ZeroPEN

Penetrační testování Veeam Backup & Recovery

“Nula kompromisů.” — Najděte to dřív, než útočník zničí vaše Veeam backupy.

Problém: Veeam je standardem pro enterprise backup — a cíl číslo jedna pro útočníky. Zranitelnosti jako CVE-2024-40711 a CVE-2023-27532 aktivně využívají ransomwarové skupiny včetně Akira a Fog k ovládnutí Veeam serverů a mazání backupů.

Co ZeroPEN dělá

- Řízená simulace ransomwarového kill-chainu proti Veeamu.
- Cílí na VBR server, Enterprise Manager, Veeam ONE, konfigurační DB a repozitáře.
- Ověřuje immutability, RBAC a úroveň patchů; vytváří Veeam hardening scorecard.
- Prokazuje schopnost neutralizace backupů a exfiltrace — bez způsobení skutečných škod.

Čtyři vrstvy, nula kompromisů

ZeroMON Monitoring	**ZeroTAM** Poradenství	**ZeroPEN** Pentest	**ZeroVault** Cloud storage

Regulatorní pokrytí

BDDK IT regulace Art.45/51/17	SPK III-35.1 kontinuita provozu
DORA Art.11/12/17 TLPT	KVKK Art.12 zabezpečení dat
GDPR Art.25/32/33	ISO 27001 / NIST A.12.3 / SP 800-115

Výstupy

Manažerské shrnutí · technický report mapovaný na CWE/CVE · Veeam hardening scorecard · MITRE ATT&CK kill-chain · matice regulatorního mapování · prioritizovaná náprava · retest.

Jak začít: Vyplňte formulář pro vymezení rozsahu a my vám krátce poté dodáme testovací proceduru na míru.

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