

Alanata TALKS: Veeam a ExaGrid – zladený tandem pre ochranu zálohovaných dát

Panelová diskusia

Ransomware v roku 2023

In 2023 within EMEA:



Paid and were able to recover their data from the attack



Paid but could not recover data lost in the attack



Recovered *without paying* the ransom that was demanded



Cyber is the new disaster

KATEGÓRIA	DISASTER RECOVERY	CYBER RECOVERY
Čas obnovy	Limitne blízke 0, RTO	Spoľahlivé a rýchle
Bod obnovy	Ideálne nepretržite, RPO	Primárne denné
Povaha katastrofy	Povodeň, výpadok elektriny, ľudský faktor	Kybernetický útok, cielený
Vplyv katastrofy	Regionálne, metropolitné	Globálne, celopodnikové
Topológia	Prepojená	Izolovaná
Povaha obnovy	Komplexná, všetky dáta, aplikácie, databázy	Selektívna, zahŕňa základné/nevyhnutné služby
Proces obnova	Štandardný DR proces/obnova, prepnutie do záložného DC	Iteratívne, selektívne zotavenie infraštruktúry



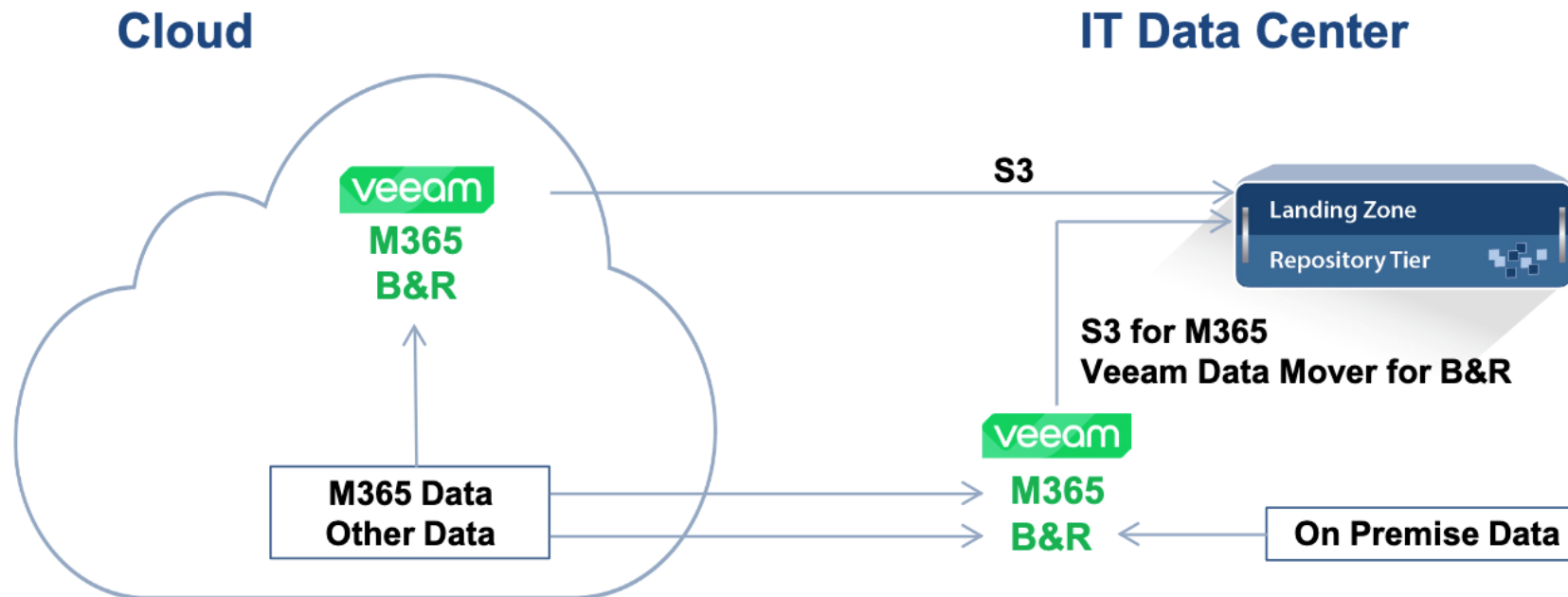
Best Practices pre zálohovanie a obnovu

- Č. 1: Zálohujte správne údaje správnym spôsobom (zálohovanie s ohľadom na aplikácie, integrácia snapshots úložiska atď.)
- Č. 2: Používajte nemenné záložné úložisko (hardened repository, nemenný S3, WORM, zariadenia s dedup)
- Č. 3: Testujte svoje zálohy a kontrolujte ich stav obnoviteľnosti
- Č. 4: Zabezpečte, aby bol hardvér dostatočne rýchly na zálohovanie a obnovu
- Č. 5: Vyberte si správny režim obnovy LAN free, SAN, granular atd.
- č. 6: Pripravte si náhradný hardvér
- č. 7: Vyhnite sa vajce/sliepka problému
- č. 8: Otestujte plán obnovy po havárii
- č. 9: Umožnite vlastníkom aplikácií využívať samoobslužné funkcie obnovy
- č. 10: Udržujte zálohovacie prostredie aktuálne

Ochrana dát spoločnosti začína na perimetri, pokračuje edukáciou zamestnancov, monitorovaním anomálií a disaster recovery a cyber recovery plánom.



Veeam Microsoft 365 S3 to Exagrid



Veeam Security and Compliance Analyzer

Security & Compliance Analyzer

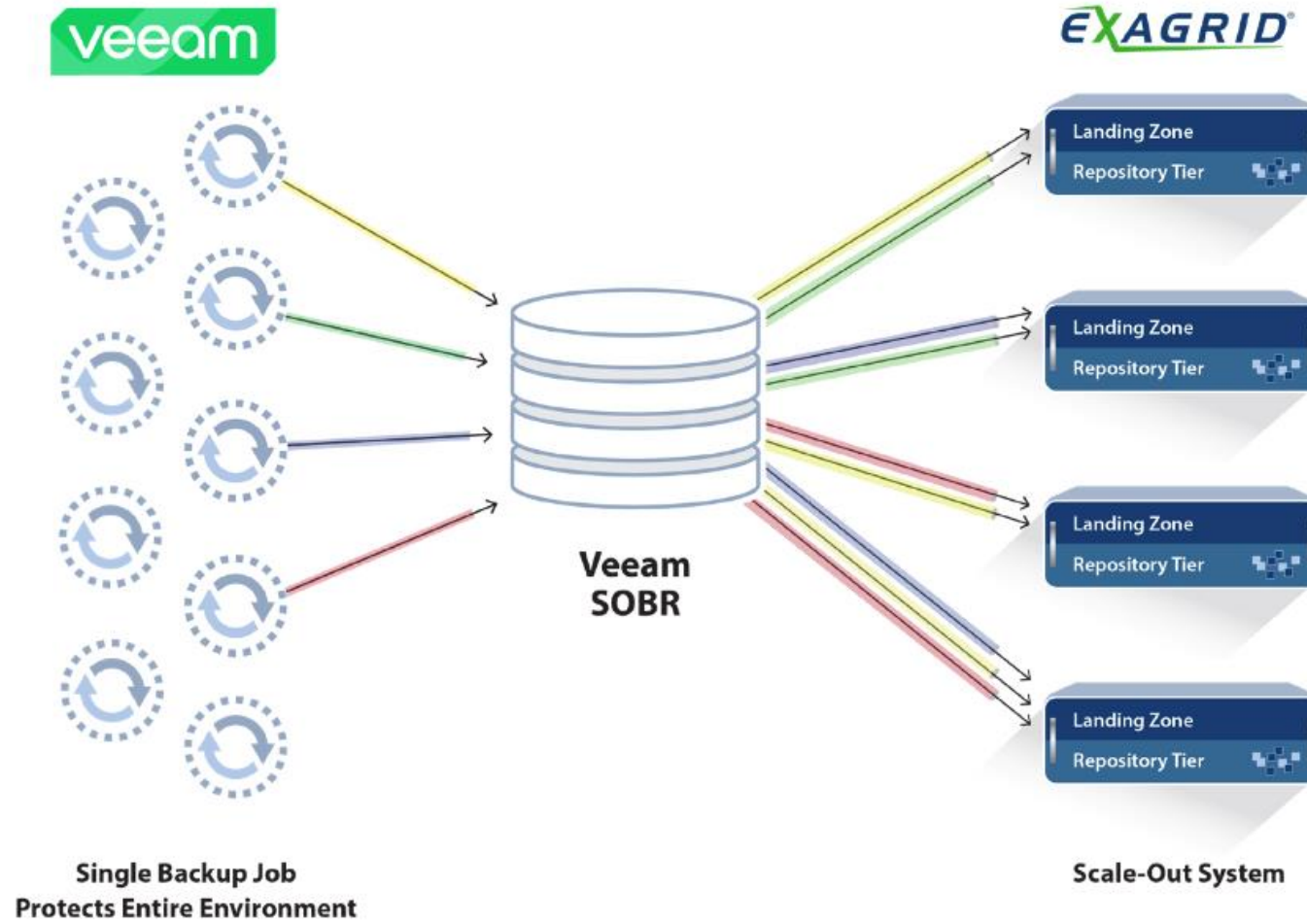
The following best practices are guidelines from data protection and cyber-security experts. Not following them exposes your backup infrastructure to significant risks and reduces chances of successful recovery following a cyber attack, a natural disaster or a hardware malfunction.

Best Practice	Status
Backup infrastructure security	
Remote Desktop Service (TermService) should be disabled	✗ Not implemented
Remote Registry service (RemoteRegistry) should be disabled	✗ Not implemented
Windows Remote Management (WinRM) service should be disabled	✗ Not implemented
Windows Firewall should be enabled	✗ Not implemented
WDigest credentials caching should be disabled	✓ Passed
Web Proxy Auto-Discovery service (WinHttpAutoProxySvc) should be disabled	✗ Not implemented
Deprecated versions of SSL and TLS should be disabled	⚠ Unable to detect
Windows Script Host should be disabled	✓ Passed
SMBv1 protocol should be disabled	✓ Passed
Link-Local Multicast Name Resolution (LLMNR) should be disabled	✗ Not implemented
SMBv3 signing and encryption should be enabled	✗ Not implemented
Product configuration	
MFA for the backup console should be enabled	✗ Not implemented
Immutable or offline (air gapped) media should be used	✓ Passed
Password loss protection should be enabled	✗ Not implemented
Backup server should not be a part of the production domain	⚠ Unable to detect
Email notifications should be enabled	✗ Not implemented

Buttons: Analyze, Schedule..., Suppress, Reset, Reset All, Last run..., Close, Copy to Clipboard



Veeam Scale-Out Backup Repository (SOBR)



Kyberhygiena zálohovacieho prostredia

- založte a diverzifikujte pamäťové médium, aby ste predišli jedinému bodu zlyhania (SPOF)
- nasledujte princíp ukladania záloh 3-2-1, ktorý hovorí o troch kópiách dát (1 x produkčné dáta a 2 x zálohované kópie) na dvoch rôznych médiách (napr. disk a páska) s jednou kópiou mimo primárneho dátového centra na obnovu po havárii + **jedna kópia CyberVault**
- aktualizujte SW serverov, používajte najnovšie patche a firmware,
- implementujte zásadu najmenších oprávnení pre používateľské účty,
- sledujte sieťovú aktivitu a systémové protokoly,
- sledujte záznamy o udalostiach, aby ste identifikovali anomálie,
- použite kombináciu filtrovania IP, systému detekcie narušenia (IDS) a systému prevencie narušenia (IPS),
- implementujte segmentáciu siete a rozdeľovanie údajov, aby ste minimalizovali vplyv potenciálneho útoku ransomware,
- auditujte systémy v pravidelných intervaloch.
- vzdelávajte zamestnancov**

"3-2-1" Backup Strategy



At least three sets of your data



Store two copies on different storage types



Keep one copy off-site



Alanata

Technology Meets Business

Alanata a.s.

Einsteinova Business Center
Krasovského 14
851 01 Bratislava 5
Slovenská republika

www.alanata.sk