ZeroPEN

Veeam Backup & Recovery Penetratietesten

"Zero compromise." — Vind het voordat de aanvaller uw Veeam-backups vernietigt.

Het probleem: Veeam is de standaard voor enterprise backup — en het doelwit nummer één van aanvallers. Kwetsbaarheden zoals CVE-2024-40711 en CVE-2023-27532 zijn actief misbruikt door ransomwaregroepen als Akira en Fog om Veeam-servers over te nemen en backups te verwijderen.

Wat ZeroPEN doet

- Gecontroleerde simulatie van de ransomware-kill-chain tegen Veeam.
- Richt zich op de VBR-server, Enterprise Manager, Veeam ONE, config-DB en repositories.
- Verifieert immutability, RBAC en patchniveau; levert een Veeam-hardening-scorecard.
- Bewijst het vermogen tot backup-neutralisatie en -exfiltratie — zonder echte schade te veroorzaken.

Vier lagen, zero compromise

ZeroMON Monitoring	**ZeroTAM** Advies	**ZeroPEN** Pentest	**ZeroVault** Cloud Storage

Dekking van regelgeving

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

Opleveringen

Managementsamenvatting · technisch rapport gekoppeld aan CWE/CVE · Veeam-hardening-scorecard · MITRE ATT&CK-kill-chain · matrix met koppeling aan regelgeving · geprioriteerde remediatie · hertest.

Aan de slag: Vul het scopeformulier in en wij leveren kort daarna een op maat gemaakte testprocedure.

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