SAMPLE SECURITY ASSESSMENT REPORT · ŚRODOWISKO TESTOWE

Przykładowy raport z audytu

Raport z audytu cyberbezpieczeństwa i AI Security fikcyjnej organizacji w środowisku testowym. Pokazuje strukturę i poziom szczegółowości raportu. Wszystkie nazwy, adresy i dane są fikcyjne.

ORGANIZACJA (FIKCYJNA)

Przykładowa Spółka Testowa sp. z o.o.

domena testowa: przyklad-testowy.example

WYKONAWCA

AI Business Lab

CLEARWISE sp. z o.o.

Podsumowanie dla zarządu

Audyt objął pocztę i domenę, środowisko Microsoft 365, stronę WordPress, kopie zapasowe, narzędzia AI używane przez zespół oraz agenta AI obsługującego zapytania ofertowe. Stwierdzono 14 ustaleń, w tym 2 krytyczne. Najpilniejsze: włączenie uwierzytelniania wieloskładnikowego dla administratorów i odseparowanie kopii zapasowych z testem odtworzenia. Oba ryzyka mogą prowadzić do przejęcia środowiska lub utraty danych bez możliwości odtworzenia.

2	4	5	3
Krytyczne	Wysokie	Średnie	Niskie

Decyzje dla zarządu

- Zatwierdzić obowiązkowe MFA dla wszystkich kont, w pierwszej kolejności administratorów.
- Zatwierdzić budżet na kopię zapasową odseparowaną od sieci firmowej i kwartalny test odtworzenia.
- Zatwierdzić politykę korzystania z AI i przeniesienie zespołu na konta firmowe.

01 Zakres i metoda

Pozycja	Opis
Okres	Środowisko testowe, prace w uzgodnionym oknie (przykład)
Systemy	Domena przyklad-testowy.example, Microsoft 365 (tenant testowy), strona WordPress, serwer plików, agent AI obsługi zapytań
Dostępy	Konta tylko do odczytu, agent AI na kopii z wyłączoną wysyłką
Standardy	CIS Controls, OWASP WSTG, OWASP Top 10 for LLM Applications
Ograniczenia	Bez testów obciążeniowych i socjotechniki; sieć wewnętrzna poza zakresem

02 Lista ustaleń

ID	Poziom	Ustalenie	Obszar	Status
K-01	Krytyczny	Konta administratorów bez uwierzytelniania wieloskładnikowego	Microsoft 365	Do naprawy
K-02	Krytyczny	Kopia zapasowa bez separacji i bez testu odtworzenia	Serwer plików	Do naprawy

PRZYKŁAD

ID	Poziom	Ustalenie	Obszar	Status
W-03	Wysoki	Brak egzekwowanej polityki DMARC (p=none)	Domena	Naprawione
W-04	Wysoki	Nieaktualne wtyczki WordPress ze znanymi podatnościami	Strona	Naprawione
W-05	Wysoki	Agent AI: prompt injection pośredni prowadzi do wysyłki e-mail	Agent obsługi zapytań	Do naprawy
W-06	Wysoki	Aplikacje OAuth z pełnym dostępem do skrzynek, niezatwierdzone	Microsoft 365	W planie
S-07	Średni	Prywatne konta narzędzi AI używane do danych klientów	Narzędzia AI	W planie
S-08	Średni	Panel administracyjny WordPress dostępny z całego internetu	Strona	W planie
S-09	Średni	Aktywne konta dwóch byłych pracowników bez licencji	Microsoft 365	Naprawione
S-10	Średni	Rekord SPF z miękkim odrzuceniem (~all)	Domena	W planie
S-11	Średni	Brak spisanej procedury zgłaszania incydentów	Organizacja	W planie
N-12	Niski	Brak nagłówków Content-Security-Policy i HSTS	Strona	W planie
N-13	Niski	Brak pliku security.txt	Strona	W planie
N-14	Niski	Logi logowania przechowywane krócej niż 30 dni	Microsoft 365	W planie

PRZYKŁAD

03 Ustalenia szczegółowe (wybór)

Krytyczny K-01 · Konta administratorów bez uwierzytelniania wieloskładnikowego

Obszar	Microsoft 365
Opis	3 z 4 kont z rolą Global Administrator nie mają zarejestrowanej metody MFA. Brak zasad dostępu warunkowego wymuszających MFA.
Dowód	Eksport ról i stanu rejestracji MFA z centrum administracyjnego (zrzut w załączniku A, przykład).
Wpływ	Przejęcie jednego hasła administratora daje pełną kontrolę nad pocztą, plikami i kontami całej organizacji.
Rekomendacja	Wymusić MFA (preferowane klucze FIDO2 lub aplikacja) dla administratorów, osobne konta administracyjne, zasady dostępu warunkowego, blokada starszych protokołów uwierzytelniania.
Odniesienie	CIS Controls 6.3, 6.5

Krytyczny K-02 · Kopia zapasowa bez separacji i bez testu odtworzenia

Obszar	Serwer plików
Opis	Kopia wykonywana na dysk sieciowy dostępny z tych samych kont co serwer. Brak zapisu z testu odtworzenia.
Dowód	Konfiguracja zadania kopii i uprawnień udziału (załącznik B, przykład).
Wpływ	Ransomware szyfrujący serwer zaszyfruje także kopię. Odtworzenie danych może być niemożliwe.
Rekomendacja	Kopia odseparowana (niezmienialna lub poza domeną), reguła 3-2-1, kwartalny test odtworzenia z protokołem.
Odniesienie	CIS Controls 11.1-11.5

PRZYKŁAD

Wysoki

W-05 · Agent AI: prompt injection pośredni prowadzi do wysyłki e-mail

Obszar	Agent AI obsługi zapytań
Opis	Agent czyta treść maili klientów i ma narzędzie wysyłki e-mail bez ograniczenia odbiorców. Instrukcja ukryta w treści wiadomości testowej spowodowała przygotowanie wysyłki cennika na adres spoza domeny klienta.
Dowód	Zapis rozmowy testowej i wywołania narzędzia `send_email(to: "test@example.com")` na kopii agenta (załącznik C, przykład).
Wpływ	Wyciek dokumentów handlowych lub danych klientów przez wiadomość przygotowaną przez atakującego.
Rekomendacja	Ograniczyć odbiorców narzędzia do nadawcy wątku, wysyłkę załączników zatwierdza człowiek, oddzielić treść zewnętrzną od instrukcji, rejestrować wywołania narzędzi.
Odniesienie	OWASP LLM01 (Prompt Injection), LLM06 (Excessive Agency)

04 Plan naprawczy

Kolejność	Działanie	Właściciel	Ustalenia
1	MFA dla administratorów, dostęp warunkowy	IT	K-01
2	Kopia odseparowana i test odtworzenia	IT	K-02
3	Ograniczenie narzędzia e-mail agenta, akceptacja człowieka	Zespół AI / dostawca	W-05
4	Przegląd aplikacji OAuth, polityka zgód	IT	W-06
5	Polityka AI i konta firmowe	Zarząd / IT	S-07
6	Ograniczenie panelu WordPress, nagłówki bezpieczeństwa	Agencja WWW	S-08, N-12

PRZYKŁAD

Dokument przykładowy. Organizacja, domena, systemy i ustalenia są fikcyjne i służą pokazaniu struktury raportu AI Business Lab. Nie odnoszą się do żadnego klienta.