ZeroPEN

Testy penetracyjne Veeam Backup & Recovery

“Zero kompromisów.” — Znajdź to, zanim atakujący zniszczy Twoje backupy Veeam.

Problem: Veeam to standard w backupie klasy enterprise — i cel numer jeden dla atakujących. Podatności takie jak CVE-2024-40711 i CVE-2023-27532 były aktywnie wykorzystywane przez grupy ransomware, w tym Akira i Fog, do przejmowania serwerów Veeam i usuwania backupów.

Co robi ZeroPEN

- Kontrolowana symulacja łańcucha ataku (kill-chain) ransomware wymierzona w Veeam.
- Obiera na cel serwer VBR, Enterprise Manager, Veeam ONE, bazę konfiguracyjną (config DB) i repozytoria.
- Weryfikuje niezmienność, RBAC i poziom aktualizacji; tworzy kartę oceny hardeningu Veeam.
- Dowodzi możliwości neutralizacji backupu i eksfiltracji — bez wyrządzania rzeczywistych szkód.

Cztery warstwy, zero kompromisów

ZeroMON Monitorowanie	**ZeroTAM** Doradztwo	**ZeroPEN** Pentest	**ZeroVault** Cloud Storage

Zakres regulacyjny

BDDK Regulacja IT Art.45/51/17	SPK III-35.1 Ciągłość działania
DORA Art.11/12/17 TLPT	KVKK Art.12 bezpieczeństwo danych
GDPR Art.25/32/33	ISO 27001 / NIST A.12.3 / SP 800-115

Rezultaty

Podsumowanie dla kadry zarządzającej · raport techniczny zmapowany na CWE/CVE · karta oceny hardeningu Veeam · kill-chain MITRE ATT&CK · macierz mapowania regulacyjnego · priorytetyzowana remediacja · ponowny test.

Rozpocznij: Wypełnij formularz zakresu, a wkrótce dostarczymy dopasowaną procedurę testową.

www.backupsec.com · info@backupsec.com · BackupSec