikację najwyższego poziomu, która określa interfejsy sprzętowe istotne z punktu widzenia bezpieczeństwa, aplikacje oraz oprogramowanie układowe powiązane merytorycznie z wyjątkami, komunikatami o błędach i skutkami;

(b) Wykazał poprzez [*Realizacja: nieformalna prezentacja, przekonujący argument metodami formalnymi, jeśli jest to wykonalne*], że opisowa specyfikacja najwyższego poziomu jest zgodna z formalnym modelem polityki;

(c) Wykazał poprzez nieformalną prezentację, że opisowa specyfikacja najwyższego poziomu obejmuje interfejsy z istotnym dla bezpieczeństwa sprzętem, aplikacjami i oprogramowaniem układowym;

(d) Wykazał, że opisowa specyfikacja najwyższego poziomu jest dokładnym opisem interfejsów, do istotnego z punktu widzenia bezpieczeństwa, sprzętu, aplikacji i oprogramowania układowego;

(e) Opisał mechanizmy związane z bezpieczeństwem sprzętu, aplikacji i oprogramowania układowego, które nie zostały wykazane w opisowej specyfikacji najwyższego poziomu, ale ściśle dotyczą sprzętu, oprogramowania i oprogramowania układowego związanego z bezpieczeństwem.

Zabezpieczenia powiązane: SA-5.

(5) ARCHITEKTURA I PROJEKT BEZPIECZEŃSTWA DEWELOPERA | PROSTY KONCEPCYJNIE PLAN

Organizacja wymaga od twórcy systemu teleinformatycznego, komponentu systemu lub usługi systemu teleinformatycznego, aby:

(a) Projektował i konstruował istotny dla bezpieczeństwa sprzęt, aplikacje i oprogramowanie układowe w celu wykorzystania kompletnego, koncepcyjnie prostego mechanizmu ochronnego z precyzyjnie zdefiniowaną semantyką;

(b) Ustrukturyzował wewnętrznie istotny dla bezpieczeństwa sprzęt, aplikacje i oprogramowanie układowe, ze szczególnym uwzględnieniem tego mechanizmu.

Zabezpieczenia powiązane: SC-3.

(6) ARCHITEKTURA I PROJEKT BEZPIECZEŃSTWA DEWELOPERA | STRUKTURA DO TESTOWANIA

Organizacja wymaga od twórcy systemu teleinformatycznego, komponentu systemu lub usługi systemu teleinformatycznego, aby ustrukturyzował istotny dla bezpieczeństwa sprzęt, aplikacje i oprogramowanie układowe w celu umożliwienia przeprowadzenia testów.

Zabezpieczenia powiązane: SA-11.

(7) ARCHITEKTURA I PROJEKT BEZPIECZEŃSTWA DEWELOPERA | STRUKTURA DLA NAJNIŻSZYCH UPRAWNIEŃ

Organizacja wymaga od dewelopera systemu teleinformatycznego, komponentu systemu lub usługi systemu teleinformatycznego, aby ustrukturyzował sprzęt, aplikacje i oprogramowanie układowe związane z bezpieczeństwem, aby ułatwić kontrolę dostępu z najmniejszymi uprawnieniami.

Zabezpieczenia powiązane: AC-5, AC-6.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	SA-17 (opcjonalnie)	SA-17 (opcjonalnie)	SA-17

SA-18 ODPORNOŚĆ NA SABOTAŻ I WYKRYWANIE MANIPULACJI

Zabezpieczenie: Organizacja wdraża program ochrony przed manipulacją systemu teleinformatycznego, komponentu systemu lub usługi systemu teleinformatycznego.

Zabezpieczenia powiązane: PE-3, SA-12, SI-7.

Zabezpieczenia rozszerzone:

(1) ODPORNOŚĆ NA SABOTAŻ I WYKRYWANIE MANIPULACJI | WIELOFAZOWOŚĆ CYKLU ŻYCIA SYSTEMU

Organizacja stosuje technologie i techniki zapobiegania manipulacjom podczas wielu faz cyklu życia systemu (SDLC - Systems Development Life Cycle), w tym projektowania, rozwoju, integracji, operacji i utrzymania systemu.

Zabezpieczenia powiązane: SA-3.

(2) ODPORNOŚĆ NA SABOTAŻ I WYKRYWANIE MANIPULACJI | KONTROLA SYSTEMÓW INFORMATYCZNYCH, KOMPONENTÓW LUB URZĄDZEŃ

Organizacja sprawdza [*Realizacja: zdefiniowane przez organizację systemy informacyjne, komponenty systemu lub urządzenia*] [*Wybór (jeden lub więcej): losowo; w [Realizacja: częstotliwość zdefiniowana przez organizację], po [Realizacja: wskazanie potrzeby kontroli określone przez organizację]*] w celu wykrycia naruszenia.

Zabezpieczenia powiązane: SI-4.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P0	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	SA-18 (opcjonalnie)	SA-18 (opcjonalnie)	SA-18 (opcjonalnie)

SA-19 AUTENTYCZNOŚĆ KOMPONENTÓW

Zabezpieczenie: Organizacja:

a. Opracowuje i wdraża politykę i procedury dotyczące zwalczania obrotu towarami nieautentycznymi, które obejmują środki wykrywania i zapobiegania przedostawaniu się podrobionych składników do systemu teleinformatycznego;

b. Zgłasza podrabiane komponenty systemu teleinformatycznego do [*Wybór (jeden lub więcej): źródło podrobionego komponentu; [Realizacja: zdefiniowane przez organizację zewnętrzne organy ścigania] ; [Realizacja: personel lub role zdefiniowane przez organizację]*].

Zabezpieczenia powiązane: PE-3, SA-12, SI-7.

Zabezpieczenia rozszerzone:

(1) AUTENTYCZNOŚĆ KOMPONENTÓW | SZKOLENIE / ROZPOZNAWANIE AUTENTYCZNOŚCI

Organizacja szkoli [*Realizacja: personel lub role zdefiniowane przez organizację*] w zakresie wykrywania nieautentycznych elementów systemu teleinformatycznego (w tym sprzętu, aplikacji i oprogramowania układowego).

(2) AUTENTYCZNOŚĆ KOMPONENTÓW | KONTROLA KONFIGURACJI NA POTRZEBY SERWISOWANIA / NAPRAWY KOMPONENTÓW

Organizacja utrzymuje kontrolę konfiguracji [*Realizacja: komponenty systemu teleinformatycznego zdefiniowane przez organizację*] oczekujących na serwis / naprawę i elementów poddanym serwisowaniu / komponentami naprawionymi oczekującymi na ponowne użycie.

(3) AUTENTYCZNOŚĆ KOMPONENTÓW | UTYLIZACJA KOMPONENTÓW

Organizacja pozbywa się komponentów systemu teleinformatycznego przy użyciu [*Realizacja: techniki i metody zdefiniowane przez organizację*].

(4) AUTENTYCZNOŚĆ KOMPONENTÓW | SKANOWANIE AUTENTYCZNOŚCI

Organizacja skanuje komponenty systemu teleinformatycznego w poszukiwaniu nieoryginalnych elementów z częstotliwością [*Realizacja: częstotliwość zdefiniowana przez organizację*].

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P0	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	SA-19 (opcjonalnie)	SA-19 (opcjonalnie)	SA-19 (opcjonalnie)

SA-20 NIESTANDARDOWA (NA ZAMÓWIENIE) ROZBUDOWA KOMPONENTÓW KRYTYCZNYCH

Zabezpieczenie: organizacja ponownie implementuje lub opracowuje na zamówienie [*Realizacja: zdefiniowane przez organizację elementy systemu informacji krytycznej*].

Zabezpieczenia powiązane: CP-2, SA-8, SA-14.

Zabezpieczenia rozszerzone: Brak.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P0	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	SA-20 (opcjonalnie)	SA-20 (opcjonalnie)	SA-20 (opcjonalnie)

SA-21 DOBÓR DEWELOPERÓW

Zabezpieczenie: organizacja wymaga, aby twórca [*Realizacja: system teleinformatyczny zdefiniowany przez organizację, komponent systemu lub usługa systemu teleinformatycznego*]:

a. Posiadał odpowiednie uprawnienia dostępu określone przez przydzielone obowiązki [*Realizacja: oficjalne obowiązki określone przez organizację*];

b. Spełniał dodatkowe kryteria [*Realizacja: zdefiniowane przez organizację dodatkowe kryteria kontroli personelu*].

Zabezpieczenia powiązane: PS-3, PS-7.

Zabezpieczenia rozszerzone:

(1) DOBÓR DEWELOPERÓW | OCENA PRZEGLĄDU

Organizacja wymaga od twórcy systemu teleinformatycznego, komponentu systemu lub usługi systemu teleinformatycznego podjęcia środków [*Realizacja: działania zdefiniowane przez organizację*], aby upewnić się, że spełnione są wymagane uprawnienia dostępu i kryteria kontroli.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P0	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	SA-21 (opcjonalnie)	SA-21 (opcjonalnie)	SA-21 (opcjonalnie)

SA-22 KOMPONENTY SYSTEMU BEZ WSPARCIA

Zabezpieczenie: Organizacja:

a. Zastępuje komponenty systemu teleinformatycznego, gdy wsparcie dla komponentów nie jest już zapewniane przez twórcę, dostawcę lub producenta;

b. Dostarcza uzasadnienie i dokumenty potwierdzające dalsze używanie nieobsługiwanych komponentów systemu wymaganych do spełnienia wymagań biznesowych.

Zabezpieczenia powiązane: PL-2, SA-3.

Zabezpieczenia rozszerzone:

(1) KOMPONENTY SYSTEMU BEZ WSPARCIA | ALTERNATYWNE ŹRÓDŁA STAŁEGO WSPARCIA

Organizacja zapewnia [*Wybór (jeden lub więcej): wsparcie wewnętrzne; [Realizacja: wsparcie zdefiniowane przez organizację od zewnętrznych dostawców]*] dla nieobsługiwanych komponentów systemu teleinformatycznego.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P0	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	SA-22 (opcjonalnie)	SA-22 (opcjonalnie)	SA-22 (opcjonalnie)

KATEGORIA: OCHRONA SYSTEMÓW I SIECI TELEKOMUNIKACYJNYCH

SC-1 POLITYKA I PROCEDURY OCHRONY SYSTEMÓW I SIECI TELEKOMUNIKACYJNYCH

Zabezpieczenie: Organizacja:

a. Opracowuje, dokumentuje i rozpowszechnia w odniesieniu do [*Realizacja: personel lub role zdefiniowane przez organizację*]:

   1. Politykę ochrony systemów i sieci telekomunikacyjnych, która dotyczy celu, zakresu, ról, obowiązków, zaangażowania kierownictwa, koordynacji między jednostkami organizacyjnymi oraz spójności działania;

   2. Procedury ułatwiające wdrażanie polityki ochrony systemów i sieci telekomunikacyjnych oraz powiązane środki ochrony systemów i sieci telekomunikacyjnych;

b. Przegląda i aktualizuje bieżącą:

   1. Politykę ochrony systemów i sieci telekomunikacyjnych z częstotliwością [*Realizacja: częstotliwość określona przez organizację*];

   2. Procedury ochrony systemów i sieci telekomunikacyjnych z częstotliwością [*Realizacja: częstotliwość określona przez organizację*].

Zabezpieczenia powiązane: PM-9.

Zabezpieczenia rozszerzone: Brak.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	SC-1	SC-1	SC-1

SC-2 SEPARACJA

Zabezpieczenie: System teleinformatyczny oddziela funkcje użytkownika (w tym usługi interfejsu użytkownika) od funkcji zarządzania systemem teleinformatycznym.

Zabezpieczenia powiązane: SA-4, SA-8, SC-3.

Zabezpieczenia rozszerzone:

(1) SEPARACJA | INTERFEJSY DLA UŻYTKOWNIKÓW NIEUPRZYWILEJOWANYCH

System teleinformatyczny zapobiega prezentacji funkcji związanych z zarządzaniem systemem teleinformatycznym w interfejsie dedykowanym dla użytkowników nieuprzywilejowanych.

Zabezpieczenia powiązane: AC-3.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	SC-2 (opcjonalnie)	SC-2	SC-2

SC-3 IZOLACJA FUNKCJI BEZPIECZEŃSTWA

Zabezpieczenie: System teleinformatyczny izoluje funkcje bezpieczeństwa od funkcji niezwiązanych z bezpieczeństwem.

Zabezpieczenia powiązane: AC-3, AC-6, SA-4, SA-5, SA-8, SA-13, SC-2, SC-7, SC-39.

Zabezpieczenia rozszerzone:

(1) IZOLACJA FUNKCJI BEZPIECZEŃSTWA | SEPARACJA PODZESPOŁÓW

System teleinformatyczny wykorzystuje podstawowe mechanizmy separacji podzespołów do wdrożenia izolacji funkcji bezpieczeństwa.

(2) IZOLACJA FUNKCJI BEZPIECZEŃSTWA | FUNKCJE KONTROLI DOSTĘPU / PRZEPŁYWU

System teleinformatyczny izoluje funkcje bezpieczeństwa wymuszające kontrolę dostępu i przepływu informacji od innych funkcji bezpieczeństwa oraz funkcji niezwiązanych z bezpieczeństwem.

(3) IZOLACJA FUNKCJI BEZPIECZEŃSTWA | MINIMALIZACJA FUNKCJONALNOŚCI NIEZWIĄZANYCH Z BEZPIECZEŃSTWEM

Organizacja minimalizuje liczbę funkcji niezwiązanych z zabezpieczeniami i izoluje je od funkcji bezpieczeństwa.

(4) IZOLACJA FUNKCJI BEZPIECZEŃSTWA | MODUŁ SPRZĘŻENIA I SPÓJNOŚCI

Organizacja wdraża funkcje bezpieczeństwa jako niezależne moduły, które maksymalizują wewnętrzną spójność modułów i minimalizują sprzężenie między modułami.

(5) IZOLACJA FUNKCJI BEZPIECZEŃSTWA | STRUKTURY WARSTWOWE

Organizacja wdraża funkcje bezpieczeństwa jako strukturę warstwową, minimalizując interakcje między warstwami projektu i unikając jakiejkolwiek zależności niższych warstw od funkcjonalności lub poprawności wyższych warstw.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	SC-3 (opcjonalnie)	SC-3 (opcjonalnie)	SC-3

SC-4 INFORMACJE NA WSPÓŁDZIELONYCH ZASOBACH

Zabezpieczenie: System teleinformatyczny zapobiega nieautoryzowanemu i niezamierzonemu przesyłaniu informacji za pośrednictwem współużytkowanych zasobów systemowych.

Zabezpieczenia powiązane: AC-3, AC-4, MP-6.

Zabezpieczenia rozszerzone:

(1) INFORMACJE NA WSPÓŁDZIELONYCH ZASOBACH | POZIOMY BEZPIECZEŃSTWA

[Włączone do SC-4].

(2) INFORMACJE NA WSPÓŁDZIELONYCH ZASOBACH | PRZETWARZANIE OKRESOWE

System teleinformatyczny zapobiega nieuprawnionemu przesyłaniu informacji za pośrednictwem współdzielonych zasobów zgodnie z [*Realizacja: procedury zdefiniowane przez organizację*], gdy system procesujący przełącza się między różnymi poziomami klasyfikacji informacji lub kategoriami bezpieczeństwa.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	SC-4 (opcjonalnie)	SC-4	SC-4

SC-5 OCHRONA PRZED BLOKADĄ USŁUG (DoS)

Zabezpieczenie: System teleinformatyczny chroni przed lub ogranicza skutki następujących rodzajów ataków typu „blokada usługi": [*Realizacja: typy ataków typu „blokada usługi" zdefiniowane przez organizację lub odniesienia do źródeł takich informacji*] poprzez zastosowanie [*Realizacja: zdefiniowane przez organizację środki bezpieczeństwa*].

Zabezpieczenia powiązane: SC-6, SC-7.

Zabezpieczenia rozszerzone:

(1) OCHRONA PRZED BLOKADĄ USŁUGI (DoS, DDoS) | OGRANICZENIE UŻYTKOWNIKÓW WEWNĘTRZNYCH

System teleinformatyczny ogranicza zdolność osób do przeprowadzania ataków [*Realizacja: ataki typu „blokada usługi" zdefiniowana przez organizację*] na inne systemy teleinformatyczne.

(2) OCHRONA PRZED BLOKADĄ USŁUGI | NADMIAROWOŚĆ / SZEROKOŚĆ PASMA / REDUNDANCJA

System teleinformatyczny zarządza nadmiarowością przepustowości, szerokością pasma lub innym tożsamym zabezpieczeniem w celu ograniczenia skutków ataków typu „blokada usługi" DoS.

(3) OCHRONA PRZED BLOKADĄ USŁUGI | WYKRYWANIE / MONITOROWANIE

Organizacja:

(a) Wykorzystuje [*Realizacja: narzędzia monitorowania zdefiniowane przez organizację*] do wykrywania wskaźników ataków typu „blokada usługi" na system teleinformatyczny;

(b) Monitoruje [*Realizacja: zasoby systemu teleinformatycznego zdefiniowane przez organizację*] celem ustalenia, czy istnieją wystarczające zasoby zabezpieczające przed skutecznymi atakami typu „blokada usługi".

Zabezpieczenia powiązane: CA-7, SI-4.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	SC-5	SC-5	SC-5

SC-6 DOSTĘPNOŚĆ ZASOBÓW

Zabezpieczenie: System teleinformatyczny chroni dostępność zasobów, przydzielając [*Realizacja: zasoby zdefiniowane przez organizację*] przez stosowanie [*Wybór (jeden lub więcej); pierwszeństwo; przydział; [Realizacja: zabezpieczenia bezpieczeństwa zdefiniowane przez organizację]*].

Zabezpieczenia rozszerzone: Brak.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P0	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	SC-6 (opcjonalnie)	SC-6 (opcjonalnie)	SC-6 (opcjonalnie)

SC-7 OCHRONA POŁĄCZEŃ BRZEGOWYCH

Zabezpieczenie: System teleinformatyczny:

a. Monitoruje i kontroluje komunikację brzegowych urządzeń systemu i na kluczowych wewnętrznych granicach w systemie;

b. Implementuje podsieci publicznie dostępnych komponentów systemu, które są [*Wybór: fizycznie; logicznie*] oddzielone od wewnętrznych sieci organizacyjnych;

c. Łączy się z zewnętrznymi sieciami lub systemami teleinformatycznymi tylko za pośrednictwem zarządzanych interfejsów składających się z chronionych urządzeń brzegowych zainstalowanych zgodnie z architekturą bezpieczeństwa organizacji.

Zabezpieczenia powiązane: AC-4, AC-17, CA-3, CM-7, CP-8, IR-4, RA-3, SC-5, SC-13.

Zabezpieczenia rozszerzone:

(1) OCHRONA POŁĄCZEŃ BRZEGOWYCH | FIZYCZNIE ODDZIELONE PODSIECI

[Włączono do SC-7].

(2) OCHRONA POŁĄCZEŃ BRZEGOWYCH | DOSTĘP PUBLICZNY

[Włączone do SC-7].

(3) OCHRONA POŁĄCZEŃ BRZEGOWYCH | PUNKTY DOSTĘPOWE

Organizacja ogranicza liczbę zewnętrznych połączeń sieciowych do systemu teleinformatycznego.

(4) OCHRONA POŁĄCZEŃ BRZEGOWYCH | ZEWNĘTRZNE USŁUGI TELEKOMUNIKACYJNE

Organizacja:

(a) Wdraża interfejs zarządzany dla każdej zewnętrznej usługi telekomunikacyjnej;

(b) Ustanawia politykę przepływu ruchu dla każdego zarządzanego interfejsu;

(c) Chroni poufność i integralność informacji przesyłanych przez każdy interfejs;

(d) Dokumentuje każdy wyjątek od polityki przepływu ruchu wynikający z misji / potrzeb biznesowych i czas trwania tego wyjątku;

(e) Przegląda wyjątki od polityki przepływu ruchu z częstotliwością [*Realizacja: częstotliwość zdefiniowana przez organizację*] i usuwa te wyjątki, które nie są już wymagane.

Zabezpieczenia powiązane: SC-8.

(5) OCHRONA POŁĄCZEŃ BRZEGOWYCH | ODRZUĆ DOMYŚLNIE / POZWÓL NA WYJĄTEK

System teleinformatyczny na zarządzanych interfejsach domyślnie blokuje telekomunikacyjny ruch sieciowy i zezwala na ten ruch w drodze wyjątku (tj. odmawiaj wszystkim, zezwalaj na wyjątek).

(6) OCHRONA POŁĄCZEŃ BRZEGOWYCH | ODPOWIEDŹ NA ROZPOZNANE AWARIE

[Włączono do SC-7 (18)].

(7) OCHRONA POŁĄCZEŃ BRZEGOWYCH | ZAPOBIEGANIE PODZIAŁOWI TUNELOWANIA ZDALNYCH URZĄDZEŃ

System teleinformatyczny, połączony ze zdalnym urządzeniem, zapobiega równoczesnemu nawiązywaniu przez to urządzenie połączenia z tym systemem i komunikowania się za pośrednictwem innego połączenia z zasobami sieci zewnętrznych.

(8) OCHRONA POŁĄCZEŃ BRZEGOWYCH | RUCH TELEKOMUNIKACYJNY DO AUTORYZOWANYCH SERWERÓW PROXY

System teleinformatyczny kieruje [*Realizacja: ruch telekomunikacyjny zdefiniowany przez organizację*] do [*Realizacja: sieci zewnętrzne zdefiniowane przez organizację*] przez zarządzane interfejsy uwierzytelnionych serwerów proxy.

Zabezpieczenia powiązane: AC-3, AU-2.

(9) OCHRONA POŁĄCZEŃ BRZEGOWYCH | OGRANICZENIE ZAGROŻEŃ WYJŚCIOWEGO RUCHU TELEKOMUNIKACYJNEGO

System teleinformatyczny:

(a) Wykrywa i odrzuca wychodzący ruch telekomunikacyjny stanowiący zagrożenie dla zewnętrznych systemów teleinformatycznych;

(b) Kontroluje tożsamość użytkowników wewnętrznych skojarzonych z odmową komunikacji.

Zabezpieczenia powiązane: AU-2, AU-6, SC-38, SC-44, SI-3, SI-4.

(10) OCHRONA POŁĄCZEŃ BRZEGOWYCH | ZAPOBIEGANIE NIEAUTORYZOWANEJ EKSFILTRACJI

Organizacja zapobiega nieautoryzowanej eksfiltracji informacji między zarządzanymi interfejsami.

Zabezpieczenia powiązane: SI-3.

(11) OCHRONA POŁĄCZEŃ BRZEGOWYCH | OGRANICZENIE DOTYCZĄCE RUCHU WEJŚCIOWEGO

System teleinformatyczny pozwala jedynie na przekazywanie komunikacji przychodzącej z [*Realizacja: autoryzowane źródła zdefiniowane przez organizację*] do [*Realizacja: autoryzowane miejsca docelowe zdefiniowane przez organizację*].

Zabezpieczenia powiązane: AC-3.

(12) OCHRONA POŁĄCZEŃ BRZEGOWYCH | SYSTEM OCHRONY KOMPUTERA GŁÓWNEGO TYPU HOST

Organizacja wdraża *[Realizacja: zdefiniowane przez organizację mechanizmy ochrony granic systemu oparte na komputerze głównym typu Host*] w [Realizacja: zdefiniowane przez organizację elementy systemu teleinformatycznego].

(13) OCHRONA POŁĄCZEŃ BRZEGOWYCH | IZOLACJA NARZĘDZI BEZPIECZEŃSTWA / MECHANIZMÓW / KOMPONENTÓW WSPARCIA

Organizacja izoluje *[Realizacja: zdefiniowane przez organizację narzędzia, mechanizmy i komponenty bezpieczeństwa informacji*] od innych wewnętrznych komponentów systemu teleinformatycznego, wdrażając fizycznie oddzielone podsieci z zarządzanymi interfejsami do innych komponentów systemu.

Zabezpieczenia powiązane: SA-8, SC-2, SC-3.

(14) OCHRONA POŁĄCZEŃ BRZEGOWYCH | OCHRONA PRZED NIEAUTORYZOWANYMI POŁĄCZENIAMI FIZYCZNYMI

Organizacja chroni przed nieautoryzowanymi połączeniami fizycznymi do [*Realizacja: interfejsy zarządzane zdefiniowane przez organizację*].

Zabezpieczenia powiązane: PE-4, PE-19.

(15) OCHRONA POŁĄCZEŃ BRZEGOWYCH | DOSTĘP DO SIECI UPRAWNIONEJ

System teleinformatyczny kieruje wszystkie uprzywilejowane połączenia sieciowe poprzez dedykowany, zarządzany interfejs w celu kontroli dostępu i audytu.

Zabezpieczenia powiązane: AC-2, AC-3, AU-2, SI-4.

(16) OCHRONA POŁĄCZEŃ BRZEGOWYCH | ZAPOBIEGANIE WYKRYWANIU KOMPONENTÓW / URZĄDZEŃ

System teleinformatyczny zapobiega wykrywaniu określonych składników systemu tworzących interfejs zarządzany.

(17) OCHRONA POŁĄCZEŃ BRZEGOWYCH | AUTOMATYCZNE EGZEKWOWANIE FORMATÓW PROTOKOŁU

System teleinformatyczny automatycznie wymusza przestrzeganie formatów protokołów.

Zabezpieczenia powiązane: SC-4.

(18) OCHRONA POŁĄCZEŃ BRZEGOWYCH | BŁĄD BEZPIECZEŃSTWA

W przypadku awarii urządzenia brzegowego zabezpieczającego granicę systemu teleinformatycznego system przechodzi do stanu bezpiecznego.

Zabezpieczenia powiązane: CP-2, SC-24.

(19) OCHRONA POŁĄCZEŃ BRZEGOWYCH | BLOKOWANIE TELEKOMUNIKACJI Z HOSTAMI SPOZA ORGANIZACJI

System teleinformatyczny blokuje zarówno przychodzący, jak i wychodzący ruch telekomunikacyjny między [*Realizacja: klientami telekomunikacji zdefiniowanymi przez organizację*], który jest niezależnie konfigurowany przez użytkowników końcowych i zewnętrznych dostawców usług.

(20) OCHRONA POŁĄCZEŃ BRZEGOWYCH | DYNAMICZNA IZOLACJA / SEGREGACJA

System teleinformatyczny umożliwia dynamiczną izolację / segregację [*Realizacja: elementy systemu teleinformatycznego zdefiniowane przez organizację*] od innych elementów systemu.

(21) OCHRONA POŁĄCZEŃ BRZEGOWYCH | IZOLACJA KOMPONENTÓW SYSTEMU TELEINFORMATYCZNEGO

Organizacja stosuje mechanizmy ochrony granic, aby oddzielić [*Realizacja: komponenty systemu teleinformatycznego zdefiniowane przez organizację*] wspierające [*Realizacja: misje i / lub funkcje biznesowe zdefiniowane przez organizację*].

Zabezpieczenia powiązane: CA-9, SC-3.

(22) OCHRONA POŁĄCZEŃ BRZEGOWYCH | ODDZIELNE PODSIECI DO PODŁĄCZENIA DO RÓŻNYCH DOMEN BEZPIECZEŃSTWA

System teleinformatyczny implementuje oddzielne adresy sieciowe (tj. różne podsieci) w celu łączenia się z systemami w różnych domenach bezpieczeństwa.

(23) OCHRONA POŁĄCZEŃ BRZEGOWYCH | WYŁĄCZENIE INFORMACJI ZWROTNEJ NADAWCY W PRZYPADKU AWARII PROTOKOŁU UWIERZYTELNIAJĄCEGO

System teleinformatyczny wyłącza informacje zwrotne do nadawców przy niepowodzeniu uwierzytelnienia poprawności formatu protokołu.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	SC-7	SC-7 (3) (4) (5) (7)	SC-7 (3) (4) (5) (7) (8) (18) (21)

SC-8 POUFNOŚĆ I INTEGRALNOŚĆ TRANSMISJI

Zabezpieczenie: System teleinformatyczny chroni [*Wybór (jeden lub więcej): poufność; integralność*] przesyłanych informacji.

Zabezpieczenia powiązane: AC-17, PE-4.

Zabezpieczenia rozszerzone:

(1) POUFNOŚĆ I INTEGRALNOŚĆ TRANSMISJI | KRYPTOGRAFICZNA LUB ALTERNATYWNA OCHRONA FIZYCZNA

System teleinformatyczny wprowadza mechanizmy kryptograficzne celem [*Wybór (jeden lub więcej): zapobieganie nieuprawnionemu ujawnieniu informacji; wykrywanie zmian informacji*] podczas transmisji, chyba że jest ona chroniony przez [*Realizacja: zdefiniowane przez organizację alternatywne zabezpieczenia fizyczne*].

Zabezpieczenia powiązane: SC-13.

(2) POUFNOŚĆ I INTEGRALNOŚĆ TRANSMISJI | OBSŁUGA „PRZED" i „PO" TRANSMISJI

System teleinformatyczny utrzymuje [*Wybór (jeden lub więcej): poufność; integralność*] informacji podczas przygotowania do transmisji i po odbiorze.

Zabezpieczenia powiązane: AU-10.

(3) POUFNOŚĆ I INTEGRALNOŚĆ TRANSMISJI | OCHRONA KRYPTOGRAFICZNA ZEWNĘTRZNYCH KOMUNIKATÓW

System teleinformatyczny wdraża mechanizmy kryptograficzne w celu ochrony zewnętrznych wiadomości[48], chyba że jest chroniony przez [*Realizacja: zdefiniowane przez organizację alternatywne zabezpieczenia fizyczne*[49]].

Zabezpieczenia powiązane: SC-12, SC-13.

[48] Zewnętrzne wiadomości obejmują na przykład nagłówki wiadomości / informacje o routingu.

[49] Alternatywne zabezpieczenia fizyczne obejmują np. chronione systemy dystrybucji.

(4) POUFNOŚĆ I INTEGRALNOŚĆ TRANSMISJI | KOMUNIKACJA UKRYTA / LOSOWA

System teleinformatyczny wdraża mechanizmy kryptograficzne w celu maskowania lub nadania losowości wzorcom komunikacji, chyba że jest chroniony przez [*Realizacja: zdefiniowane przez organizację alternatywne zabezpieczenia fizyczne*].

Zabezpieczenia powiązane: SC-12, SC-13.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	SC-8 (opcjonalnie)	SC-8 (1)	SC-8 (1)

SC-9 POUFNOŚĆ TRANSMISJI

[Włączony do SC-8].

SC-10 ZAKOŃCZENIE POŁĄCZENIA SIECIOWEGO

Zabezpieczenie: System teleinformatyczny przerywa połączenie sieciowe związane z sesją komunikacyjną po zakończeniu sesji lub po bezczynności trwającej [*Realizacja: okres zdefiniowany przez organizację*] .

Zabezpieczenia rozszerzone: Brak.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P2	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	SC-10 (opcjonalnie)	SC-10	SC-10

SC-11 ZAUFANA ŚCIEŻKA KOMUNIKACYJNA

Zabezpieczenie: System teleinformatyczny ustanawia zaufaną ścieżkę komunikacyjną[50] między użytkownikiem, a następującymi funkcjami bezpieczeństwa systemu: [*Realizacja: funkcje bezpieczeństwa zdefiniowane przez organizację, które obejmują co najmniej podwójne uwierzytelnianie systemu teleinformatycznego*].

Zabezpieczenia powiązane: AC-16, AC-25.

Zabezpieczenia rozszerzone:

(1) ZAUFANA ŚCIEŻKA KOMUNIKACYJNA | IZOLACJA LOGICZNA

System teleinformatyczny zapewnia zaufaną ścieżkę komunikacyjną, która jest logicznie izolowana i odróżnia się od innych ścieżek.

Zabezpieczenia powiązane: Brak.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P0	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	SC-11 (opcjonalnie)	SC-11 (opcjonalnie)	SC-11 (opcjonalnie)

SC-12 GENEROWANIE I ZARZĄDZANIE KLUCZAMI KRYPTOGRAFICZNYMI

Zabezpieczenie: Organizacja ustanawia i zarządza kluczami kryptograficznymi systemu kryptograficznego stosowanego w systemie teleinformatycznym zgodnie z polityką [*Realizacja: zdefiniowane przez organizację wymagania dotyczące generowania, dystrybucji, przechowywania, dostępu i niszczenia kluczy*].

Zabezpieczenia powiązane: SC-13, SC-17.

[50] Zaufane ścieżki - mechanizmy, za pomocą których użytkownicy mogą komunikować się za pośrednictwem urządzeń wejściowych bezpośrednio z funkcjami bezpieczeństwa systemów teleinformatycznych z niezbędną gwarancją wsparcia zasad bezpieczeństwa informacji.

Zabezpieczenia rozszerzone:

(1) GENEROWANIE I ZARZĄDZANIE KLUCZAMI KRYPTOGRAFICZNYMI | DOSTĘPNOŚĆ

Organizacja utrzymuje dostępność informacji w przypadku utraty kluczy kryptograficznych przez użytkowników.

(2) GENEROWANIE I ZARZĄDZANIE KLUCZAMI KRYPTOGRAFICZNYMI | KLUCZE SYMETRYCZNE

Organizacja generuje, kontroluje i dystrybuuje symetryczne klucze kryptograficzne przy użyciu [*Wybór jednego: Realizacja: zgodnie z wewnętrzną regulacją organizacji lub przepisami prawa; zatwierdzone przez rola w organizacji*] procesem generowania i zarządzania kluczami.

(3) GENEROWANIE I ZARZĄDZANIE KLUCZAMI KRYPTOGRAFICZNYMI | KLUCZE ASYMETRYCZNE

Organizacja generuje, kontroluje i dystrybuuje asymetryczne klucze kryptograficzne przy użyciu [*Wybór jednego: Realizacja: technologia i procesy zarządzania kluczami zatwierdzone przez rola w organizacji; zatwierdzone certyfikaty infrastruktury klucza publicznego klasy 3 lub wstępnie przygotowany materiał klucza; zatwierdzone certyfikaty infrastruktury klucza publicznego klasy 3 lub klasy 4*[51] *oraz sprzętowe tokeny zabezpieczające, które chronią klucz prywatny użytkownika*].

(4) GENEROWANIE I ZARZĄDZANIE KLUCZAMI KRYPTOGRAFICZNYMI | CERTYFIKATY INFRASTRUKTURY KLUCZA PUBLICZNEGO

[Włączone do SC-12].

(5) GENEROWANIE I ZARZĄDZANIE KLUCZAMI KRYPTOGRAFICZNYMI | CERTYFIKATY INFRASTRUKTURY KLUCZA PUBLICZNEGO / TOKENY SPRZĘTOWE

[Włączono do SC-12].

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	SC-12	SC-12	SC-12 (1)

[51] Klasa 1 dla osób fizycznych, przeznaczona do wiadomości e-mail.
Klasa 2 dla organizacji, dla których wymagany jest dowód tożsamości.
Klasa 3 do podpisywania serwerów i oprogramowania, dla których przeprowadzana jest niezależna weryfikacja i kontrola tożsamości i uprawnień przez urząd certyfikacji.
Klasa 4 do transakcji biznesowych online między firmami.
Klasa 5 dla organizacji prywatnych lub bezpieczeństwa rządowego.

SC-13 OCHRONA KRYPTOGRAFICZNA

Zabezpieczenie: System teleinformatyczny wdraża [*Realizacja: zdefiniowane przez organizację zastosowania kryptograficzne i rodzaj kryptografii wymagany do każdego użycia*] zgodnie z obowiązującymi przepisami, zarządzeniami wykonawczymi, dyrektywami, politykami, przepisami i standardami.

Zabezpieczenia powiązane: AC-2, AC-3, AC-7, AC-17, AC-18, AU-9, AU-10, CM-11, CP-9, IA-3, IA-7, MA-4 , MP-2, MP-4, MP-5, SA-4, SC-8, SC-12, SC-28, SI-7.

Zabezpieczenia rozszerzone: Brak.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	SC-13	SC-13	SC-13

SC-14 OCHRONA DOSTĘPU PUBLICZNEGO

[Zdolność zapewniona przez AC-2, AC-3, AC-5, AC-6, SI-3, SI-4, SI-5, SI-7, SI-10].

SC-15 WSPÓŁPRACUJĄCE URZĄDZENIA KOMPUTEROWE

Zabezpieczenie: System teleinformatyczny:

a. Zabrania zdalnej aktywacji współpracujących urządzeń komputerowych z następującymi wyjątkami: [*Realizacja: zdefiniowane przez organizację wyjątki, w których dozwolona jest zdalna aktywacja*];

b. Zapewnia wyraźne wskazanie fizycznego użytkownika urządzenia.

Zabezpieczenia powiązane: AC-21.

Zabezpieczenia rozszerzone:

(1) WSPÓŁPRACUJĄCE URZĄDZENIA KOMPUTEROWE | ODŁĄCZENIE FIZYCZNE

System teleinformatyczny zapewnia fizyczne odłączenie współpracujących urządzeń w sposób ułatwiający obsługę.

(2) WSPÓŁPRACUJĄCE URZĄDZENIA KOMPUTEROWE | BLOKOWANIE RUCHU WEJŚCIOWEGO / WYJŚCIOWEGO

[Włączono do SC-7].

(3) WSPÓŁPRACUJĄCE URZĄDZENIA KOMPUTEROWE | DEZAKTYWACJA / USUWANIE W CHRONIONYCH OBSZARACH PRACY

Organizacja dezaktywuje lub usuwa współpracujące urządzenia komputerowe z [*Realizacja: zdefiniowane przez organizację systemy teleinformatyczne lub elementy systemu teleinformatycznego*] w [*Realizacja: zdefiniowane przez organizację bezpieczne obszary pracy*].

(4) WSPÓŁPRACUJĄCE URZĄDZENIA KOMPUTEROWE | WYRAŹNIE WYKAZANIE AKTUALNYCH UŻYTKOWNIKÓW

System teleinformatyczny zapewnia wyraźne wskazanie aktualnych uczestników [*Realizacja: zdefiniowane przez organizację spotkania online i telekonferencje*].

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	SC-15	SC-15	SC-15

SC-16 TRANSMISJA ATRYBUTÓW BEZPIECZEŃSTWA

Zabezpieczenie: System teleinformatyczny kojarzy *[Realizacja: atrybuty bezpieczeństwa zdefiniowane przez organizację*] z informacjami wymienianymi między systemami teleinformatycznymi i między komponentami systemu.

Zabezpieczenia powiązane: AC-3, AC-4, AC-16.

Zabezpieczenia rozszerzone:

(1) PRZEKAZYWANIE ATRYBUTÓW BEZPIECZEŃSTWA | OCENA INTEGRALNOŚCI

System teleinformatyczny sprawdza integralność transmitowanych atrybutów bezpieczeństwa.

Zabezpieczenia powiązane: AU-10, SC-8.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P0	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	SC-16 (opcjonalnie)	SC-16 (opcjonalnie)	SC-16 (opcjonalnie)

SC-17 CERTYFIKATY INFRASTRUKTURY KLUCZA PUBLICZNEGO

Zabezpieczenie: Organizacja wydaje certyfikaty klucza publicznego w ramach [*Realizacja: polityka certyfikatów zdefiniowana przez organizację*] lub uzyskuje certyfikaty klucza publicznego od zatwierdzonego usługodawcy.

Zabezpieczenia powiązane: SC-12.

Zabezpieczenia rozszerzone: Brak.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	SC-17 (opcjonalnie)	SC-17	SC-17

SC-18 KOD MOBILNY

Zabezpieczenie: Organizacja:

a. Definiuje akceptowalny i niedopuszczalny kod mobilny i technologie kodów mobilnych;

b. Ustanawia ograniczenia użytkowania i wytyczne dotyczące implementacji akceptowalnego kodu mobilnego i technologii kodu mobilnego;

c. Autoryzuje, monitoruje i kontroluje użycie kodu mobilnego w systemie teleinformatycznym.

Zabezpieczenia powiązane: AU-2, AU-12, CM-2, CM-6, SI-3.

Zabezpieczenia rozszerzone:

(1) KOD MOBILNY | IDENTYFIKACJA NIEDOPUSZCZALNEGO KOD / PODEJMOWANIE DZIAŁAŃ NAPRAWCZYCH

System teleinformatyczny identyfikuje [*Realizacja: niedopuszczalny kod mobilny zdefiniowany przez organizację*] i podejmuje [*Realizacja: działania naprawcze zdefiniowane przez organizację*].

(2) KOD MOBILNY | NABYCIE / OPRACOWYWANIE / UŻYTKOWANIE

Organizacja zapewnia, że pozyskiwanie, opracowywanie i wykorzystywanie kodu mobilnego do wdrożenia w systemie teleinformatycznym spełnia [*Realizacja: wymagania dotyczące kodu mobilnego zdefiniowane przez organizację*].

(3) KOD MOBILNY | ZAPOBIEGANIE POBIERANIU / WYKONANIU

System teleinformatyczny zapobiega pobieraniu i wykonywaniu [*Realizacja: kod mobilny zdefiniowany przez organizację*].

(4) KOD MOBILNY | ZAPOBIEGANIE AUTOMATYCZNEMU WYKONANIU

System teleinformatyczny zapobiega automatycznemu wykonywaniu kodu mobilnego w [*Realizacja: aplikacje zdefiniowane przez organizację*] i egzekwuje [*Realizacja: działania zdefiniowane przez organizację]* przed wykonaniem kodu.

(5) KOD MOBILNY | POZWALANIE NA WYKONANIE TYLKO W OGRANICZONYCH ŚRODOWISKACH

Organizacja umożliwia wykonywanie dozwolonego kodu mobilnego tylko w ograniczonych środowiskach maszyn wirtualnych.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P2	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	SC-18 (opcjonalnie)	SC-18	SC-18

SC-19 PROTOKÓŁ TRANSMISJI PAKIETOWEJ (VoIP)

Zabezpieczenie: Organizacja:

a. Ustanawia zasady użycia i wytyczne dotyczące implementacji technologii pakietowej VoIP (Voice over Internet Protocol) w systemie teleinformatycznym, uwzględniając potencjalne uszkodzenie systemu teleinformatycznego w przypadku złośliwego użycia;

b. Autoryzuje, monitoruje i kontroluje korzystanie z transmisji VoIP w systemie teleinformatycznym.

Zabezpieczenia powiązane: CM-6, SC-7, SC-15.

Zabezpieczenia rozszerzone: Brak.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	SC-19 (opcjonalnie)	SC-19	SC-19

SC-20 BEZPIECZEŃSTWO NAZW DOMEN / ADRESÓW IP (AUTENTYCZNOŚĆ POCHODZENIA)

Zabezpieczenie: System teleinformatyczny:

a. Zapewnia dodatkowe artefakty uwierzytelniania i weryfikacji pochodzenia danych oraz wiarygodne dane rozpoznawania nazw, które system zwraca w odpowiedzi na zapytania dotyczące rozpoznawania nazw / adresów zewnętrznych;

b. Zapewnia środki do wskazywania statusu bezpieczeństwa stref podrzędnych i (jeśli ta podrzędna strefa zapewnia obsługę środków bezpieczeństwa) w celu umożliwienia weryfikacji łańcucha zaufania między domenami nadrzędnymi i podrzędnymi, w przypadku gdy działają one w ramach rozproszonej, hierarchicznej przestrzeni nazw.

Zabezpieczenia powiązane: AU-10, SC-8, SC-12, SC-13, SC-21, SC-22.

Zabezpieczenia rozszerzone:

(1) BEZPIECZEŃSTWO NAZW DOMEN / ADRESÓW (AUTENTYCZNOŚĆ POCHODZENIA) | STREFA PODRZĘDNA (PODPRZESTRZEŃ)

[Włączony do SC-20].

(2) BEZPIECZEŃSTWO NAZW DOMEN / ADRESÓW (AUTENTYCZNOŚĆ POCHODZENIA) | INTEGRALNOŚĆ DANYCH

System teleinformatyczny zapewnia artefakty ochrony pochodzenia i integralności danych wewnętrznych zapytań dotyczących rozpoznawania nazw / adresów.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	SC-20	SC-20	SC-20

SC-21 BEZPIECZEŃSTWO NAZW DOMEN / USŁUGA USTALANIA ADRESU IP

Zabezpieczenie: System teleinformatyczny żąda i przeprowadza uwierzytelnianie źródła danych oraz weryfikację integralności danych w odpowiedziach na rozpoznanie nazwy / adresu otrzymanych przez system z wiarygodnych źródeł.

Zabezpieczenia powiązane: SC-20, SC-22.

Zabezpieczenia rozszerzone: Brak.

(1) BEZPIECZEŃSTWO NAZW DOMEN / USŁUGA USTALANIA ADRESU IP | INTEGRALNOŚĆ

[Włączone do SC-21].

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	SC-21	SC-21	SC-21

SC-22 ARCHITEKTURA NAZW DOMEN / ADRESÓW IP / ZAMAWIANIE USŁUGI DNS

Zabezpieczenie: Systemy teleinformatyczne, które łącznie zapewniają organizacji usługę rozpoznawania nazw / adresów, są odporne na błędy i wdrażają wewnętrzne / zewnętrzne rozdzielenie ról.

Zabezpieczenia powiązane: SC-2, SC-20, SC-21, SC-24.

Zabezpieczenia rozszerzone: Brak.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	SC-22	SC-22	SC-22

SC-23 AUTENTYCZNOŚĆ SESJI

Zabezpieczenie: System teleinformatyczny chroni autentyczność sesji komunikacyjnych.

Zabezpieczenia powiązane: SC-8, SC-10, SC-11.

Zabezpieczenia rozszerzone:

(1) AUTENTYCZNOŚĆ SESJI | UNIEWAŻNIENIE IDENTYFIKATORÓW SESJI PO WYLOGOWANIU

System teleinformatyczny unieważnia identyfikatory sesji po wylogowaniu użytkownika lub innym zakończeniu sesji.

(2) AUTENTYCZNOŚĆ SESJI | WYLOGOWANIE INICJOWANE PRZEZ UŻYTKOWNIKA / WYŚWIETLANIE WIADOMOŚCI

[Włączone do AC-12 (1)].

(3) AUTENTYCZNOŚĆ SESJI | LOSOWE UNIKALNE IDENTYFIKATORY SESJI

System teleinformatyczny generuje unikalny identyfikator sesji dla każdej sesji za pomocą [*Realizacja: wymagania dotyczące losowości zdefiniowane przez organizację*] i rozpoznaje identyfikatory sesji wygenerowane wyłącznie przez ten system.

Zabezpieczenia powiązane: SC-13.

(4) AUTENTYCZNOŚĆ SESJI | LOSOWE UNIKALNE IDENTYFIKATORY SESJI

[Włączono do SC-23 (3)].

(5) AUTENTYCZNOŚĆ SESJI | AUTORYZOWANE URZĘDY CERTYFIKACYJNE

System teleinformatyczny pozwala jedynie na użycie [*Realizacja: urzędy certyfikacji zdefiniowane przez organizację*] do weryfikacji ustanowienia chronionych sesji[52].

Zabezpieczenia powiązane: SC-13.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	SC-23 (opcjonalnie)	SC-23	SC-23

SC-24 PRZEJŚCIE DO OKREŚLONEGO STANU SYSTEMU PO BŁĘDZIE

Zabezpieczenie: System teleinformatyczny przechodzi do stanu bezpiecznego (po błędzie) [*Realizacja: znany stan zdefiniowany przez organizację*] w odniesieniu do [*Realizacja: typy błędów zdefiniowane przez organizację*] zachowując [*Realizacja: informacje o stanie systemu[53] zdefiniowane przez organizację*] w przypadku niepowodzenia.

Zabezpieczenia powiązane: CP-2, CP-10, CP-12, SC-7, SC-22.

Zabezpieczenia rozszerzone: Brak.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	SC-24 (opcjonalnie)	SC-24 (opcjonalnie)	SC-24

[52] Ustanowienia bezpiecznych sesji obejmuje, np. użycie certyfikatów Secure Socket Layer (SSL) i / lub Transport Layer Security (TLS).

[53] Zachowanie informacji o stanie systemu informacji ułatwia ponowne uruchomienie systemu i powrót do trybu operacyjnego organizacji przy mniejszym zakłóceniu procesów misji / biznesowych.

SC-25 THIN NODES / TERMINALOWE STACJE ROBOCZE

Zabezpieczenie: Organizacja stosuje [*Realizacja: komponenty systemu teleinformatycznego zdefiniowane przez organizację*] o ograniczonej funkcjonalności i pojemności[54].

Zabezpieczenia powiązane: SC-30.

Zabezpieczenia rozszerzone: Brak.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P0	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	SC-25 (opcjonalnie)	SC-25 (opcjonalnie)	SC-25 (opcjonalnie)

SC-26 HONEYPOTS

Zabezpieczenie: System teleinformatyczny zawiera komponenty specjalnie zaprojektowane jako cel złośliwych ataków, w celu wykrywania, odbijania i analizowania takich ataków. Honeypot jest ustanowiony jako wabik, aby zwrócić uwagę przeciwników i odwrócić ich ataki od systemów operacyjnych wspierających misje organizacyjne / funkcje biznesowe.

Zabezpieczenia powiązane: SC-30, SC-44, SI-3, SI-4.

Zabezpieczenia rozszerzone: Brak.

(1) HONEYPOTS | WYKRYWANIE ZŁEGO KODU

[Włączono do SC-35].

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P0	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	SC-26 (opcjonalnie)	SC-26 (opcjonalnie)	SC-26 (opcjonalnie)

[54] Np. terminale bezdyskowe i technologie cienkiego klienta (Thin Client).

SC-27 WIELOPLATFORMOWOŚĆ APLIKACJI

Zabezpieczenie: System teleinformatyczny obejmuje: [*Realizacja: zdefiniowane przez organizację aplikacje niezależne od platformy*[55]].

Zabezpieczenia powiązane: SC-29.

Zabezpieczenia rozszerzone: Brak.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P0	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	SC-27 (opcjonalnie)	SC-27 (opcjonalnie)	SC-27 (opcjonalnie)

SC-28 OCHRONA DANYCH W SKŁADOWANIU / KOPIE KONFIGURACJI SYSTEMU

Zabezpieczenie: System teleinformatyczny chroni [*Wybór (jeden lub więcej): poufność; integralność*] [*Realizacja: informacje zdefiniowane przez organizację w spoczynku*[56]].

Zabezpieczenia powiązane: AC-3, AC-6, CA-7, CM-3, CM-5, CM-6, PE-3, SC-8, SC-13, SI-3, SI-7.

Zabezpieczenia rozszerzone:

(1) OCHRONA DANYCH W SKŁADOWANIU / KOPIE KONFIGURACJI SYSTEMU | OCHRONA KRYPTOGRAFICZNA

System teleinformatyczny implementuje mechanizmy kryptograficzne mające za zadanie zapobieganie nieuprawnionemu ujawnieniu i modyfikacji [*Realizacja: informacje zdefiniowane przez organizację*] w [*Realizacja: elementy systemu teleinformatycznego zdefiniowane przez organizację*].

Zabezpieczenia powiązane: AC-19, SC-12.

[55] Platformy są kombinacjami sprzętu i oprogramowania używanego do uruchamiania aplikacji. Platformy obejmują: systemy operacyjne, podstawowe architektury komputerów lub oba. Aplikacje niezależne od platformy, to aplikacje działające na wielu platformach.

[56] Informacje w spoczynku to dane nieaktywne, fizycznie przechowywane w bazach danych, magazynach danych, arkuszach obliczeniowych, archiwach, kasetach, kopiach zapasowych poza miejscem przetwarzania (kopie off-site), itp. Informacje związane z systemem wymagające ochrony obejmują na przykład konfiguracje lub zestawy reguł odnoszących się do zapór ogniowych, bram, systemów wykrywania / zapobiegania włamaniom, routerów filtrujących i treści uwierzytelniających.

(2) OCHRONA DANYCH W SKŁADOWANIU / KOPIE KONFIGURACJI SYSTEMU | PRZECHOWYWANIE OFF-LINE

Organizacja usuwa z pamięci online i przechowuje off-line w bezpiecznej lokalizacji [*Realizacja: informacje zdefiniowane przez organizację*].

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	SC-28 (opcjonalnie)	SC-28	SC-28

SC-29 HETEROGENICZNOŚĆ SYSTEMU

Zabezpieczenie: Organizacja przy wdrażaniu systemu teleinformatycznego stosuje różnorodny zbiór technologii teleinformatycznych do [*Realizacja: komponenty systemu teleinformatycznego zdefiniowane przez organizację*] .

Zabezpieczenia powiązane: SA-12, SA-14, SC-27.

Zabezpieczenia rozszerzone:

(2) HETEROGENICZNOŚĆ | TECHNIKI WIRTUALIZACJI

Organizacja stosuje techniki wirtualizacji wspierające wdrażanie różnorodnych systemów operacyjnych i aplikacji, które są zmieniane z częstotliwością [*Realizacja: częstotliwość zdefiniowana przez organizację*].

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P0	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	SC-29 (opcjonalnie)	SC-29 (opcjonalnie)	SC-29 (opcjonalnie)

SC-30 MASKOWANIE I DEZINFORMACJA

Zabezpieczenie: Celem zmylenia i wprowadzenia w błąd przeciwników, organizacja stosuje *[Realizacja: zdefiniowane przez organizację techniki maskowania i dezinformacji*] w [*Realizacja: systemy informacyjne zdefiniowane przez organizację*] w okresie [*Realizacja: okresy zdefiniowane przez organizację*].

Zabezpieczenia powiązane: SC-26, SC-29, SI-14.

Zabezpieczenia rozszerzone:

(1) MASKOWANIE I DEZINFORMACJA | TECHNIKI WIRTUALIZACJI

[Włączono do SC-29 (1)].

(2) MASKOWANIE I DEZINFORMACJA | LOSOWOŚĆ

Organizacja stosuje [*Realizacja: techniki wprowadzające w błąd*[57] *zdefiniowane przez organizację*] w celu wprowadzenia losowości w operacjach i zasobach organizacyjnych.

(3) MASKOWANIE I DEZINFORMACJA | ZMIANA LOKALIZACJI PRZETWARZANIA / PRZECHOWYWANIA

Organizacja zmienia lokalizację [*Realizacja: przetwarzanie i / lub przechowywanie zdefiniowane przez organizację*] z częstotliwością [Realizacja: [*Realizacja: częstotliwość czasowa zdefiniowana przez organizację] ; w losowych odstępach czasu*]].

(4) MASKOWANIE I DEZINFORMACJA | INFORMACJE DEZINFORMUJĄCE

Organizacja stosuje realistyczne, ale wprowadzające w błąd informacje dezinformujące[58] w [*Realizacja: elementy systemu teleinformatycznego zdefiniowane przez organizację*] w odniesieniu do zakresu środków bezpieczeństwa stosowanych przez organizacje.

(5) MASKOWANIE I DEZINFORMACJA | UKRYWANIE KOMPONENTÓW SYSTEMU

Organizacja stosuje [*Realizacja: techniki zdefiniowane przez organizację*] do ukrywania lub zmieniania[59] [*Realizacja: komponenty systemu teleinformatycznego zdefiniowane przez organizację*].

[57] Losowe techniki wprowadzające w błąd obejmują np. wykonywanie określonych rutynowych czynności o różnych porach dnia, stosowanie różnych technologii teleinformatycznych (np. przeglądarek, wyszukiwarek), korzystanie z różnych dostawców oraz zmienianie ról i obowiązków personelu organizacyjnego.

[58] Np. umieszczanie przez organizacje wprowadzających w błąd informacji dotyczących konkretnych środków bezpieczeństwa wdrożonych w zewnętrznych systemach teleinformatycznych. Inną techniką jest stosowanie sieci dezinformujących (np. Honeynetów, środowisk zwirtualizowanych), które naśladują rzeczywiste aspekty systemów teleinformatycznych organizacji, ale wykorzystują na przykład nieaktualne konfiguracje oprogramowania.

[59] Np. konfiguracja routerów lub wykorzystanie technologii honeynet lub technik wirtualizacji.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P0	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	SC-30 (opcjonalnie)	SC-30 (opcjonalnie)	SC-30 (opcjonalnie)

SC-31 ANALIZA UKRYTEGO KANAŁU KOMUNIKACJI

Zabezpieczenie: Organizacja:

a. Przeprowadza analizę kanału ukrytego w celu zidentyfikowania tych aspektów komunikacji w systemie teleinformatycznym, które są potencjalnymi trasami ukrytych kanałów np. [*Wybór (jeden lub więcej): przechowywanie; synchronizacja*];

b. Szacuje maksymalną przepustowość tych kanałów.

Zabezpieczenia powiązane: AC-3, AC-4, PL-2.

Zabezpieczenia rozszerzone:

(1) ANALIZA UKRYTEGO KANAŁU KOMUNIKACJI | TESTOWANIE KANAŁÓW UKRYTYCH

Organizacja testuje podzbiór zidentyfikowanych ukrytych kanałów możliwych do prowadzenia wyzyskiwania.

(2) ANALIZA UKRYTEGO KANAŁU KOMUNIKACJI | MAKSYMALNA PRZEPUSTOWOŚĆ ŁĄCZA

Organizacja zmniejsza maksymalną przepustowość łącza w odniesieniu do zidentyfikowanych ukrytych kanałów [*Wybór (jeden lub więcej); przechowywanie; synchronizacja*] do [*Realizacja: wartość przepustowości zdefiniowana przez organizację*].

(3) ANALIZA UKRYTEGO KANAŁU KOMUNIKACJI | POMIAR PRZEPUSTOWOŚCI W ŚRODOWISKU OPERACYJNYM

Organizacja mierzy pasmo ukrytych kanałów [*Realizacja: zdefiniowany przez organizację podzbiór zidentyfikowanych ukrytych kanałów*] w środowisku operacyjnym systemu teleinformatycznego.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P0	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	SC-31 (opcjonalnie)	SC-31 (opcjonalnie)	SC-31 (opcjonalnie)

SC-32 DZIELENIE SYSTEMU TELEINFORMATYCZNEGO NA PARTYCJE

Zabezpieczenie: Organizacja dzieli system teleinformatyczny na [*Realizacja: komponenty systemu teleinformatycznego zdefiniowane przez organizację*[60]] rezydujące w oddzielnych domenach fizycznych lub środowiskach w oparciu o [*Realizacja: zdefiniowane przez organizację okoliczności dotyczące fizycznego oddzielenia komponentów*].

Zabezpieczenia powiązane: AC-4, SA-8, SC-2, SC-3, SC-7.

Zabezpieczenia rozszerzone: Brak.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P0	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	SC-32 (opcjonalnie)	SC-32 (opcjonalnie)	SC-32 (opcjonalnie)

SC-33 INTEGRALNOŚĆ TRANSMISJI

[Włączony do SC-8].

[60] Zarządzane interfejsy ograniczają lub zabraniają dostępu do sieci i przepływu informacji między komponentami systemu teleinformatycznego podzielonymi na partycje.

SC-34 NIEMODYFIKOWALNE PROGRAMY WYKONYWALNE

Zabezpieczenie: System teleinformatyczny w komponentach [*Realizacja: komponenty systemu teleinformatycznego zdefiniowane przez organizację*]:

a. Ładuje i wykonuje środowisko operacyjne z wdrożonego do używania nośnika tylko do odczytu;

b. Ładuje i wykonuje aplikacje [*Realizacja: aplikacje zdefiniowane przez organizację*] z wdrożonego do używania nośnika tylko do odczytu.

Zabezpieczenia powiązane: AC-3, SI-7.

Zabezpieczenia rozszerzone:

(1) NIEMODYFIKOWALNE PROGRAMY WYKONYWALNE | NIEZAPISYWALNE PAMIĘCI

Organizacja stosuje [*Realizacja: komponenty systemu teleinformatycznego zdefiniowane przez organizację*] z niezapisywalnymi pamięciami, których zawartość pozostaje niezmienna po ponownym uruchomieniu komponentu lub włączeniu / wyłączeniu zasilania.

Zabezpieczenia powiązane: AC-19, MP-7.

(2) NIEMODYFIKOWALNE PROGRAMY WYKONYWALNE | OCHRONA INTEGRALNOŚCI / MEDIA TYLKO DO ODCZYTU

Organizacja chroni integralność informacji przechowywanej na nośniku tylko do odczytu i zabezpiecza nośnik po zapisaniu takich informacji na nośniku.

Zabezpieczenia powiązane: AC-5, CM-3, CM-5, CM-9, MP-2, MP-4, MP-5, SA-12, SC-28, SI-3.

(3) NIEMODYFIKOWALNE PROGRAMY WYKONYWALNE | OCHRONA SPRZĘTOWA

Organizacja:

(a) Stosuje sprzętową ochronę przed zapisem w oprogramowaniu układowym (firmware) [*Realizacja: elementy oprogramowania układowego systemu teleinformatycznego zdefiniowane przez organizację*];

(b) Wprowadza określone procedury dla personelu [*Realizacja: osoby upoważnione zdefiniowane przez organizację*], umożliwiające ręczne wyłączanie sprzętowej ochrony przed zapisem w przypadku modyfikacji oprogramowania układowego i ponowne włączanie ochrony przed zapisem przed powrotem systemu do trybu operacyjnego.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P0	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	SC-34 (opcjonalnie)	SC-34 (opcjonalnie)	SC-34 (opcjonalnie)

SC-35 HONEYCLIENTS[61]

Zabezpieczenie: System teleinformatyczny zawiera komponenty mające na celu świadomą identyfikację złośliwych stron internetowych i / lub złośliwy kod internetowy.

Honeyclients różnią się od honeypots tym, że komponenty aktywnie badają Internet w poszukiwaniu złośliwego kodu (np. robaków) zawartego na zewnętrznych stronach internetowych. Podobnie jak w przypadku honeypotów, honeyclient wymagają pewnych pomocniczych środków izolacji (np. wirtualizacji), aby upewnić się, że każdy złośliwy kod wykryty podczas wyszukiwania, a następnie wykonany nie infekuje systemów teleinformatycznych organizacji.

Zabezpieczenia powiązane: SC-26, SC-44, SI-3, SI-4.

Zabezpieczenia rozszerzone: Brak.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P0	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	SC-35 (opcjonalnie)	SC-35 (opcjonalnie)	SC-35 (opcjonalnie)

SC-36 PRZETWARZANIE I PRZECHOWYWANIE ROZPROSZONE

Zabezpieczenie: Organizacja przeprowadza [*Realizacja: przetwarzanie i przechowywanie informacji zdefiniowane przez organizację*] w wielu fizycznych lokalizacjach.

Zabezpieczenia powiązane: CP-6, CP-7.

Zabezpieczenia rozszerzone:

(2) PRZETWARZANIE I PRZECHOWYWANIE ROZPROSZONE | TECHNIKI PRZEGLĄDANIA CYKLICZNEGO

Organizacja stosuje techniki cyklicznego przeglądania w celu identyfikacji potencjalnych wad, błędów lub naruszeń w [*Realizacja: zdefiniowane przez organizację rozproszone komponenty przetwarzania i przechowywania*].

[61] Honeyclient różni się od honeypot tym, że komponenty honyclient proaktywnie badają Internet w poszukiwaniu złośliwego kodu (np. robaków) zawartego na zewnętrznych stronach internetowych.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P0	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	SC-36 (opcjonalnie)	SC-36 (opcjonalnie)	SC-36 (opcjonalnie)

SC-37 KANAŁY POZAPASMOWE

Zabezpieczenie: Organizacja stosuje [*Realizacja: organizacyjnie zdefiniowane kanały poza pasmem*[62]] do fizycznej dostawy lub elektronicznego przesyłu [*Realizacja: informacje o organizacji*[63]*, komponenty systemu teleinformatycznego, lub urządzenia*] do [*Realizacja: organizacyjne określone jednostki lub systemy informacyjne*].

Zabezpieczenia powiązane: AC-2, CM-3, CM-5, CM-7, IA-4, IA-5, MA-4, SC-12, SI-3, SI-4, SI-7.

Zabezpieczenia rozszerzone:

(1) KANAŁY POZAPASMOWE | GWARANTOWANA DOSTAWA / TRANSMISJA

Organizacja stosuje [*Realizacja: środki bezpieczeństwa zdefiniowane przez organizację*] w celu zapewnienia otrzymywania informacji [*Realizacja: informacje zdefiniowane przez organizację, elementy systemu teleinformatycznego lub urządzenia*] tylko i wyłącznie przez [*Realizacja: osoby lub systemy informacyjne zdefiniowane przez organizację*].

[62] Kanały pozapasmowe obejmują np. dostęp lokalny (RS, USB, itp.) do systemów teleinformatycznych, ścieżki sieciowe fizycznie oddzielone od ścieżek sieciowych wykorzystywanych do ruchu operacyjnego lub ścieżki nieelektroniczne (serwisy pocztowe).

[63] Kanały pozapasmowe mogą być wykorzystywane do dostarczania lub przesyłania wiadomości organizacyjnych takich jak: identyfikatory / uwierzytelniacze, zmiany zarządzania konfiguracją sprzętu, oprogramowanie układowe lub aplikacje, informacje o zarządzaniu kluczami kryptograficznymi, aktualizacje zabezpieczeń, kopie zapasowe systemu / danych , informacje o konserwacji oraz aktualizacje ochrony przed złośliwym kodem.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P0	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	SC-37 (opcjonalnie)	SC-37 (opcjonalnie)	SC-37 (opcjonalnie)

SC-38 BEZPIECZEŃSTWO OPERACJI

Zabezpieczenie: Organizacja stosuje [*Realizacja: środki bezpieczeństwa operacji zdefiniowane przez organizację*] w celu ochrony kluczowych informacji organizacyjnych w całym cyklu rozwoju systemu.

Zabezpieczenia powiązane: RA-2, RA-5, SA-12.

Zabezpieczenia rozszerzone: Brak.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P0	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	SC-38 (opcjonalnie)	SC-38 (opcjonalnie)	SC-38 (opcjonalnie)

SC-39 IZOLACJA PROCESÓW

Zabezpieczenie: System teleinformatyczny utrzymuje osobną domenę wykonawczą dla każdego procesu wykonawczego.

Zabezpieczenia powiązane: AC-3, AC-4, AC-6, SA-4, SA-5, SA-8, SC-2, SC-3.

Zabezpieczenia rozszerzone:

(1) IZOLACJA PROCESÓW | SEPARACJA SPRZĘTOWA

System teleinformatyczny wprowadza podstawowe mechanizmy separacji sprzętowej, aby ułatwić separację procesów.

(2) IZOLACJA PROCESÓW | IZOLACJA WĄTKÓW

System teleinformatyczny utrzymuje osobną domenę wykonawczą dla każdego wątku w [*Realizacja: przetwarzanie wielowątkowe zdefiniowane przez organizację*].

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	SC-39	SC-39	SC-39

SC-40 OCHRONA ŁĄCZA BEZPRZEWODOWEGO

Zabezpieczenie: System teleinformatyczny chroni zewnętrzne i wewnętrzne [*Realizacja: zdefiniowane przez organizację łącza bezprzewodowe*] przed [*Realizacja: zdefiniowane przez organizację typy parametrów atakowanych sygnałów lub odniesienia do źródeł takich ataków*].

Zabezpieczenia powiązane: AC-18, SC-5.

Zabezpieczenia rozszerzone:

(1) OCHRONA POŁĄCZENIA BEZPRZEWODOWEGO | INTERFERENCJA ELEKTROMAGNETYCZNA

System teleinformatyczny wdraża mechanizmy kryptograficzne, które osiągają [*Realizacja: poziom ochrony zdefiniowany przez organizację*] przed skutkami zamierzonych zakłóceń elektromagnetycznych.

Zabezpieczenia powiązane: SC-12, SC-13.

(2) OCHRONA ŁĄCZA BEZPRZEWODOWEGO | REDUKCJA POTENCJALNEJ DETEKCJI

System teleinformatyczny wdraża mechanizmy kryptograficzne w celu zmniejszenia potencjału wykrywania połączeń bezprzewodowych z [*Realizacja: poziom redukcji*[64] *zdefiniowany przez organizację*].

Zabezpieczenia powiązane: SC-12, SC-13.

(3) OCHRONA ŁĄCZA BEZPRZEWODOWEGO | NAŚLADOWCZE LUB MANIPULACYJNE OSZUSTWO TELEKOMUNIKACYJNE

System teleinformatyczny implementuje mechanizmy kryptograficzne do identyfikowania i odrzucania transmisji bezprzewodowych, które są celowymi próbami uwierzytelnienia oszustwa opartego na naśladownictwie lub manipulacji parametrami sygnału.

Zabezpieczenia powiązane: SC-12, SC-13.

(4) OCHRONA ŁĄCZA BEZPRZEWODOWEGO | IDENTYFIKACJA PARAMETRÓW SYGNAŁU

System teleinformatyczny implementuje mechanizmy kryptograficzne, aby zapobiec identyfikacji [*Realizacja: nadajniki bezprzewodowe zdefiniowane przez organizację*] za pomocą parametrów sygnału nadajnika.

Zabezpieczenia powiązane: SC-12, SC-13.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P0	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	SC-40 (opcjonalnie)	SC-40 (opcjonalnie)	SC-40 (opcjonalnie)

SC-41 DOSTĘP DO PORTÓW I URZĄDZEŃ WEJŚCIA / WYJŚCIA

Zabezpieczenie: Organizacja fizycznie wyłącza lub usuwa [*Realizacja: zdefiniowane przez organizację połączenia portów lub urządzeń wejścia / wyjścia*] w [*Realizacja: zdefiniowane przez organizację systemy informacyjne lub elementy systemu teleinformatycznego*].

Zabezpieczenia rozszerzone: Brak.

[64] Wymagania dotyczące misji, przewidywane zagrożenia, koncepcja operacji oraz obowiązujące przepisy, dyrektywy, regulacje, zasady, standardy i wytyczne określają poziomy, na których łącza bezprzewodowe powinny być niewykrywalne.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P0	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	SC-41 (opcjonalnie)	SC-41 (opcjonalnie)	SC-41 (opcjonalnie)

SC-42 CZUJNIKI

Zabezpieczenie: System teleinformatyczny:

a. Zabrania zdalnej aktywacji funkcji wykrywania otoczenia z następującymi wyjątkami: [*Realizacja: wyjątki zdefiniowane przez organizację, w których dozwolona jest zdalna aktywacja czujników*];

b. Zapewnia wyraźne wskazanie użycia czujnika[65] przez [*Realizacja: klasa użytkowników zdefiniowana przez organizację*].

Zabezpieczenia rozszerzone:

(1) CZUJNIKI | RAPORTOWANIE DO UPOWAŻNIONYCH OSÓB LUB RÓL

Organizacja zapewnia skonfigurowanie systemu teleinformatycznego w sposób umożliwiający gromadzenie danych lub informacji przez [*Realizacja: czujniki zdefiniowane przez organizację*] i zgłaszanie tych danych tylko upoważnionym osobom lub rolom.

(2) CZUJNIKI | AUTORYZOWANE UŻYCIE

Organizacja stosuje następujące środki: [*Realizacja: środki zdefiniowane przez organizację*], dzięki czemu dane lub informacje zebrane przez [*Realizacja: czujniki zdefiniowane przez organizację*] są wykorzystywane wyłącznie do celów autoryzowanych.

(3) CZUJNIKI | ZABRONIONE WYKORZYSTANIE URZĄDZEŃ

Organizacja zabrania używania urządzeń posiadających [*Realizacja: zdefiniowane przez organizację możliwości detekcji otoczenia*] w [*Realizacja: obiekty, obszary lub systemy zdefiniowane przez organizację*].

[65] Czujniki wbudowane w urządzenia mobilne obejmują na przykład kamery, mikrofony, mechanizmy globalnego systemu pozycjonowania (GPS) i akcelerometry.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P0	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	SC-42 (opcjonalnie)	SC-42 (opcjonalnie)	SC-42 (opcjonalnie)

SC-43 OGRANICZENIA UŻYCIA

Zabezpieczenie: Organizacja:

a. Ustanawia ograniczenia użytkowania i wskazówki dotyczące implementacji [*Realizacja: komponenty systemu teleinformatycznego*[66] *zdefiniowane przez organizację*] w oparciu o możliwość spowodowania uszkodzenia systemu teleinformatycznego użytego w sposób złośliwy;

b. Autoryzuje, monitoruje i kontroluje użycie takich komponentów w systemie teleinformatycznym.

Zabezpieczenia powiązane: CM-6, SC-7.

Zabezpieczenia rozszerzone: Brak.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P0	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	SC-43 (opcjonalnie)	SC-43 (opcjonalnie)	SC-43 (opcjonalnie)

[66] Komponenty systemu teleinformatycznego obejmują sprzęt, oprogramowanie lub komponenty oprogramowania układowego (np. Voice over Internet Protocol, kod mobilny, kopiarki cyfrowe, drukarki, skanery, urządzenia optyczne, technologie bezprzewodowe, urządzenia mobilne).

SC-44 KOMORY DETONACYJNE

Zabezpieczenie: Organizacja wykorzystuje funkcję komory detonacyjnej w [*Realizacja: system teleinformatyczny zdefiniowany przez organizację, komponent systemu lub lokalizacja*] .

Zabezpieczenia powiązane: SC-7, SC-25, SC-26, SC-30.

Zabezpieczenia rozszerzone: Brak.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P0	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	SC-44 (opcjonalnie)	SC-44 (opcjonalnie)	SC-44 (opcjonalnie)

KATEGORIA: INTEGRALNOŚĆ SYSTEMU I INFORMACJI

SI-1 POLITYKA I PROCEDURY INTEGRALNOŚCI SYSTEMU I INFORMACJI

Zabezpieczenie: Organizacja:

a. Opracowuje, dokumentuje i rozpowszechnia w odniesieniu do [*Realizacja: personel lub role zdefiniowane przez organizację*]:

   1. Politykę integralności systemu i informacji, która dotyczy celu, zakresu, ról, obowiązków, zaangażowania kierownictwa, koordynacji między jednostkami organizacyjnymi i spójności działania;

   2. Procedury ułatwiające wdrożenie polityki integralności systemu i informacji oraz powiązanych zabezpieczeń integralności systemu i informacji;

b. Recenzuje i aktualizuje aktualną:

   1. Politykę integralności systemu i informacji z częstotliwością [*Realizacja: częstotliwość określona przez organizację*];

   2. Procedury dotyczące integralności systemu i informacji z częstotliwością [*Realizacja: częstotliwość określona przez organizację*].

Zabezpieczenia powiązane: PM-9.

Zabezpieczenia rozszerzone: Brak.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	SI-1	SI-1	SI-1

SI-2 USUWANIE USTEREK

Zabezpieczenie: Organizacja:

a. Identyfikuje, zgłasza i koryguje niedoskonałości systemu teleinformatycznego;

b. Testuje, przed instalacją, aktualizacje aplikacji i oprogramowania układowego związane z usuwaniem usterek pod kątem skuteczności i potencjalnych skutków ubocznych;

c. Instaluje oprogramowanie i aktualizacje oprogramowania związane z bezpieczeństwem w ciągu [*Realizacja: okres zdefiniowany przez organizację]* od wydania aktualizacji;

d. Włącza usuwanie wad oprogramowania w proces zarządzania konfiguracją organizacji.

Zabezpieczenia powiązane: CA-2, CA-7, CM-3, CM-5, CM-8, MA-2, IR-4, RA-5, SA-10, SA-11, SI-11.

Zabezpieczenia rozszerzone:

(1) USUWANIE USTEREK | ZARZĄDZANIE CENTRALNE

Organizacja centralnie zarządza[67] procesem usuwania usterek.

(2) USUWANIE USTEREK | ZAUTOMATYZOWANE USUWANIA USTEREK

Organizacja stosuje zautomatyzowane mechanizmy określające z częstotliwością [*Realizacja: częstotliwość zdefiniowana przez organizację*] stan elementów systemu teleinformatycznego w zakresie usuwania wad.

Zabezpieczenia powiązane: CM-6, SI-4.

(3) USUWANIE USTEREK | CZAS DO USUNIĘCIA USTERKI / STANDARDY DZIAŁAŃ NAPRAWCZYCH

Organizacja:

(a) Mierzy czas między identyfikacją i usunięciem usterki;

(b) Ustanawia [*Realizacja: standardy zdefiniowane przez organizację*] w celu podjęcia działań naprawczych.

(4) USUWANIE USTEREK | AUTOMATYCZNE ŚCIEŻKI ZARZĄDZANIA NARZĘDZIAMI

[Włączono do SI-2].

(5) USUWANIE USTEREK | AUTOMATYCZNE AKTUALIZACJE APLIKACJI / OPROGRAMOWANIA UKŁADOWEGO

Organizacja instaluje automatycznie [*Realizacja: organizacyjnie zdefiniowane aktualizacje środków bezpieczeństwa aplikacji i oprogramowania układowego firmware*] w [*Realizacja: organizacyjne zdefiniowane komponenty systemu teleinformacyjnego*].

(6) USUWANIE USTEREK | USUWANIE POPRZEDNICH WERSJI APLIKACJI / OPROGRAMOWANIA UKŁADOWEGO

Organizacja usuwa [*Realizacja: aplikacje zdefiniowane przez organizację i składniki oprogramowania układowego*] po zainstalowaniu zaktualizowanych wersji.

[67] Centralne zarządzanie obejmuje planowanie, wdrażanie, ocenę, autoryzację i monitorowanie zdefiniowanych przez organizację zarządzanych środków bezpieczeństwa w zakresie usuwania wad / niedociągnięć systemu.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	SI-2	SI-2 (2)	SI-2 (1) (2)

SI-3 ZABEZPIECZENIE PRZED ZŁOŚLIWYM KODEM

Zabezpieczenie: Organizacja:

a. Wykorzystuje mechanizmy ochrony przed złośliwym kodem w punktach wejścia i wyjścia z systemu teleinformatycznego w celu wykrywania i eliminacji złośliwego kodu;

b. Aktualizuje mechanizmy ochrony przed złośliwym kodem, ilekroć dostępne są nowe wersje, zgodnie z zasadami i procedurami zarządzania konfiguracją organizacji;

c. Konfiguruje mechanizmy ochrony przed złośliwym kodem:

   1. Wykonując okresowe skanowanie systemu teleinformatycznego z częstotliwością [*Realizacja: częstotliwość zdefiniowana przez organizację*] oraz skanowanie plików w czasie rzeczywistym ze uzyskiwanych ze źródeł zewnętrznych w [*Wybór (jeden lub więcej); punkt końcowy; sieciowe punkty wejścia / wyjścia*] podczas pobierania, otwierania lub wykonywania plików zgodnie z zasadami bezpieczeństwa organizacji;

   2. [*Wybór (jeden lub więcej): blokuj złośliwy kod; poddaj kwarantannie złośliwy kod; wyślij alert do administratora}* w momencie *[Realizacja: działanie zdefiniowane przez organizację]*] w odpowiedzi na wykrycie złośliwego kodu;

d. Rozwiązuje problem otrzymywania fałszywych alarmów podczas wykrywania i usuwania złośliwego kodu oraz wynikającego z tego potencjalnego wpływu na dostępność systemu teleinformatycznego.

Zabezpieczenia powiązane: CM-3, MP-2, SA-4, SA-8, SA-12, SA-13, SC-7, SC-26, SC-44, SI-2, SI-4, SI-7.

Zabezpieczenia rozszerzone:

(1) ZABEZPIECZENIE PRZED ZŁOŚLIWYM KODEM | ZARZĄDZANIE CENTRALNE

Organizacja centralnie zarządza mechanizmami ochrony przed złośliwym kodem.

Zabezpieczenia powiązane: AU-2, SI-8.

(2) ZABEZPIECZENIE PRZED ZŁOŚLIWYM KODEM | AUTOMATYCZNE AKTUALIZACJE

System teleinformatyczny automatycznie aktualizuje mechanizmy ochrony przed złośliwym kodem.

Zabezpieczenia powiązane: SI-8.

(3) ZABEZPIECZENIE PRZED ZŁOŚLIWYM KODAMI | NIEUPRZYWILEJOWANI UŻYTKOWNICY

[Włączone do AC-6 (10)].

(4) ZABEZPIECZENIE PRZED ZŁOŚLIWYM KODEM | AKTUALIZACJE WYŁĄCZNIE PRZEZ UPRAWNIONYCH UŻYTKOWNIKÓW

System teleinformatyczny aktualizuje mechanizmy ochrony przed złośliwym kodem tylko na polecenie personelu wyznaczonego przez kierownika jednostki organizacyjnej.

Zabezpieczenia powiązane: AC-6, CM-5.

(5) ZABEZPIECZENIE PRZED ZŁOŚLIWYM KODEM | PRZENOŚNE URZĄDZENIA MAGAZYNUJĄCE

[Włączone do MP-7].

(6) ZABEZPIECZENIE PRZED ZŁOŚLIWYM KODEM | TESTOWANIE / WERYFIKACJA

Organizacja:

(a) Testuje mechanizmy ochrony przed złośliwym kodem z częstotliwością [*Realizacja: częstotliwość zdefiniowana przez organizację*] poprzez wprowadzenie znanego łagodnego, nierozprzestrzeniającego się przypadku testowego do systemu teleinformatycznego;

(b) Sprawdza, czy następuje zarówno wykrycie przypadku testowego, jak i związane z nim zgłoszenie incydentu.

Zabezpieczenia powiązane: CA-2, CA-7, RA-5.

(7) ZABEZPIECZENIE PRZED ZŁOŚLIWYM KODEM | WYKRYWANIE BEZSYGNATUROWE

System teleinformatyczny implementuje mechanizmy wykrywania złośliwego kodu w oparciu o bezsygnaturowe systemy wykrywania zaawansowanych ataków.

(8) ZABEZPIECZENIE PRZED ZŁOŚLIWYM KODEM | WYKRYWANIE NIEAUTORYZOWANYCH KOMEND

System teleinformatyczny wykrywa [*Realizacja: zdefiniowane przez organizację nieautoryzowane polecenia systemu operacyjnego*] za pośrednictwem interfejsu programowania aplikacji jądra w [*Realizacja: elementy sprzętowe systemu teleinformatycznego zdefiniowane przez organizację*] i [*Wybór (jeden lub więcej): wydaje ostrzeżenie; kontroluje wykonanie polecenia; zapobiega wykonaniu polecenia*].

Zabezpieczenia powiązane: AU-6.

(9) ZABEZPIECZENIE PRZED ZŁOŚLIWYM KODEM | ZDALNE POLECENIA AUTENTYFIKACYJNE

System teleinformatyczny implementuje [*Realizacja: środki bezpieczeństwa zdefiniowane przez organizację*] w celu uwierzytelnienia [*Realizacja: zdalne polecenia zdefiniowane przez organizację*].

Zabezpieczenia powiązane: SC-12, SC-13, SC-23.

(10) ZABEZPIECZENIE PRZED ZŁOŚLIWYM KODEM | ANALIZA KODU ZŁOŚLIWEGO

Organizacja:

(a) Wykorzystuje [*Realizacja: narzędzia i techniki zdefiniowane przez organizację*] do analizy cech i zachowania szkodliwego kodu;

(b) Włącza wyniki analizy złośliwego kodu do procesów reagowania na incydenty organizacyjne i usuwania wad.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	SI-3	SI-3 (1) (2)	SI-3 (1) (2)

SI-4 MONITOROWANIE SYSTEMU TELEINFORMATYCZNEGO

Zabezpieczenie: Organizacja:

a. Monitoruje system teleinformatyczny w celu wykrycia:

   1. Ataków i oznak potencjalnych ataków zgodnie z [*Realizacja: cele monitorowania określone przez organizację*];

   2. Nieautoryzowanych połączeń lokalnych, sieciowych i zdalnych;

b. Identyfikuje nieuprawnione korzystanie z systemu teleinformatycznego poprzez [*Realizacja: techniki i metody zdefiniowane przez organizację*];

c. Wdraża w systemach teleinformatycznych urządzenia monitorujące:

   1. Długofalowo, w celu gromadzenia istotnych informacji ustalonych przez organizację;

   2. W lokalizacjach doraźnych, w celu śledzenia określonych rodzajów transakcji będących przedmiotem zainteresowania organizacji;

d. Chroni informacje uzyskane z narzędzi do monitorowania włamań, przed nieautoryzowanym dostępem, modyfikacją i usunięciem;

e. Zwiększa poziom monitorowania systemu teleinformatycznego, ilekroć istnieje oznaka zwiększonego ryzyka operacji i aktywów organizacyjnych, osób, innych organizacji lub instytucji, w oparciu o informacje organów ścigania, dane wywiadowcze lub inne wiarygodne źródła informacji;

f. Uzyskuje opinie prawne dotyczące działań związanych z monitorowaniem systemu teleinformatycznego zgodnie z obowiązującymi przepisami, zarządzeniami wykonawczymi, dyrektywami, politykami lub przepisami;

g. Dostarcza [*Realizacja: informacje monitorowania systemu teleinformatycznego zdefiniowane przez organizację*] do [*Realizacja: personel lub role zdefiniowane przez organizację*] [*Wybór (jeden lub więcej): w razie potrzeby; z częstotliwością określoną przez organizację]*].

Zabezpieczenia powiązane: AC-3, AC-4, AC-8, AC-17, AU-2, AU-6, AU-7, AU-9, AU-12, CA-7, IR-4, PE-3 , RA-5, SC-7, SC-26, SC-35, SI-3, SI-7.

Zabezpieczenia rozszerzone:

(1) MONITOROWANIE SYSTEMU TELEINFORMATYCZNEGO | SYSTEMOWY WYKRYWANIA WŁAMAŃ

Organizacja łączy i konfiguruje poszczególne narzędzia wykrywania włamań w system wykrywania włamań, obejmujący cały system teleinformatyczny.

(2) MONITOROWANIE SYSTEMU TELEINFORMATYCZNEGO | AUTOMATYCZNE NARZĘDZIA ANALIZY W CZASIE RZECZYWISTYM

Organizacja wykorzystuje zautomatyzowane narzędzia do wspierania analizy zdarzeń w czasie zbliżonym do rzeczywistego.

(3) MONITOROWANIE SYSTEMU TELEINFORMATYCZNEGO | AUTOMATYCZNA INTEGRACJA NARZĘDZI

Organizacja wykorzystuje zautomatyzowane narzędzia do integracji narzędzi wykrywania włamań z mechanizmami kontroli dostępu i kontroli przepływu w celu szybkiego reagowania na ataki, umożliwiając rekonfigurację tych mechanizmów w celu wsparcia izolacji i eliminacji ataków.

(4) MONITOROWANIE SYSTEMU TELEINFORMATYCZNEGO | PRZYJŚCIOWY / WYJŚCIOWY RUCH TELEKOMUNIKACYJNY

System teleinformatyczny monitoruje przychodzący i wychodzący ruch telekomunikacyjny z częstotliwością [*Realizacja: częstotliwość określona przez organizację*] pod kątem nietypowych lub nieautoryzowanych działań.

(5) MONITOROWANIE SYSTEMU TELEINFORMATYCZNEGO | ALERTY SYSTEMOWE

System teleinformatyczny ostrzega [*Realizacja: personel lub role zdefiniowane przez organizację*] w przypadku wystąpienia następujących oznak naruszenia lub potencjalnego naruszenia: [*Realizacja: wskaźniki naruszenia zdefiniowane przez organizację*].

Zabezpieczenia powiązane: AU-5, PE-6.

(6) MONITOROWANIE SYSTEMU TELEINFORMATYCZNEGO | OGRANICZANIE NIEUPRZYWILEJOWANYCH UŻYTKOWNIKÓW

[Włączono do AC-6 (10)].

(7) MONITOROWANIE SYSTEMU TELEINFORMATYCZNEGO | AUTOMATYCZNA ODPOWIEDŹ NA PODEJRZANE ZDARZENIA

System teleinformatyczny powiadamia [*Realizacja: personel reagowania na incydenty zdefiniowane przez organizację (zidentyfikowane według nazwiska i / lub roli)*] o wykrytych podejrzanych zdarzeniach i podejmuje [*Realizacja: zdefiniowane przez organizację działania najmniej zakłócające pracę systemu, w celu wyeliminowania podejrzanych zdarzeń*].

(8) MONITOROWANIE SYSTEMU TELEINFORMATYCZNEGO | OCHRONA INFORMACJI MONITORUJĄCYCH

[Włączono do SI-4].

(9) MONITOROWANIE SYSTEMU TELEINFORMATYCZNEGO | TESTOWANIE NARZĘDZI MONITORUJĄCYCH

Organizacja testuje narzędzia do monitorowania włamań z częstotliwością [*Realizacja: częstotliwość zdefiniowana przez organizację*].

Zabezpieczenia powiązane: CP-9.

(10) MONITOROWANIE SYSTEMU TELEINFORMATYCZNEGO | INSPEKCJA ZASZYFROWANYCH KOMUNIKATÓW

Organizacja zapewnia, że [*Realizacja: zdefiniowany przez organizację zaszyfrowany ruch telekomunikacyjny*] jest widoczny przez [*Realizacja: narzędzia monitorowania systemu teleinformatycznego zdefiniowane przez organizację*].

(11) MONITOROWANIE SYSTEMU TELEINFORMATYCZNEGO | ANALIZA ANOMALII RUCHU TELEKOMUNIKACYJNEGO

Organizacja analizuje wychodzący ruch telekomunikacyjny na urządzeniach brzegowych systemu teleinformatycznego i definiuje, celem wykrycia anomalii[68] [*Realizacja: zdefiniowane przez organizację punkty wewnętrzne w systemie (np. podsieci, podsystemy)*].

(12) MONITOROWANIE SYSTEMU TELEINFORMATYCZNEGO | AUTOMATYCZNE ALERTY

Organizacja stosuje zautomatyzowane mechanizmy ostrzegania pracowników ochrony o następujących nieodpowiednich lub nietypowych działaniach mających wpływ na bezpieczeństwo: [*Realizacja: działania zdefiniowane przez organizację, które wyzwalają alarmy*].

Zabezpieczenia powiązane: AC-18, IA-3.

(13) MONITOROWANIE SYSTEMU TELEINFORMATYCZNEGO | ANALIZA MODELU RUCHU / ZDARZEŃ TELEKOMUNIKACYJNYCH

Organizacja:

(a) Analizuje model ruchu / zdarzeń telekomunikacyjnych danego systemu teleinformatycznego;

[68] Np. duże transfery plików, długotrwałe połączenia, nietypowe protokoły i porty w użyciu oraz próby komunikacji z podejrzanymi złośliwymi adresami zewnętrznymi.

(b) Opracowuje profile reprezentujące typowe wzorce ruchu i / lub zdarzenia;

(c) Wykorzystuje profile ruchu / zdarzeń do przystosowywania urządzeń monitorujących system, celem zmniejszenia liczby fałszywych i rzeczywistych alarmów.

(14) MONITOROWANIE SYSTEMU TELEINFORMATYCZNEGO | WYKRYWANIE ATAKÓW BEZPRZEWODOWYCH

Organizacja wykorzystuje bezprzewodowy system wykrywania włamań do identyfikowania nieautoryzowanych urządzeń bezprzewodowych oraz wykrywania prób ataków i potencjalnych zagrożeń / naruszeń systemu teleinformatycznego.

Zabezpieczenia powiązane: AC-18, IA-3.

(15) MONITOROWANIE SYSTEMU TELEINFORMATYCZNEGO | TELEKOMUNIKACJA BEZPRZEWODOWA / PRZEWODOWA

Organizacja stosuje system wykrywania włamań do monitorowania ruchu telekomunikacyjnego generowanego przez urządzenia bezprzewodowe i nawiązywania połączeń z sieci bezprzewodowych do przewodowych.

Zabezpieczenia powiązane: AC-18.

(16) MONITOROWANIE SYSTEMU TELEINFORMATYCZNEGO | KORELOWANIE INFORMACJI MONITORUJĄCYCH

Organizacja koreluje informacje z poszczególnych narzędzi monitorowania stosowanych w całym systemie teleinformatycznym.

Zabezpieczenia powiązane: AU-6.

(17) MONITOROWANIE SYSTEMU TELEINFORMATYCZNEGO | ZINTEGROWANA ŚWIADOMOŚĆ SYTUACYJNA

Organizacja koreluje informacje z monitorowania działań fizycznych, cybernetycznych i łańcucha dostaw w celu osiągnięcia zintegrowanej świadomości sytuacyjnej w całej organizacji.

Zabezpieczenia powiązane: SA-12.

(18) MONITOROWANIE SYSTEMU TELEINFORMATYCZNEGO | ANALIZA RUCHU / ZAPOBIEGANIE EKSFILTRACJI

Organizacja analizuje wychodzący ruch telekomunikacyjny na urządzeniach brzegowych systemu teleinformatycznego (tj. na obrzeżach systemu) i w [*Realizacja: zdefiniowane przez organizację punkty wewnętrzne w systemie (np. podsystemy, podsieci)*] w celu wykrycia ukrytej eksfiltracji informacji.

(19) MONITOROWANIE SYSTEMU TELEINFORMATYCZNEGO | ZWIĘKSZONE RYZYKO GENEROWANE PRZEZ OSOBY

Organizacja wdraża [*Realizacja: zdefiniowane przez organizację dodatkowe monitorowanie*] osób, które zostały zidentyfikowane przez [*Realizacja: źródła zdefiniowane przez organizację*] jako stwarzające zwiększony poziom ryzyka.

(20) MONITOROWANIE SYSTEMU TELEINFORMATYCZNEGO | UPRZYWILEJOWANI UŻYTKOWNICY

Organizacja wdraża [*Realizacja: zdefiniowane przez organizację dodatkowe monitorowanie*] uprzywilejowanych użytkowników.

(21) MONITOROWANIE SYSTEMU TELEINFORMATYCZNEGO | OKRESY PRÓBNE

Organizacja realizuje [*Realizacja: dodatkowe monitorowanie zdefiniowane przez organizację*] osób podczas [*Realizacja: okres próbny zdefiniowany przez organizację*].

(22) MONITOROWANIE SYSTEMU TELEINFORMATYCZNEGO | NIEAUTORYZOWANE USŁUGI SIECIOWE

System teleinformatyczny wykrywa usługi sieciowe, w [*Realizacja: procesy autoryzacji lub zatwierdzania zdefiniowane przez organizację*] i [*Wybór (jeden lub więcej): audyty; alerty]* które nie zostały autoryzowane ani zatwierdzone przez *[Realizacja: personel lub role zdefiniowane przez organizację]*].

Zabezpieczenia powiązane: AC-6, CM-7, SA-5, SA-9.

(23) MONITOROWANIE SYSTEMU TELEINFORMATYCZNEGO | KOMPUTER GŁÓWNY (HOST)

Organizacja wdraża [*Realizacja: zdefiniowane przez organizację mechanizmy monitorowania oparte na hoście*] w [*Realizacja: zdefiniowane przez organizację elementy systemu teleinformatycznego*].

(24) MONITOROWANIE SYSTEMU TELEINFORMATYCZNEGO | WSKAŹNIKI RYZYKA

System teleinformatyczny odkrywa, gromadzi, dystrybuuje i wykorzystuje wskaźniki ryzyka[69].

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	SI-4	SI-4 (2) (4) (5)	SI-4 (2) (4) (5)

[69] Wskaźniki ryzyka (Indicators of Compromise - IOC) to artefakty kryminalistyczne pochodzące z włamań, które są identyfikowane w organizacyjnych systemach informatycznych (na poziomie hosta lub sieci). IOC dostarczają organizacjom cennych informacji na temat obiektów lub systemów informatycznych, które zostały naruszone.

SI-5 ALERTY BEZPIECZEŃSTWA, PORADY I DYREKTYWY

Zabezpieczenie: Organizacja:

a. Otrzymuje na bieżąco powiadomienia o bezpieczeństwie systemu teleinformatycznego, porady i wytyczne od [*Realizacja: organizacje zewnętrzne zdefiniowane przez organizację*];

b. Generuje alarmy bezpieczeństwa wewnętrznego, porady i wytyczne, jeśli uzna to za konieczne;

c. Rozpowszechnia alerty bezpieczeństwa, porady i wytyczne: [*Wybór (jeden lub więcej): [Realizacja: personel lub role zdefiniowane przez organizację*]; [*Realizacja: elementy zdefiniowane przez organizację w organizacji]; [Realizacja: organizacje zewnętrzne zdefiniowane przez organizację]*];

d. Wdraża dyrektywy bezpieczeństwa zgodnie z ustalonymi ramami czasowymi lub powiadamia organizację wydającą o stopniu niezgodności.

Zabezpieczenia powiązane: SI-2.

Zabezpieczenia rozszerzone:

(1) ALERTY BEZPIECZEŃSTWA, PORADY I DYREKTYWY | AUTOMATYCZNE ALERTY I PORADY

Organizacja stosuje zautomatyzowane mechanizmy, udostępniające alerty bezpieczeństwa i informacje doradcze w całej organizacji.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	SI-5	SI-5	SI-5 (1)

SI-6 WERYFIKACJA FUNKCJI BEZPIECZEŃSTWA

Zabezpieczenie: System teleinformatyczny:

a. Sprawdza poprawność działania [*Realizacja: funkcje bezpieczeństwa zdefiniowane przez organizację*];

b. Dokonuje weryfikacji poprawności działania [*Wybór (jeden lub więcej): [Realizacja: stany przejściowe[70] systemu zdefiniowane przez organizację]; na polecenie użytkownika z odpowiednimi uprawnieniami; [Realizacja: częstotliwość określona przez organizację]*];

c. Powiadamia [*Realizacja: personel lub role zdefiniowane przez organizację*] o nieudanych testach weryfikacji bezpieczeństwa;

d. [*Wybór (jeden lub więcej): zamyka system teleinformatyczny; ponownie uruchamia system teleinformatyczny; [Realizacja: zdefiniowane przez organizację działania alternatywne]*] w przypadku wykrycia anomalii.

Zabezpieczenia powiązane: CA-7, CM-6.

Zabezpieczenia rozszerzone:

(1) WERYFIKACJA FUNKCJI BEZPIECZEŃSTWA | POWIADOMIENIE O NIEUDANYCH TESTACH BEZPIECZEŃSTWA

[Włączono do SI-6].

(2) WERYFIKACJA FUNKCJI BEZPIECZEŃSTWA | WSPARCIE AUTOMATYZACYJNE BADAŃ ROZPROSZONYCH

System teleinformatyczny wdraża zautomatyzowane mechanizmy wspierające zarządzanie rozproszonymi testami bezpieczeństwa.

Zabezpieczenia powiązane: SI-2.

(3) WERYFIKACJA FUNKCJI BEZPIECZEŃSTWA | RAPORT Z WYNIKÓW WERYFIKACJI

Organizacja raportuje wyniki weryfikacji funkcji bezpieczeństwa poniższym: [*Realizacja: personel lub role zdefiniowane przez organizację*].

Zabezpieczenia powiązane: SA-12, SI-4, SI-5.

[70] Stany przejściowe dla systemów teleinformatycznych obejmują np. uruchomienie, restart, zamknięcie i przerwanie działania systemu.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	SI-6 (opcjonalnie)	SI-6 (opcjonalnie)	SI-6

SI-7 APLIKACJE, OPROGRAMOWANIE UKŁADOWE I INTEGRALNOŚĆ INFORMACJI

Zabezpieczenie: Organizacja wykorzystuje narzędzia do weryfikacji integralności w celu wykrycia nieautoryzowanych zmian w [*Realizacja: aplikacje, oprogramowanie układowe i informacje zdefiniowane przez organizację*].

Zabezpieczenia powiązane: SA-12, SC-8, SC-13, SI-3.

Zabezpieczenia rozszerzone:

(1) APLIKACJE, OPROGRAMOWANIE UKŁADOWE I INTEGRALNOŚĆ INFORMACJI | KONTROLE INTEGRALNOŚCI

System teleinformatyczny sprawdza integralność [*Realizacja: aplikacje zdefiniowane przez organizację, oprogramowanie układowe i informacje*] [*Wybór (jeden lub więcej): przy uruchomieniu; w [Realizacja: stany przejściowe zdefiniowane przez organizację lub zdarzenia istotne dla bezpieczeństwa[71]]; [Realizacja: częstotliwość zdefiniowana przez organizację]*].

(2) APLIKACJE, OPROGRAMOWANIE UKŁADOWE I INTEGRALNOŚĆ INFORMACJI | AUTOMATYCZNE POWIADOMIENIA O NARUSZENIACH INTEGRALNOŚCI

Organizacja stosuje zautomatyzowane narzędzia, które powiadamiają [*Realizacja: personel lub role zdefiniowane przez organizację*] po wykryciu rozbieżności podczas weryfikacji integralności.

(3) APLIKACJE, OPROGRAMOWANIE UKŁADOWE I INTEGRALNOŚĆ INFORMACJI | NARZĘDZIA DO CENTRALNEGO ZARZĄDZANIA INTEGRALNOŚCIĄ

Organizacja wykorzystuje centralnie zarządzane narzędzia do weryfikacji integralności.

Zabezpieczenia powiązane: AU-3, SI-2, SI-8.

[71] Zdarzenia istotne dla bezpieczeństw obejmują np. identyfikację nowego zagrożenia, na które podatne są systemy teleinformacyjne organizacji, oraz instalację nowego sprzętu, aplikacji lub oprogramowania układowego.

(4) APLIKACJE, OPROGRAMOWANIE UKŁADOWE I INTEGRALNOŚĆ INFORMACJI | OCHRONA PRZED NARUSZENIAMI

[Włączone do SA-12].

(5) APLIKACJE, OPROGRAMOWANIE UKŁADOWE | INTEGRALNOŚĆ INFORMACJI | AUTOMATYCZNA ODPOWIEDŹ NA NARUSZENIA INTEGRALNOŚCI

System teleinformatyczny automatycznie [*Wybór (jeden lub więcej): zamyka system teleinformatyczny; ponownie uruchamia system teleinformatyczny; automatycznie implementuje*[72] *[Realizacja: środki bezpieczeństwa zdefiniowane przez organizację]*] po wykryciu naruszenia integralności.

(6) APLIKACJE, OPROGRAMOWANIE UKŁADOWE I INTEGRALNOŚĆ INFORMACJI | OCHRONA KRYPTOGRAFICZNA

System teleinformatyczny implementuje mechanizmy kryptograficzne do wykrywania nieautoryzowanych zmian w aplikacjach, oprogramowaniu układowym i informacjach.

Zabezpieczenia powiązane: SC-13.

(7) APLIKACJE, OPROGRAMOWANIE UKŁADOWE | INTEGRALNOŚĆ INFORMACJI | INTEGRACJA WYKRYWANIA I ODPOWIEDZI

Organizacja włącza wykrywanie nieautoryzowanych zmian[73] [*Realizacja: zmiany w systemie teleinformatycznym dotyczące bezpieczeństwa określone przez organizację*] do zdolności reagowania na incydenty organizacyjne.

Zabezpieczenia powiązane: IR-4, IR-5, SI-4.

(8) APLIKACJE, OPROGRAMOWANIE UKŁADOWE | INTEGRALNOŚĆ INFORMACJI | ZDOLNOŚĆ AUDYTU ISTOTNYCH ZDARZEŃ

Organizacje wybierają działania reagowania na podstawie rodzajów oprogramowania, określonego oprogramowania lub informacji, w przypadku których mogą wystąpić naruszenia integralności.

Zabezpieczenia powiązane: AU-2, AU-6, AU-12.

[72] Automatyczna implementacja określonych zabezpieczeń w organizacyjnych systemach teleinformatycznych obejmuje np. cofanie zmian, zatrzymywanie systemu teleinformatycznego lub wyzwalanie alertów kontrolnych w przypadku nieautoryzowanych modyfikacji krytycznych plików bezpieczeństwa.

[73] Np. nieautoryzowane zmiany w ustalonych ustawieniach konfiguracji lub nieuprawnione podniesienie uprawnień systemu teleinformatycznego.

(9) APLIKACJE, OPROGRAMOWANIE UKŁADOWE | INTEGRALNOŚĆ INFORMACJI | WERYFIKACJA PROCESU URUCHAMIANIA

System teleinformatyczny weryfikuje integralność procesu uruchamiania[74] [*Realizacja: urządzenia zdefiniowane przez organizację*].

(10) APLIKACJE, OPROGRAMOWANIE UKŁADOWE , I INTEGRALNOŚĆ INFORMACJI | OCHRONA URUCHAMIANIA OPROGRAMOWANIA UKŁADOWEGO

System teleinformatyczny implementuje [*Realizacja: środki bezpieczeństwa zdefiniowane przez organizację*] w celu ochrony integralności oprogramowania układowego[75] w [*Realizacja: urządzenia zdefiniowane przez organizację*].

(11) APLIKACJE, OPROGRAMOWANIE UKŁADOWE I INTEGRALNOŚĆ INFORMACJI | ZAMKNIĘTE ŚRODOWISKO Z OGRANICZONYMI UPRAWNIENIAMI

Organizacja wymaga, aby [*Realizacja: oprogramowanie zdefiniowane przez użytkownika*] działało w ograniczonym środowisku maszyny fizycznej lub wirtualnej z ograniczonymi uprawnieniami.

(12) APLIKACJE, OPROGRAMOWANIE UKŁADOWE I INTEGRALNOŚĆ INFORMACJI | WERYFIKACJA INTEGRALNOŚCI

Organizacja wymaga sprawdzenia integralności [*Realizacja: oprogramowanie zainstalowane przez użytkownika*] przed jego wykonaniem.

(13) APLIKACJE, OPROGRAMOWANIE UKŁADOWE I INTEGRALNOŚĆ INFORMACJI | WYKONANIE KODU W ŚRODOWISKACH CHRONIONYCH

Organizacja zezwala na wykonywanie kodu binarnego lub kodu maszynowego, uzyskanego ze źródeł z ograniczoną gwarancją lub bez gwarancji i bez udostępnienia kodu źródłowego tylko w ograniczonych środowiskach fizycznych lub maszynach wirtualnych i za wyraźną zgodą [*Realizacja: personel lub role zdefiniowane przez organizację*] .

(14) APLIKACJE, OPROGRAMOWANIE UKŁADOWE I INTEGRALNOŚĆ INFORMACJI | KOD WYKONYWALNY BINARNY LUB MASZYNOWY

Organizacja:

(a) zabrania używania kodu wykonywalnego binarnego lub kodu maszynowego (w tym oprogramowania komercyjnego / oprogramowania układowego i oprogramowania open source) ze źródeł z ograniczoną gwarancją lub bez gwarancji i bez podania kodu źródłowego;

(b) Zapewnia wyjątki od wymogu dotyczącego kodu źródłowego tylko w przypadku istotnych wymagań misji / operacyjnych i za zgodą upoważnionej osoby.

Zabezpieczenia powiązane: SA-5.

[74] Mechanizmy weryfikacji integralności zapewniają pracownikom organizacji pewność, że tylko zaufany kod jest wykonywany podczas procesów rozruchu.

[75] Urządzenia mogą chronić integralność oprogramowania rozruchowego w systemach informacji organizacyjnej poprzez weryfikację integralności i autentyczności wszystkich aktualizacji oprogramowania rozruchowego przed zastosowaniem zmian w urządzeniach rozruchowych, oraz zapobieganie modyfikowaniu oprogramowania układowego przez nieautoryzowane procesy.

(15) APLIKACJE, OPROGRAMOWANIE UKŁADOWE I INTEGRALNOŚĆ INFORMACJI | AUTORYZACJA KODU

System teleinformatyczny implementuje, przed instalacją, mechanizmy kryptograficzne do uwierzytelnienia [*Realizacja: aplikacje zdefiniowane przez organizację lub elementy oprogramowania układowego*].

(16) APLIKACJE, OPROGRAMOWANIE UKŁADOWE I INTEGRALNOŚĆ INFORMACJI | LIMIT CZASU NA WYKONANIE PROCESU BEZ NADZORU

Organizacja nie zezwala na wykonywanie procesów bez nadzoru[76] przez okres dłuższy niż [Realizacja: okres zdefiniowany przez organizację].

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	SI-7 (opcjonalnie)	SI-7 (1) (7)	SI-7 (1) (2) (5) (7) (14)

SI-8 OCHRONA PRZED SPAMEM

Zabezpieczenie: Organizacja:

a. Stosuje mechanizmy ochrony przed spamem w punktach wejścia i wyjścia z systemu teleinformatycznego w celu wykrywania niechcianych wiadomości i podejmowania stosownych działań;

b. Aktualizuje mechanizmy ochrony przed spamem zgodnie z zasadami i procedurami zarządzania konfiguracją organizacji.

Zabezpieczenia powiązane: AT-2, AT-3, SC-5, SC-7, SI-3.

Zabezpieczenia rozszerzone:

(1) OCHRONA PRZED SPAMEM | CENTRALNE ZARZĄDZANIE

Organizacja centralnie zarządza mechanizmami ochrony przed spamem.

Zabezpieczenia powiązane: AU-3, SI-2, SI-7.

(2) OCHRONA PRZED SPAMEM | AUTOMATYCZNE AKTUALIZACJE

System teleinformatyczny automatycznie aktualizuje mechanizmy ochrony przed spamem.

[76] Nadzór obejmuje np. liczniki czasu systemu operacyjnego, automatyczne odpowiedzi lub ręczny nadzór i reakcję na wystąpienie anomalii procesu teleinformatycznego.

(3) OCHRONA PRZED SPAMEM | CIĄGŁA ZDOLNOŚĆ DO NAUKI

System teleinformatyczny wdraża mechanizmy ochrony przed spamem z możliwością uczenia się w celu skuteczniejszej identyfikacji legalnego ruchu telekomunikacyjnego.

Zabezpieczenia powiązane: Brak

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P2	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	SI-8 (opcjonalnie)	SI-8 (1) (2)	SI-8 (1) (2

SI-9 OGRANICZENIA WPROWADZANIA INFORMACJI

[Włączony do AC-2, AC-3, AC-5, AC-6].

SI-10 WERYFIKACJA WPROWADZANYCH INFORMACJI

Zabezpieczenie: System teleinformatyczny sprawdza prawidłowość [*Realizacja: dane wejściowe określone przez organizację*].

Zabezpieczenia rozszerzone:

(1) WERYFIKACJA WPROWADZANIA INFORMACJI | RĘCZNE ZASTĘPOWANIE

System teleinformatyczny:

(a) Zapewnia możliwość ręcznego zastąpienia w celu zatwierdzenia danych wejściowych [*Realizacja: dane zdefiniowane przez organizację*];

(b) Ogranicza możliwość ręcznego zastąpienia tylko do [*Realizacja: osoby upoważnione zdefiniowane przez organizację*];

(c) Kontroluje wykorzystanie możliwości ręcznego obejścia.

Zabezpieczenia powiązane: CM-3, CM-5,

(2) WERYFIKACJA WPROWADZANIA INFORMACJI | PRZEGLĄD / USUWANIE BŁĘDÓW

Organizacja zapewnia, że błędy sprawdzania poprawności danych wejściowych są przeglądane i usuwane w ciągu [*Realizacja: okres zdefiniowany przez organizację*].

(3) WERYFIKACJA WPROWADZANIA INFORMACJI | PRZEWIDYWALNE ZACHOWANIE

System teleinformatyczny zachowuje się w przewidywalny i udokumentowany sposób, który odzwierciedla cele organizacyjne i systemowe po otrzymaniu nieprawidłowych danych wejściowych.

(4) WERYFIKACJA WPROWADZANIA INFORMACJI | INTERAKCJE CZASOWE

Organizacja bierze pod uwagę interakcje czasowe między komponentami systemu teleinformatycznego w określaniu odpowiednich odpowiedzi na nieprawidłowe dane wejściowe.

(5) WERYFIKACJA WPROWADZANIA INFORMACJI | OGRANICZANIE DANYCH WEJŚCIOWYCH DO ZAUFANYCH ŹRÓDEŁ I ZATWIERDZONYCH FORMATÓW

Organizacja ogranicza wykorzystanie danych wejściowych do *[Realizacja: zaufane źródła zdefiniowane przez organizację*] i / lub [*Realizacja: formaty zdefiniowane przez organizację*].

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	SI-10 (opcjonalnie)	SI-10	SI-10

SI-11 OBSŁUGA BŁĘDÓW

Zabezpieczenie: system teleinformatyczny:

a. Generuje komunikaty o błędach, które dostarczają informacji niezbędnych do działań naprawczych bez ujawniania informacji, które mogą zostać wykorzystane przez przeciwników;

b. Wyświetla komunikaty o błędach tylko zdefiniowanemu [*Realizacja: personel lub role zdefiniowane przez organizację*].

Zabezpieczenia powiązane: AU-2, AU-3, SC-31.

Zabezpieczenia rozszerzone: Brak.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P2	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	SI-11 (opcjonalnie)	SI-11	SI-11

SI-12 PRZECHOWYWANIE I RETENCJA INFORMACJI

Zabezpieczenie: Organizacja przetwarza i przechowuje informacje w systemie teleinformatycznym oraz informacje wyjściowe z systemu zgodnie z obowiązującymi przepisami, zarządzeniami wykonawczymi, dyrektywami, politykami, przepisami, standardami i wymaganiami operacyjnymi.

Zabezpieczenia powiązane: AC-16, AU-5, AU-11, MP-2, MP-4.

Zabezpieczenia rozszerzone: Brak.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P2	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	SI-12	SI-12	SI-12

SI-13 PRZEWIDYWANIE AWARII

Zabezpieczenie: Organizacja:

a. Określa średni czas między awariami odnoszący się do *[Realizacja: elementy systemu teleinformatycznego zdefiniowane przez organizację*] w określonych środowiskach działania;

b. Zapewnia zastępcze komponenty systemu teleinformatycznego i środki do wymiany aktywnych i rezerwowych komponentów w [*Realizacja: zdefiniowane przez organizację kryteria wymiany*].

Zabezpieczenia powiązane: CP-2, CP-10, MA-6.

Zabezpieczenia rozszerzone:

(1) PRZEWIDYWANIE AWARII | PRZENIESIENIE ODPOWIEDZIALNOŚCI KOMPONENTÓW

Organizacja wyłącza komponenty systemu teleinformatycznego, przenosząc odpowiedzialność za komponenty na części zastępujące nie później niż [*Realizacja: część lub procent zdefiniowany przez organizację*] średniego czasu do awarii.

(2) PRZEWIDYWANIE AWARII | LIMIT CZASU NA WYKONANIE PROCESU BEZ NADZORU

[Włączono do SI-7 (16)].

(3) PRZEWIDYWANIE AWARII | RĘCZNY TRANSFER MIĘDZY SKŁADNIKAMI

Organizacja ręcznie inicjuje przekazywanie między aktywnymi i rezerwowymi komponentami systemu teleinformatycznego z częstotliwością[*Realizacja: częstotliwość zdefiniowana przez organizację*], jeśli średni czas do wystąpienia awarii przekracza [*Realizacja: okres zdefiniowany przez organizację*].

(4) PRZEWIDYWANIE AWARII | INSTALACJA KOMPONENTÓW Z LISTY REZERWOWEJ / POWIADOMIENIE

Organizacja, jeśli zostaną wykryte awarie komponentów systemu teleinformatycznego:

(a) Zapewnia, że komponenty rezerwowe zostaną pomyślnie i przejrzyście zainstalowane w okresie [*Realizacja: okres zdefiniowany przez organizację*];

(b) [*Wybór (jeden lub więcej): aktywuje [Realizacja: alarm zdefiniowany przez organizację]; automatycznie wyłącza system teleinformatyczny*].

(5) PRZEWIDYWANIE AWARII | PRZEŁĄCZANIE AWARYJNE

Organizacja zapewnia *[Realizacja: w czasie rzeczywistym; z akceptowanym czasem odpowiedzi*] [*Realizacja: przełączanie awaryjne*[77] *zdefiniowane przez organizację*] w systemie teleinformatycznym.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P0	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	SI-13 (opcjonalnie)	SI-13 (opcjonalnie)	SI-13 (opcjonalnie)

SI-14 ZAPOBIEGANIE ZAAWANSOWANYM DŁUGOTRWAŁYM ATAKOM (ATAKI TYPU APT)

Zabezpieczenie: Organizacja wdraża tzw. nietrwałości *[Realizacja: komponenty i usługi systemu teleinformatycznego zdefiniowane przez organizację*], które są inicjowane w znanym stanie i zakończone [*Wybór (jeden lub więcej): po zakończeniu sesji użytkowania; okresowo w [Realizacja: częstotliwość określona przez organizację]*].

Zabezpieczenia powiązane: SC-30, SC-34.

Zabezpieczenia rozszerzone:

(1) ZAPOBIEGANIE ZAAWANSOWANYM DŁUGOTRWAŁYM ATAKOM TYPU APT | ODŚWIEŻANIE Z ZAUFANYCH ŹRÓDEŁ

Organizacja zapewnia, że oprogramowanie i dane wykorzystywane podczas odświeżania komponentów systemu teleinformatycznego i usług są uzyskiwane z [*Realizacja: zaufane źródła zdefiniowane przez organizację*].

[77] Funkcja przełączania awaryjnego obejmuje np. włączenie operacji systemu lustrzanego systemu teleinformatycznego w alternatywnych miejscach przetwarzania lub okresowe tworzenie kopii danych w regularnych odstępach czasu określonych przez okresy odtwarzania organizacji.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P0	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	SI-14 (opcjonalnie)	SI-14 (opcjonalnie)	SI-14 (opcjonalnie)

SI-15 FILTROWANIE INFORMACJI WYJŚCIOWYCH

Zabezpieczenie: System teleinformatyczny weryfikuje dane wyjściowe[78] z *[Realizacja: oprogramowanie i / lub aplikacje zdefiniowane przez organizację*], aby upewnić się, że informacje są zgodne z oczekiwaną treścią.

Zabezpieczenia powiązane: SI-3, SI-4.

Zabezpieczenia rozszerzone: Brak.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P0	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	SI-15 (opcjonalnie)	SI-15 (opcjonalnie)	SI-15 (opcjonalnie)

SI-16 OCHRONA PAMIĘCI

Zabezpieczenie: System teleinformatyczny implementuje [*Realizacja: środki bezpieczeństwa zdefiniowane przez organizację*], chroniące swoją pamięć przed nieautoryzowanym uruchomieniem kodu.

Zabezpieczenia powiązane: AC-25, SC-3.

Zabezpieczenia rozszerzone: Brak.

[78] Zabezpieczenie skupia się na wykrywaniu obcych treści, zapobieganiu wyświetlaniu takich obcych treści oraz aktualizacji narzędzi monitorowania o wykryciu nietypowego zachowania.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P1	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	SI-16 (opcjonalnie)	SI-16	SI-16

SI-17 BEZPIECZNE PROCEDURY

Zabezpieczenie: System teleinformatyczny wdraża [*Realizacja: organizacyjne zdefiniowane procedury bezpieczeństwa*[79] *w przypadku wystąpienia awarii*], gdy [*Realizacja: wystąpiły warunki awarii*[80] *zdefiniowane przez organizację*].

Zabezpieczenia powiązane: CP-12, CP-13, SC-24, SI-13.

Zabezpieczenia rozszerzone: Brak.

Priorytet wdrożenia zabezpieczenia oraz potencjalny wpływ na ustanowione atrybuty bezpieczeństwa

Priorytet wdrożenia	**Potencjalny wpływ na atrybuty bezpieczeństwa systemu teleinformatycznego i informacji**		
P0	NISKI	UMIARKOWANY	WYSOKI
	Kategoria zabezpieczeń		
	SI-17 (opcjonalnie)	SI-17 (opcjonalnie)	SI-17 (opcjonalnie)

[79] Procedury bezpieczeństwa w razie wystąpienia awarii obejmują np. ostrzeganie personelu operatora i udzielanie szczegółowych instrukcji na temat kolejnych kroków, które należy podjąć (np. nic nie rób, przywróć ustawienia systemu, zamknij procesy, ponownie uruchom system lub skontaktuj się z wyznaczonym personelem organizacyjnym).

[80] Warunki wystąpienia awarii obejmują np. utratę komunikacji między krytycznymi komponentami systemu lub między komponentami systemu i obiektami operacyjnymi.