ZeroPEN

Veeam Backup & Recovery Penetration Testing

“Zero compromise.” Find it before the attacker destroys your Veeam backups.

The problem: Veeam is the standard for enterprise backup, and the attacker’s number-one target. Flaws like CVE-2024-40711 and CVE-2023-27532 have been actively used by ransomware groups including Akira and Fog to take over Veeam servers and delete backups.

What ZeroPEN does

- Controlled simulation of the ransomware kill-chain against Veeam.
- Targets the VBR server, Enterprise Manager, Veeam ONE, config DB and repositories.
- Verifies immutability, RBAC and patch level; produces a Veeam hardening scorecard.
- Proves backup-neutralization and exfiltration capability, without causing real damage.

Five layers, zero compromise

ZeroMON	ZeroTAM	ZeroPEN	Stork365	ZeroVault
Monitoring	Advisory	Pentest	M365 Backup	Cloud Storage

Regulatory coverage

BDDK IT Regulation Art.45/51/17	SPK III-35.1 Business Continuity
DORA Art.11-12, 24-25 (not an Art.26 TLPT)	KVKK Art.12 data security
GDPR Art.25/32/33	ISO 27001 / NIST A.12.3 / SP 800-115

Deliverables

Executive summary · CWE/CVE-mapped technical report · Veeam hardening scorecard · MITRE ATT&CK kill-chain · regulatory mapping matrix · prioritized remediation · retest.

Get started: Complete the scope form and we’ll deliver a tailored test procedure shortly thereafter.

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