mSecure

CYBERBEZPIECZEŃSTWO | AUDYT | HARDENING

RAPORT AUDYTOWY / WZORZEC PUBLICZNY

PRZYKŁADOWY RAPORT AUDYTU BEZPIECZEŃSTWA MICROSOFT 365

Ocena konfiguracji technicznej, ryzyka, ochrony danych i zdolności reagowania

Wykonawca	MSecure Michał Matuszczyk
Środowisko	Organizacja przykładowa - tenant syntetyczny
Tryb	Odczytowy / bez zmian produkcyjnych
Data / wersja	30 sierpnia 2026 / 3.0
Klasyfikacja	PUBLICZNY WZORZEC - DANE SYNTETYCZNE

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

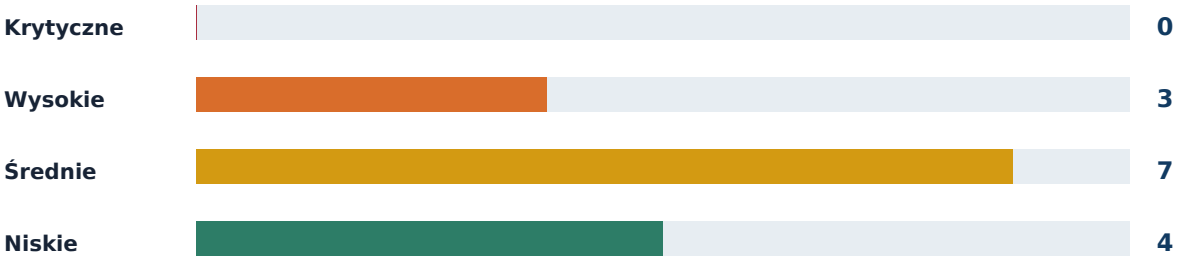
SEKCJA 01

Podsumowanie kierownicze

Jedna strona do decyzji: co działa, gdzie jest ekspozycja i jakie działania należy zatwierdzić.

Przegląd wykazał poprawnie działające fundamenty uwierzytelniania wieloskładnikowego i rejestrowania zdarzeń, ale odporność środowiska ograniczają trwałe uprawnienia aplikacji, niespójny dostęp warunkowy oraz brak zarządzania częścią urządzeń. Ryzyko oceniono jako podwyższone: nie odnotowano ustaleń krytycznych, lecz trzy ustalenia wysokie mogą istotnie zwiększyć zasięg przejęcia konta lub aplikacji.

420	63%	61/100	14
konta aktywne	urządzenia zarządzane	Secure Score - sygnał pomocniczy	ustalenia łącznie



Najważniejsze decyzje

- zatwierdzić właścicieli i przegląd uprawnień aplikacji korporacyjnych;
- wdrożyć polityki Conditional Access etapami: report-only, pilotaż, produkcja;
- objąć urządzenia mające dostęp do danych zasadami zgodności lub dostępem ograniczonym;
- wydłużyć i operacyjnie wykorzystać retencję logów dla kont uprzywilejowanych.

Rekomendowany model realizacji

Działania wysokie: 0-30 dni. Stabilizacja procesów i urządzeń: 31-60 dni. Walidacja, testy oraz cykliczny nadzór: 61-90 dni.

SEKCJA 02

Kontrola dokumentu i sposób czytania

Pole	Wartość
Cel	Przykład kompletnego rezultatu audytu M365
Status	Wzorzec publiczny, nie raport klienta
Autor	Michał Matuszczyk - MSecure
Wersja	3.0 / 30 sierpnia 2026
Klasyfikacja	Publiczny; bez danych operacyjnych i osobowych
Zakres odpowiedzialności	Ocena doradcza i techniczna; nie audyt certyfikacyjny ani opinia prawna

Skala ryzyka

Poziom	Znaczenie	Oczekiwana reakcja
Krytyczne	Aktywna lub bezpośrednia możliwość poważnego naruszenia	Natychmiastowa decyzja i ograniczenie ekspozycji
Wysokie	Realny scenariusz istotnego wpływu na dane lub ciągłość	Plan właścicielski do 30 dni
Średnie	Brak lub słabość kontroli zwiększająca prawdopodobieństwo/skutek	Realizacja w 60 dni lub formalna akceptacja
Niskie	Usprawnienie higieny, odporności lub audytowalności	Backlog do 90 dni

Zasada dowodowa

Każde ustalenie rozdziela stan faktyczny, scenariusz ryzyka, dowód, rekomendację i kryterium zamknięcia. W ten sposób ten sam materiał jest czytelny dla kierownictwa oraz wykonalny dla administratora.

SEKCJA 03

Zakres, metodologia i ograniczenia

Zakres bazowy

- Microsoft Entra ID: tożsamości, role, MFA, metody uwierzytelniania i dostęp warunkowy;
- aplikacje korporacyjne, zgody OAuth, tożsamości obciążeń i właściciele;
- Exchange Online: ochrona domen, poczta, reguły, forwarding i mechanizmy antyphishingowe;
- SharePoint, OneDrive i Teams: udostępnianie, goście, linki oraz konfiguracja współpracy;
- Microsoft Purview i Defender - wyłącznie w zakresie dostępnych licencji;
- Unified Audit Log, logi logowania i zdolność wyjaśnienia incydentu;
- urządzenia oraz zgodność - na podstawie danych dostępnych w Entra/Intune.

Metoda

Etap	Działanie	Rezultat
1. Discovery	Cel, tenanty, licencje, dane, ograniczenia, osoby odpowiedzialne	Karta zakresu i plan dowodów
2. Pozyskanie	Role tylko do odczytu, eksporty, logi, rozmowy	Rejestr źródeł i kompletności
3. Analiza	Korelacja konfiguracji z procesem i scenariuszem nadużycia	Ustalenia i ryzyka
4. Odbiór	Warsztat, ownerzy, terminy, kryteria zamknięcia	Backlog 30/60/90

Ograniczenia wzorca

Istotne

Dane na kolejnych stronach są syntetyczne. W prawdziwym audycie ograniczenia wynikają m.in. z licencji, retencji, brakujących logów, niedostępnych systemów końcowych oraz jakości danych. Brak dowodu nie jest automatycznie dowodem braku kontroli - jest ograniczeniem, które trzeba jawnie opisać.

SEKCJA 04

Charakterystyka środowiska

3	420	18	46
domeny zweryfikowane	konta aktywne	role uprzywilejowane	aplikacje korporacyjne

Obszar	Stan syntetyczny	Znaczenie dla oceny
Licencje	Mieszane: Business Premium i E3	Część zabezpieczeń dostępna nierównomiernie
Tożsamość	MFA 96%, Security Defaults wyłączone	Kontrola zależy od kompletności CA
Administracja	8 stałych kont administracyjnych	Wymaga rozdzielenia kont i redukcji ekspozycji
Urządzenia	268 zarządzanych / 158 niezarejestrowanych	Dostęp do danych z urządzeń bez oceny zgodności
Aplikacje	46 aplikacji; 7 z uprawnieniami app-only	Wymagany właściciel, przegląd i najmniejsze uprawnienia
Logi	Unified Audit Log aktywny	Pozytywny fundament; retencja zależna od licencji

Profil ekspozycji

Środowisko przykładowe jest typowe dla rozwijającej się organizacji: chmura wspiera kluczowe procesy, a liczba integracji i urządzeń rośnie szybciej niż model właścicielski. Największe znaczenie ma więc nie pojedyncze ustawienie, lecz ciągłość kontroli nad tożsamościami, aplikacjami i dostępem do danych.

SEKCJA 05

Kontrole pozytywne

Raport powinien pokazywać również mechanizmy działające prawidłowo. Pozwala to chronić dobre praktyki podczas zmian i budować plan naprawczy na istniejących fundamentach.

ID	Kontrola	Dowód / obserwacja	Wartość
P-01	Unified Audit Log aktywny	Wyszukiwanie zdarzeń zwróciło dane z okresu badania	Podstawa wyjaśniania incydentów
P-02	SPF i DKIM dla domen głównych	Rekordy i konfiguracja usług potwierdzone	Ograniczenie podszywania pod domenę
P-03	MFA dla wszystkich administratorów	Metody uwierzytelniania oraz próba polityk	Redukcja ryzyka przejęcia konta
P-04	Konta awaryjne wydzielone	Dwa konta, monitoring logowań, procedura użycia	Odporność na błędną politykę CA
P-05	Brak automatycznego forwarding zewnętrznego	Konfiguracja Exchange Online	Ograniczenie eksfiltracji poczty
P-06	Alerty wysokiego ryzyka	Defender generuje i eskaluje próbne zdarzenia	Działająca warstwa detekcji

Wniosek

Kontrole pozytywne nie równoważą automatycznie luk. Są jednak ważnym dowodem dojrzałości i wskazują, które elementy można wykorzystać do bezpiecznego wdrożenia zmian.

SEKCJA 06

Rejestr ustaleń

ID	Priorytet	Ustalenie	Właściciel	Termin
H-01	Wysokie	Trwałe uprawnienia app-only bez właścicieli i cyklu przeglądu	Security / IAM	30 dni
H-02	Wysokie	Conditional Access nie obejmuje wszystkich scenariuszy uprzywilejowanych	IAM	30 dni
H-03	Wysokie	Dostęp do danych z urządzeń bez oceny zgodności	Workplace	30-60 dni
M-01	Średnie	Brak cyklicznej recertyfikacji gości	Właściciele usług	60 dni
M-02	Średnie	Ograniczona retencja logów dla części licencji	Security	60 dni
M-03	Średnie	Niespójne rozdzielenie kont administracyjnych	IAM	45 dni
M-04	Średnie	Anonimowe linki SharePoint dostępne bez procesu wyjątków	Collaboration	60 dni
M-05	Średnie	Brak testów odtworzeniowych SaaS w ostatnich 12 miesiącach	BCM / IT	60 dni
M-06	Średnie	Brak miernika zamykania alertów wysokiego ryzyka	SOC	60 dni
M-07	Średnie	Zgody użytkowników dla aplikacji zbyt szerokie	IAM	45 dni
L-01	Niskie	Ujednolicić nazwy zasad i przypisać właścicieli	IAM	90 dni
L-02	Niskie	Udokumentować przegląd kont awaryjnych	Security	90 dni
L-03	Niskie	Włączyć cykliczny przegląd nieaktywnych urządzeń	Workplace	90 dni
L-04	Niskie	Dodać metryki wyjątków do raportu miesięcznego	Security	90 dni

Rejestr jest punktem sterowania realizacją. Szczegółowy opis ustalenia powinien być przechowywany razem z dowodem, decyzją właściciela i wynikiem walidacji.

USTALENIE H-01

Uprawnienia aplikacji app-only bez właściciela i cyklu przeglądu

WYSOKIE	Status: Siedem aktywnych aplikacji posiada uprawnienia aplikacyjne do poczty, katalogu lub plików. Dla trzech nie wskazano właściciela biznesowego, a dla żadnej nie przedstawiono dowodu kwartalnego przeglądu zakresu uprawnień.	Właściciel: Security / IAM	Termin: 30 dni

Stan faktyczny

Siedem aktywnych aplikacji posiada uprawnienia aplikacyjne do poczty, katalogu lub plików. Dla trzech nie wskazano właściciela biznesowego, a dla żadnej nie przedstawiono dowodu kwartalnego przeglądu zakresu uprawnień.

Scenariusz ryzyka i wpływ

Przejęcie sekretu lub certyfikatu aplikacji może umożliwić dostęp niezależny od sesji użytkownika i MFA. Brak właściciela wydłuża czas wykrycia oraz utrudnia bezpieczne wyłączenie integracji.

Dowód audytowy

Źródło i obserwacja

Eksport aplikacji korporacyjnych i service principals; lista appRoleAssignments; wywiad z właścicielem M365. Dowód syntetyczny: EV-APP-004.

Rekomendacja

Przypisać właścicieli biznesowych i technicznych, potwierdzić potrzebę każdej roli aplikacyjnej, usunąć nadmiarowe uprawnienia, przenieść poświadczenia do zarządzanego magazynu oraz wdrożyć cykliczną recertyfikację.

Kryterium zamknięcia

Weryfikacja

Każda aktywna aplikacja ma co najmniej dwóch właścicieli, udokumentowany cel, zatwierdzony minimalny zestaw uprawnień, datę wygaśnięcia poświadczenia i dowód przeglądu. Test integracji oraz logi sign-in potwierdzają działanie po redukcji ról.

USTALENIE H-02

Niepełne pokrycie scenariuszy uprzywilejowanych przez Conditional Access

WYSOKIE

Status: Zasady wymagają MFA dla większości administratorów, lecz nie obejmują dwóch ról katalogowych i logowań do wybranych interfejsów administracyjnych. Wyjątki nie mają terminu ani właściciela.

Właściciel: IAM

Termin: 30 dni

Stan faktyczny

Zasady wymagają MFA dla większości administratorów, lecz nie obejmują dwóch ról katalogowych i logowań do wybranych interfejsów administracyjnych. Wyjątki nie mają terminu ani właściciela.

Scenariusz ryzyka i wpływ

Atakujący wykorzystujący konto z pominiętym zakresem może wykonać operacje administracyjne bez oczekiwanej kontroli urządzenia lub lokalizacji. Nieudokumentowane wyjątki utrudniają rozpoznanie zamierzonego ryzyka.

Dowód audytowy

Źródło i obserwacja

Eksport Conditional Access, macierz użytkownik-rola-zasada, wyniki report-only z 14 dni. Dowód syntetyczny: EV-CA-011.

Rekomendacja

Zbudować macierz scenariuszy administracyjnych, ograniczyć wyjątki, najpierw uruchomić brakujące zasady w report-only, przeprowadzić pilotaż i dopiero potem egzekwować. Konta awaryjne pozostawić wyłączone z wybranych zasad, ale monitorowane.

Kryterium zamknięcia

Weryfikacja

Testy dla wszystkich ról potwierdzają wymaganą metodę uwierzytelniania i warunek urządzenia. Wyjątki mają właściciela, przyczynę, termin, zatwierdzenie ryzyka i alert użycia.

USTALENIE H-03

Dostęp do danych z urządzeń bez potwierdzonej zgodności

WYSOKIE

Status: 158 urządzeń korzystających z usług chmurowych nie jest zarządzanych lub nie raportuje statusu zgodności. Dostęp do części zasobów nie wymaga compliant device ani aplikacji objętej kontrolą.

Właściciel: Workplace

Termin: 30-60 dni

Stan faktyczny

158 urządzeń korzystających z usług chmurowych nie jest zarządzanych lub nie raportuje statusu zgodności. Dostęp do części zasobów nie wymaga compliant device ani aplikacji objętej kontrolą.

Scenariusz ryzyka i wpływ

Utrata, infekcja lub użycie prywatnego urządzenia może doprowadzić do niekontrolowanego pobrania danych. Organizacja ma ograniczoną zdolność zdalnego usunięcia danych i potwierdzenia poziomu zabezpieczeń.

Dowód audytowy

Źródło i obserwacja

Entra device inventory, Intune compliance export, sign-in logs oraz próbka dostępu do SharePoint. Dowód syntetyczny: EV-DEV-019.

Rekomendacja

Podzielić użytkowników i zasoby według ryzyka, wdrożyć enrollment lub app protection, zdefiniować standard zgodności, a dostęp do zasobów wysokiego ryzyka uzależnić od zarządzanego urządzenia. Zapewnić proces wyjątków dla kontraktorów.

Kryterium zamknięcia

Weryfikacja

Dla zasobów wysokiego ryzyka 100% aktywnych dostępów spełnia politykę urządzenia lub zatwierdzony wyjątek. Raport pokazuje liczbę wyjątków, właściciela i datę wygaśnięcia; test blokady niezgodnego urządzenia zakończony powodzeniem.

SEKCJA 07

Plan działań naprawczych 30/60/90

Horyzont	Działanie	Właściciel	Rezultat / dowód
0-30 dni	Właściciele i redukcja uprawnień aplikacji H-01	Security / IAM	Rejestr aplikacji, zatwierdzenia, test integracji
0-30 dni	Report-only i pilotaż brakujących zasad CA H-02	IAM	Macierz scenariuszy, logi pilotażu, decyzja CAB
0-30 dni	Segmentacja zasobów i urządzeń dla H-03	Workplace	Lista zasobów, polityka dostępu, grupa pilotażowa
31-60 dni	Recertyfikacja gości, uprawnień i wyjątków	Właściciele usług	Wyniki access review i decyzje ownerów
31-60 dni	Retencja, alerty i mierniki operacyjne	Security / SOC	Raport miesięczny, SLA alertów, test wyszukiwania
31-60 dni	Test odtworzenia danych SaaS	BCM / IT	Protokół testu, wynik RPO/RTO, działania korygujące
61-90 dni	Walidacja wszystkich ustaleń wysokich i średnich	Audyt / ownerzy	Dowody zamknięcia lub akceptacje ryzyka
61-90 dni	Cykliczny przegląd konfiguracji i zmian	Security	Kalendarz kontroli, dashboard, właściciele

Warunek powodzenia

Plan nie jest listą życzeń. Każde działanie ma właściciela, zależności, rezultat i dowód odbioru. Ryzyko, którego nie można usunąć w terminie, wymaga jawnej decyzji oraz daty ponownego przeglądu.

SEKCJA 08

Walidacja i kryteria odbioru

Rodzaj kontroli	Pytanie odbiorowe	Przykład dowodu
Konfiguracja	Czy ustawienie jest aktywne w oczekiwanym zakresie?	Eksport, zrzut konfiguracji, zapytanie Graph
Skuteczność	Czy kontrola blokuje lub wykrywa scenariusz ryzyka?	Próba funkcjonalna, alert, wynik sign-in
Właścicielstwo	Kto utrzymuje kontrolę i reaguje na wyjątek?	RACI, akceptacja ownera, wpis w rejestrze
Ciągłość	Czy kontrola jest przeglądana i testowana cyklicznie?	Protokół, ticket, dashboard, harmonogram
Ryzyko rezydualne	Co pozostaje po zmianie i kto to akceptuje?	Decyzja ryzyka z terminem ponownej oceny

Przykładowa karta zamknięcia

Pole	Wymagane uzupełnienie
ID ustalenia	H-01
Zmiana	Usunięto nadmiarowe role, odnowiono certyfikat, przypisano ownerów
Test	Integracja przeszła próbę; odrzucono próbę dostępu do wyłączonego zakresu
Dowód	EV-CLOSE-H01-01..04
Ryzyko rezydualne	Niskie - poświadczenie ważne 180 dni, alert przed wygaśnięciem
Akceptacja	Owner biznesowy, IAM, Security

SEKCJA 09

Rejestr dowodów i źródeł technicznych

ID	Źródło	Zakres	Data	Integralność / uwagi
EV-ID-001	Entra users export	Konta, status, typ, ostatnie logowanie	T0	CSV; SHA-256 w repozytorium audytu
EV-ROLE-002	Directory roles	Role, członkowie, eligible/active	T0	JSON; tryb read-only
EV-AUTH-003	Authentication methods	Rejestracja i metody MFA	T0	CSV; dane minimalizowane
EV-APP-004	Service principals	Uprawnienia app-only i właściciele	T0	JSON; bez sekretów
EV-CA-011	Conditional Access	Zasady, zakresy, wyjątki, report-only	T0	JSON + wyniki prób
EV-EXO-014	Exchange Online	Forwarding, reguły, ochrona domen	T0	Eksport PowerShell
EV-SPO-016	SharePoint/OneDrive	Udostępnianie i linki	T0	Eksport administracyjny
EV-DEV-019	Entra/Intune devices	Rejestracja, zgodność, systemy	T0	CSV; bez nazw użytkowników
EV-AUD-023	Unified Audit Log	Próbka zdarzeń i retencja	T0	Zapytanie i wynik kontrolny
EV-INT-027	Wywiady właścicielskie	Procesy, wyjątki, odpowiedzialności	T0+2	Notatka zatwierdzona przez rozmówcę

Zasady ochrony materiału

- minimalizacja: bez haseł, sekretów, tokenów i zbędnych danych osobowych;
- szyfrowany kanał przekazania i kontrola dostępu do repozytorium audytu;
- oznaczenie wersji oraz skróty plików istotnych dowodowo;
- retencja i bezpieczne usunięcie uzgodnione z klientem;
- oddzielenie dowodu źródłowego od publicznego lub zarządczego skrótu.

SEKCJA 10

Zakończenie i następne kroki

Profesjonalny raport ma prowadzić do decyzji, a nie kończyć projekt. Dlatego podsumowanie łączy ryzyko z właścicielem, koszt i wpływ ze sposobem wdrożenia, a rekomendację z mierzalnym kryterium odbioru.

Co otrzymuje klient

- podsumowanie dla kierownictwa z profilem ryzyka i decyzjami;
- pełny rejestr ustaleń oraz kontrole pozytywne;
- szczegółowe karty ustaleń z dowodami i scenariuszem wpływu;
- plan 30/60/90 z właścicielami, zależnościami i kryteriami odbioru;
- warsztat odbiorowy i opcjonalną walidację po wdrożeniu.

Ważne

Ten dokument jest publicznym wzorcem. Nie został wygenerowany z danych klienta, nie ujawnia wyników żadnego audytu i nie powinien być używany jako gotowa ocena innego środowiska.

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