ZeroPEN

Veeam Backup & Recovery Penetrationstesting

“Null Kompromisse.” — Finden Sie es, bevor der Angreifer Ihre Veeam-Backups zerstört.

Das Problem: Veeam ist der Standard für Enterprise-Backup — und das Ziel Nummer eins der Angreifer. Schwachstellen wie CVE-2024-40711 und CVE-2023-27532 wurden von Ransomware-Gruppen wie Akira und Fog aktiv ausgenutzt, um Veeam-Server zu übernehmen und Backups zu löschen.

Was ZeroPEN leistet

- Kontrollierte Simulation der Ransomware-Kill-Chain gegen Veeam.
- Nimmt den VBR-Server, Enterprise Manager, Veeam ONE, die Konfigurationsdatenbank und Repositories ins Visier.
- Überprüft Immutability, RBAC und Patch-Level; erstellt eine Veeam-Hardening-Scorecard.
- Weist die Fähigkeit zur Backup-Neutralisierung und Exfiltration nach — ohne realen Schaden anzurichten.

Vier Ebenen, null Kompromisse

ZeroMON	ZeroTAM	ZeroPEN	ZeroVault
Monitoring	Beratung	Pentest	Cloud Storage

Regulatorische Abdeckung

BDDK IT-Regulierung Art.45/51/17	SPK III-35.1 Geschäftskontinuität
DORA Art.11/12/17 TLPT	KVKK Art.12 Datensicherheit
GDPR Art.25/32/33	ISO 27001 / NIST A.12.3 / SP 800-115

Liefergegenstände

Management-Zusammenfassung · technischer Bericht mit CWE/CVE-Zuordnung · Veeam-Hardening-Scorecard · MITRE ATT&CK-Kill-Chain · regulatorische Mapping-Matrix · priorisierte Behebung · Retest.

So starten Sie: Füllen Sie das Scope-Formular aus, und wir liefern kurz darauf ein maßgeschneidertes Testverfahren.

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