



Od útoku k obnove: Úloha moderného zálohovania v kyberbezpečnosti

Peter Šingliar
CDP, spol. s r.o.

CDP

DELLTechnologies

veeAM

vmware

Nie je otázkou „či“, ale „kedy“

Ani dobrá ochrana nemusí stačiť

- phishing a kompromitované účty
- zneužitie legitímnych prístupov
- útoky sú rýchle a čoraz sofistikovanejšie alebo
- mesiace sledovania a plánovania pred vykonaním poslednej fázy útoku

Dopad útoku na firmu

- nedostupné alebo poškodené dáta
- výpadok systémov a prevádzky
- finančné škody
- reputačné škody
- porušenie zákonov (termíny)

Zlatý štandard zálohovania 3-2-1-0

3

KÓPIE DÁT



Produkcia



Lokálny Backup



Cloud Záloha

2

RÔZNE MÉDIÁ



Disk



S3 / Paska

1

OFFSITE LOKALITA



Mimo Lokality

0

ŽIADNE CHYBY



Testovanie



Obnova

CDP

DELL Technologies

veeAM

vmware®



Ako Veeam posúva zálohovanie na vyššiu úroveň?



Záloha ako súčasť bezpečnosti

- detekcia ransomvéru a anomálií
- kontrola integrity dát



Rýchla a automatizovaná obnova

- instant recovery
- granular restore
- automatizované DR scenáre



Ochrana pred útokom

- immutable zálohy (S3 Object Lock)
- ochrana aj pri kompromitácii admina



Overiteľnosť (0 errors)

- testovanie obnovy v sandboxe
- reporty a validácia



Monitoring a prehľad

- alerty, reporting
- plná kontrola nad zálohami

Moderné zálohy = posledná línia obrany

💡 Zálohovanie je súčasťou kyberbezpečnosti

- nie len IT operácia, ale biznis kritická funkcia
- Cieľ: návrat do prevádzky
- Rozhoduje o kontinuite prevádzky firmy

👉 „Moderné zálohovanie nie je o tom, kde dáta uložíme, ale ako rýchlo a bezpečne (a či vôbec) ich vieme obnoviť po útoku.“

CDP

DELL Technologies

VEEAM

vmware®

Posledná línia, ale prvá „vec“ na muške

- Úspechom útočníka je znemožnenie obnovy zo záloh
 - vymazanie záloh, poškodenie média (datastore, RAID)
 - zakryptovanie záloh
 - „ten istý“ ransomvér, ktorým kryptovali produkciu
 - menej prozaické možnosti
 - manipulácia s nastavením zálohovania
- Otvárate útočníkovi cestu k zálohám?
 - zálohovacie servery „zaradené v doméne“
 - zálohovacia infraštruktúra dostupná z bežných podsietí
 - opakujúce sa heslá
 - minimálny monitoring zálohovania



Najčastejšie problémy v praxi

- Zálohovanie (proces) nikto nekontroluje
- DR plán neexistuje / je zastaraný
- obnova sa nikdy netestovala
- zodpovednosť nie je jasná
- zálohy nie sú uložené v immutable/nezmazateľnej forme

Immutable backup a S3 úložisko

🔒 Nemennosť (immutability) ako ochrana záloh

- zálohy uložené v režime **immutable (WORM)**
- dáta nie je možné zmazať, prepísať, upraviť (ani administrátorom)
- ochrana aj pri kompromitovaní účtov

☁ Naše riešenie: S3 cloud backup (CDP)

- objektové úložisko s podporou **immutability**
- zálohy fyzicky oddelené od infraštruktúry zákazníka
- uloženie mimo lokality (offsite)
- vysoká odolnosť voči ransomvéru

CDP

DELL Technologies

VEEAM

vmware®

Oddelenie zálohovacej infraštruktúry od „bežnej“ siete

- segmentácia sietí
- vyňatie zálohovacej infraštruktúry z AD (domény)
- firewall ochrana proxy serverov zálohovacej infraštruktúry
- správa zálohovacej (aj virtualizačnej!) infraštruktúry z iného zariadenia, ako admin bežne používa pri práci
- „hardening“ zálohovacej infraštruktúry, ak nie je možná segmentácia
- vyňatie virtualizačnej infraštruktúry z AD (domény) je nad tým všetkým

Monitoring úspešnosti zálohovania a test obnoviteľnosti

- mailovanie je fajn, ale nestačí
- test obnoviteľnosti pred auditom „aspoň raz ročne“?
 - už aj to je u mnohých úspech, ale nestačí
 - aj po zmene hesiel
 - aj po update infraštruktúry (VMware, Hyper-V, Veeam...)
 - aj po upgrade SQL databázy
 - aj po upgrade OS (Windows, Linux, ...)
- záloha bez testu obnovy je iba **optimizmus.zip**

Last Edited ↑

3691 days ago

3690 days ago

3686 days ago

3469 days ago

3469 days ago

3279 days ago

2512 days ago

2370 days ago

2251 days ago

2251 days ago

1614 days ago

CDP

DELL Technologies

VEEAM

vmware®

Disaster recovery plán

- čo a ako zálohujem, kam zálohujem, kedy zálohujem
 - čo sa deje, ak musím obnovovať
 - čo obnovujem, keď mám obnoviť jeden logický celok
 - kto je zapojený do obnovy zo zálohy/repliky
-
- čo obetujem za to, že vyberiem konkrétnu metódu obnovy
 - RPO - maximálna prípustná strata dát (koľko dát stratím)
 - RTO - max. prípustný čas obnovy prevádzky (ako dlho budem stáť)

Zodpovednosť a komunikácia

- kto rozhodne o tom, čo obetujeme pri obnove?
 - manažment oboznámený s existenciou problematiky RPO/RTO
 - odhadnuté straty
 - odhadnutá prácnosť
- kto informuje zamestnancov, keď IT team pracuje na obnove?
 - bežné komunikačné kanály (e-mail, intranet, firemný chat)
 - záložné komunikačné kanály (sms brána, telefonáty, od dverí k dverám)
- kto schváli prácu nadčas, nočnú, striedanie pri obnove?

Disaster Recovery ako služba

- návrh a aktualizácia DR plánov
- monitoring záloh
- pravidelné testy obnovy
- asistencia pri incidente
- clean room (!)

CDP

DELLTechnologies

VEEAM

vmware



Veeam v13: silný bezpečnostný argument

- **MFA pre Veeam konzolu**
 - Samotné ukradnuté heslo nestačí na prístup do konzoly.
- **Citlivé operácie musia schváliť 2 osoby**
 - Mazanie backupov, odobratie repozitára či zmeny používateľov/MFA vyžadujú dodatočné schválenie.
- **Security Officer zvyšuje dôveru**
 - Dodávateľ alebo admin nevie sám vykonať kritickú zmenu bez potvrdenia druhej role.



DELL Technologies

VEEAM

vmware®



Veeam Recon + odporúčaná bezpečnostný štandard

- **Detekcia podozrivej aktivity**

Brute-force, neznáme prihlásenia, anomálne spojenia, manipulácia so službami či exfiltrácia dát.

- **Denný scan backup infra**

Zbiera metadáta z event logov, registrov, procesov, služieb a sieťových spojení.

- **Coveware portál + MITRE ATT&CK**

Incidenty sa vyhodnocujú v Triage Inboxe a mapujú na známe techniky útočníkov.

- **Nie je to AV/EDR**

Je to doplnková vrstva threat huntingu a forenznej viditeľnosti pre backup infraštruktúru.



Bezpečnostná hodnota opatrení

Opatrenie	Hodnota
Immutable repository (nemenné zálohy lokálne)	10/10
Offline/S3 Object Lock	10/10
MFA	9/10
Security Officer approval	9/10
Oddelené AD od zálohovacej infraštruktúry	9/10
Veeam Recon	6/10
Antivírus	5/10



Ste pripravení na obnovu?

- viete, ako dlho trvá obnova vo Vašich podmienkach?
- máte otestovaný DR plán?
- prežili by vaše zálohy útok?

CDP

DELLTechnologies

VEEAM

vmware

Ďakujem za pozornosť

Šéf: „Máme zálohy?“

Admin: „Máme.“

Šéf: „A fungujú?“

Admin: „To je veľmi osobná otázka.“

www.cdp.sk

sales@cdp.sk

CDP

DELL Technologies

VEEAM

vmware