mSecure

CYBERBEZPIECZEŃSTWO | AUDYT | HARDENING

WZORZEC PUBLICZNY / DANE SYNTETYCZNE

PLAN CYBERBEZPIECZEŃSTWA 30 / 60 / 90

Program ograniczenia ryzyka po audycie: właściciele, zależności, rezultaty i kryteria odbioru

Wykonawca	MSecure Michał Matuszczyk
Organizacja	Organizacja przykładowa
Punkt wyjścia	14 ustaleń: 3 wysokie, 7 średnich, 4 niskie
Data / wersja	30 sierpnia 2026 / 3.0
Klasyfikacja	PUBLICZNY WZORZEC

Dokument demonstracyjny. Wszystkie parametry środowiska i ustalenia są syntetyczne. Materiał nie zawiera danych żadnego klienta MSecure.

SEKCJA 01

Zasady programu

Roadmapa nie jest kalendarzem życzeń. Każda pozycja ma właściciela, zależność, mierzalny rezultat, dowód odbioru i sposób postępowania, gdy termin nie może zostać dotrzymany.

3	12	9	90 dni
strumienie pracy	rezultatów	właścicieli	pierwszy cykl

Priorytetyzacja

Zasada	Znaczenie
Najpierw ekspozycja	Ograniczamy scenariusze o największym możliwym wpływie i najkrótszej drodze nadużycia.
Potem fundament	Porządkujemy właścicieli, procesy, urządzenia, dostawców i dowody.
Na końcu trwałość	Walidujemy zmiany, mierzymy skuteczność i uruchamiamy cykliczny nadzór.

SEKCJA 02

Dni 0-30 - ograniczenie ekspozycji

ID	Działanie	Owner	Zależność	Rezultat	Dowód odbioru
A1	Zredukować app-only i przypisać właścicieli	IAM / Security	Test integracji	Minimalne role, ownerzy, rotacja	Eksport + zatwierdzenie + test
A2	Uzupełnić CA dla administratorów	IAM	Konta awaryjne	Pokryte scenariusze uprzywilejowane	Report-only + pilotaż + logi
A3	Ograniczyć dostęp z niezarządzanych urządzeń	Workplace	Grupy pilotażowe	Polityka dla danych wysokiego ryzyka	Test blokady + rejestr wyjątków
A4	Wprowadzić SLA obsługi alertów wysokich	SOC	Kanał eskalacji	Mierzona kwalifikacja i eskalacja	Próba alertu + dashboard

Brama 30 dni

Nie przechodzimy do formalnego zamknięcia, dopóki zmiana nie ma dowodu skuteczności. Konfiguracja bez próby działania pozostaje wdrożeniem niezweryfikowanym.

SEKCJA 03

Dni 31-60 - stabilizacja i proces

ID	Działanie	Owner	Rezultat	Miernik
B1	Recertyfikacja gości i ról uprzywilejowanych	Właściciele usług / IAM	Decyzje ownerów i usunięte dostępy	100% zakresu przeglądu
B2	Retencja i operacyjne użycie logów	Security / SOC	Zdefiniowane źródła i zapytania	Test wyszukiwania zakończony powodzeniem
B3	Test odtworzenia dwóch usług	BCM / IT	Zmierzony RPO/RTO i działania	Protokół zatwierdzony przez ownerów
B4	Segmentacja dostawców i klauzule	Zakupy / Security	Lista krytycznych dostawców i wymagania	100% dostawców krytycznych ocenionych

Zarządzanie zmianą

- każda polityka wpływająca na użytkowników ma pilotaż i komunikację;
- zmiany wysokiego ryzyka mają plan wycofania;
- wyjątek ma właściciela, uzasadnienie, datę wygaśnięcia i akceptację;
- status jest raportowany przez rezultat i dowód, nie przez procent wykonania deklarowany bez weryfikacji.

SEKCJA 04

Dni 61-90 - walidacja i utrzymanie

ID	Działanie	Owner	Kryterium odbioru
C1	Retest ustaleń wysokich i średnich	Security / Audyt	Dowód zamknięcia albo formalna akceptacja ryzyka
C2	Przegląd wyjątków i ryzyka rezydualnego	CISO / Ownerzy	Każdy wyjątek aktualny, zatwierdzony, z datą ponownej oceny
C3	Dashboard dla kierownictwa	CISO	Trend ryzyka, incydenty, odporność, dostawcy i decyzje
C4	Kalendarz kontroli cyklicznych	Security / IT	Owner, częstotliwość, źródło danych i ślad wykonania

Definicja ukończenia

Pytanie	Wymagana odpowiedź
Czy zmiana istnieje?	Tak - potwierdzona konfiguracją lub dokumentem
Czy działa?	Tak - potwierdzona próbą, alertem, logiem lub protokołem
Kto utrzymuje?	Właściciel zaakceptował odpowiedzialność i cykl przeglądu
Co pozostaje?	Ryzyko rezydualne opisane i zaakceptowane
Czy można odtworzyć decyzję?	Dowody, wersja, data i akceptacje są przechowywane

SEKCJA 05

Raportowanie i eskalacja

Częstotliwość	Odbiorca	Treść
Co tydzień	Ownerzy strumieni	Blokery, decyzje, dowody, działania następnego tygodnia
Co dwa tygodnie	Sponsor / CISO	Ryzyka wysokie, wyjątki, zależności i zużycie zasobów
Po 30/60/90 dniach	Kierownictwo	Zmiana profilu ryzyka, wyniki testów, akceptacje i kolejny cykl

Reguła eskalacji

Decyzja zamiast ukrytego opóźnienia

Jeżeli ustalenie wysokie nie może zostać zamknięte w terminie, owner przedstawia przyczynę, kontrolę tymczasową, nowe kryterium i datę. Ryzyko rezydualne zatwierdza osoba posiadająca odpowiedni mandat.

Wzorzec zawiera dane syntetyczne i nie jest gotowym planem dla innej organizacji. Kolejność należy ustalić po analizie ryzyka, architektury, zasobów oraz zależności operacyjnych.

msecure.com.pl | biuro@msecure.com.pl | +48 502 475 670