ZeroPEN

Penetration Testing di Veeam Backup & Recovery

"Zero compromessi." — Individualo prima che l'attaccante distrugga i tuoi backup Veeam.

Il problema: Veeam è lo standard per il backup aziendale — e il bersaglio numero uno degli attaccanti. Falle come CVE-2024-40711 e CVE-2023-27532 sono state sfruttate attivamente da gruppi ransomware come Akira e Fog per prendere il controllo dei server Veeam ed eliminare i backup.

Cosa fa ZeroPEN

- Simulazione controllata della kill-chain del ransomware contro Veeam.
- Prende di mira il server VBR, Enterprise Manager, Veeam ONE, il config DB e i repository.
- Verifica immutabilità, RBAC e livello di patch; produce una scorecard di hardening Veeam.
- Dimostra la capacità di neutralizzazione dei backup e di esfiltrazione — senza causare danni reali.

Quattro livelli, zero compromessi

ZeroMON Monitoraggio	**ZeroTAM** Consulenza	**ZeroPEN** Pentest	**ZeroVault** Cloud Storage

Copertura normativa

BDDK Normativa IT Art.45/51/17	SPK III-35.1 Continuità Operativa
DORA Art.11/12/17 TLPT	KVKK Art.12 sicurezza dei dati
GDPR Art.25/32/33	ISO 27001 / NIST A.12.3 / SP 800-115

Deliverable

Executive summary · report tecnico mappato CWE/CVE · scorecard di hardening Veeam · kill-chain MITRE ATT&CK · matrice di mappatura normativa · remediation prioritizzata · retest.

Inizia: Compila il form di scoping e ti consegneremo poco dopo una procedura di test su misura.

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