ZeroPEN

Penetrationstestning av Veeam Backup & Recovery

“Noll kompromisser.” — Hitta det innan angriparen förstör dina Veeam-backuper.

Problemet: Veeam är standarden för företagsbackup — och angriparens främsta mål. Brister som CVE-2024-40711 och CVE-2023-27532 har aktivt utnyttjats av ransomware-grupper inklusive Akira och Fog för att ta över Veeam-servrar och radera backuper.

Vad ZeroPEN gör

- Kontrollerad simulering av ransomware-kedjan (kill-chain) mot Veeam.
- Riktar in sig på VBR-servern, Enterprise Manager, Veeam ONE, konfigurationsdatabasen och repositoryer.
- Verifierar oföränderlighet, RBAC och patchnivå; producerar ett Veeam-härdningsscorecard.
- Bevisar förmåga till backup-neutralisering och exfiltrering — utan att orsaka verklig skada.

Fyra lager, noll kompromisser

ZeroMON Övervakning	**ZeroTAM** Rådgivning	**ZeroPEN** Pentest	**ZeroVault** Molnlagring

Regulatorisk täckning

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

Leveranser

Sammanfattning för ledningen · teknisk rapport mappad mot CWE/CVE · Veeam-härdningsscorecard · MITRE ATT&CK kill-chain · matris för regulatorisk mappning · prioriterad åtgärdsplan · omtest.

Kom igång: Fyll i scope-formuläret så levererar vi en skräddarsydd testprocedur strax därefter.

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