ZeroPEN

Test de penetración de Veeam Backup & Recovery

“Cero concesiones.” — Encuéntralo antes de que el atacante destruya tus backups de Veeam.

El problema: Veeam es el estándar para el backup empresarial — y el objetivo número uno del atacante. Vulnerabilidades como CVE-2024-40711 y CVE-2023-27532 han sido utilizadas activamente por grupos de ransomware como Akira y Fog para tomar el control de los servidores Veeam y eliminar los backups.

Qué hace ZeroPEN

- Simulación controlada de la kill-chain de ransomware contra Veeam.
- Se dirige al servidor VBR, Enterprise Manager, Veeam ONE, la base de datos de configuración y los repositorios.
- Verifica la inmutabilidad, RBAC y el nivel de parches; produce un scorecard de hardening de Veeam.
- Demuestra la capacidad de neutralización de backups y de exfiltración — sin causar daños reales.

Cuatro capas, cero concesiones

ZeroMON Monitorización	**ZeroTAM** Asesoría	**ZeroPEN** Pentest	**ZeroVault** Cloud Storage

Cobertura normativa

BDDK Normativa de IT Art.45/51/17	SPK III-35.1 Continuidad de negocio
DORA Art.11/12/17 TLPT	KVKK Art.12 seguridad de datos
GDPR Art.25/32/33	ISO 27001 / NIST A.12.3 / SP 800-115

Entregables

Resumen ejecutivo · informe técnico mapeado a CWE/CVE · scorecard de hardening de Veeam · kill-chain de MITRE ATT&CK · matriz de mapeo normativo · remediación priorizada · retest.

Empieza ahora: Completa el formulario de alcance y poco después te entregaremos un procedimiento de prueba a medida.

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