‘World Backup Day Pledge’ – Menti-e adatait?

World Backup Day: 2021. március 31.


WORLD BACKUP DAY
NE LÉGY ÁPRILIS BOLONDJA!
Készülj fel! Készíts másolatot a fájljaidról március 31-én.
MI AZ A BIZTONSÁGI MENTÉS? ↓
ESKÜDJ FÖL! →

Tartalom

Mentünk-e?

- **Azért mentünk, mert egy feladatot akarunk teljesíteni ('kipipálni'), vagy mert önmagunkat akarjuk álltatni, és ez jól esik magunknak vagy főnökünknek,**

- **vagy azért mentünk, hogy baj esetén valóban használát is vegyük a mentésnek?**

Alapvető backup problémák

0. Backup probléma: Nem tudjuk van-e mentés; nem tudjuk mit csinálunk; nem ismerjük kellően a végzett mentést; nem értünk a mentéshez

1. Backup probléma: Nem készült mentés

2. Backup probléma: Nincs mentés

Például:

- törlődött, törlésre került, felül lett írva, megsemmisült stb.

3. Backup probléma: Nem elérhető a mentés

Például:

- …

4. Backup probléma: Nem visszaállítható a mentés
– részben vagy egészében visszaállíthatatlan –

Például:

- titkosított a mentés, de nincs meg a titkosítókulcs,
- nincs mivel olvasni a backup médiát,
- nincs mire visszaállítani,
- stb.

5. Backup probléma: Nem érdemes vagy nem célszerű visszaállítani

Például:

- malware fertőzött,
- hibás állapotról készült (lásd idevonatkozóan még az 6-ös problémakört).

6. Backup probléma: Nem megfelelő a mentés

- hibás adatokat tartalmaz
- hiányos
  - inkomplett (pl. inkompletten futott le, és nem került megismétlésre)
  - nem kerültek mentésre bizonyos adatok
- nem elég friss
- korrupt
- inkonzisztens

7. Backup probléma: Lassú a visszaállítás

Backup üzemeltetési problémák

1. Nem indul a backup job
2. Hibásan fut le a backup job
3. Inkomplett a készült backup
4. Nem verifikáltható a backup vagy nem sikeres a verifikáció
5. Lassú a backup

Sokféle más üzemeltetési probléma is adódhat, a fentiek a legtipikusabb problémák.

Biztonsági problémák

1. A backup integritása nem védett
   1.1. illetéktelen hozzáférhetnek a mentéshez
      1.1.1. zsarolóvírus tönkreteheti a mentést
2. A backup tárolása nem elég biztonságos
   2.1. illetéktelen hozzáférhet a mentéshez
      2.1.1. a bizalmasság sérülhet
      2.1.2. megrongálhatják, tönkretehetik, módosíthatják a mentést
         2.1.2.1. ismét kiemeljük a zsarolóvírus-veszélyt
3. A backup elérhetősége nem megfelelő
   3.1. rendelkezésre-állása
      3.1.1. elérési problémák
      3.1.2. visszaállítási sebesség problémák
4. A biztonság nem verifikálható
   4.1. a mentési eljárás ezt nem tudj, vagy nem megfelelő szinten tudja biztosítani
5. A biztonság nem verifikált
   5.1. ha biztosítható is, a verifikáció nem történt meg
6. A backup bizalmassága nem kellően biztosított
7. A biztonság nem auditált
   7.1. akár lehet verifikált is, a tervezettség, az üzemeltetés, az ellenőrzések nem ellenőrzöttek, vagy csak egy szinten (pl. az üzemeltető rendszergazdák által) ellenőrzöttek (az üzemeltetők munkája már nem ellenőrzött)

Menedzsment problémák[1]

Tervezés és házirendek (policies)

1. Van-e üzletfolytonossági tervünk (BCP)?
2. Van-e backup és helyreállítási tervünk?
3. Van-e DRP tervünk?

4. Monitorozott-e a mentés?
5. Problémákról van-e riasztás?

6. Dokumentáljuk-e a folyamatokat?

7. Végzünk-e visszaállítási teszteket?
8. Tartunk-e katasztrófagyakorlatot?
9. Van-e belső, van-e külső audit?

10. Rendszeresen újragondoljuk a feladatainkat, folyamatainkat, frissítjuk adatainkat, dokumentációinkat?

Volt már adatvesztésünk, volt-e már komoly adatvesztésünk? – Nem biztos, hogy az a legjobb, ha a válasz erre nem :-(

[1] ezekhez rögtön üzemeltetési problémák is kapcsolódnak

Hogyan árthat mentésnek a zsarolóvírus?

1. Már fertőzött állományokat mentünk
2. Malware hozzáférhet a mentéshez

Súlyos baklövést kell elkövetni ahhoz, hogy malware hozzáférhessen mentéshez,
– de mégis a legsúlyosabb zsarolóvírus károk így következtek be, azaz Malware hozzáférhetett a mentéshez.

Malware rendszerint azért férhetett hozzá,

- mert a mentés és az éles rendszer,
- illetve a mentés és az éles rendszer nem volt elkülönítve,
    - például rendszergazda ugyanazon hozzáféréssel végezte a mentést, mint amit az éles rendszer üzemeltetéséhez, horribile dictu napi más feladatok végzésére használt.

[Rendszergazda notebookja administrator user] -> [éles rendszer (ugyanaz az administrator hozzáférés)]
|
|
|—> [Backup Rendszer (ugyanaz az administrator hozzáférés)]

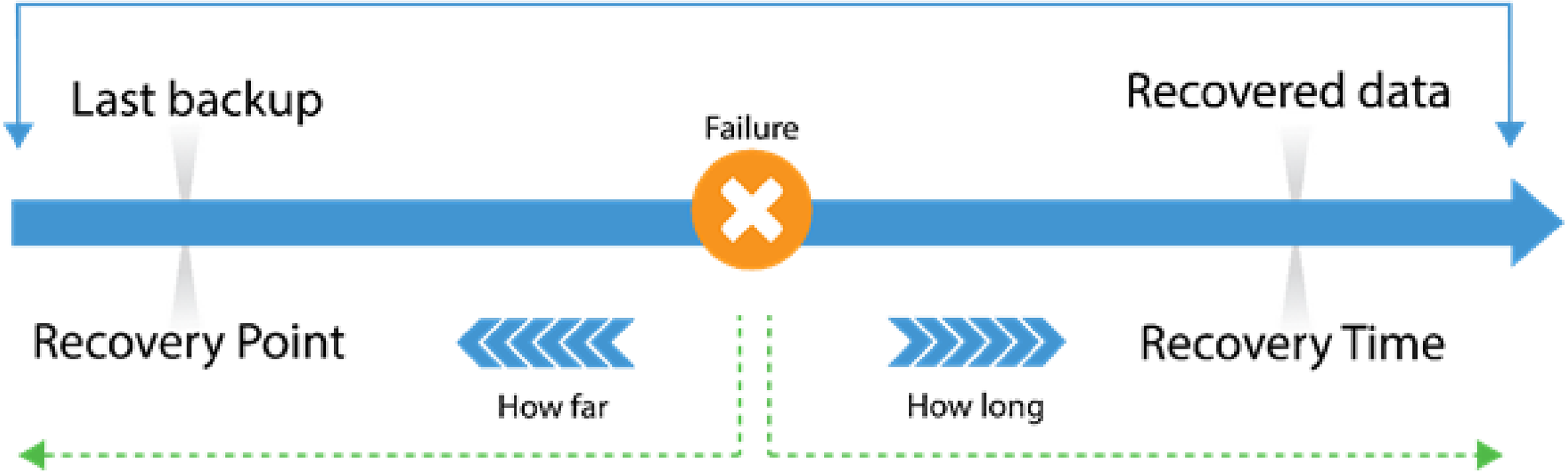
Ilyen esetben az így eljáró rendszergazda (büntetőjogi) felelőssége sem lehet kérdéses, enyhén szólva több mint gondatlanul (igen csak trehányul) jár el, ha így jár el,
– hacsak nem más felel azért, mert alkalmatlan személyre vagy félre bízta az üzemeltetést.
– Informatikai vezetők is felelősek, ha ilyen üzemeltetés megtörténhet szervezetük számára kritikus rendszereknél (bár sehol sem szabadna ilyet engedni, azaz nem kritikus rendszerekben sem).

Panacea:

- **szalagos mentés** ('old school'[2])
- **Backup as a Service (cloud backup)**

[2] https://www.techrepublic.com/article/going-old-school-with-tape-backup/

RTO és RPO



https://www.veeam.com/blog/rto-rpo-definitions-values-common-practice.html

Replikáció versus clusterezés versus backup

Mikor melyiket?

Tradicionális backupon túl

- Backup as a Service
- Replice as a Service
- DRS as a Service
- Continuous Data Protection

Section 12: Operations security

12.1 Operational procedures and responsibilities

IT operating responsibilities and procedures should be documented. Changes to IT facilities and systems should be controlled. Capacity and performance should be managed. Development, test and operational systems should be separated.

12.2 Protection from malware

Malware controls are required, including user awareness.

12.3 Backup

Appropriate backups should be taken and retained in accordance with a backup policy.

12.4 Logging and monitoring

System user and administrator/operator activities, exceptions, faults and information security events should be logged and protected. Clocks should be synchronized.

12.5 Control of operational software

Software installation on operational systems should be controlled.

12.6 Technical vulnerability management

Technical vulnerabilities should be patched, and there should be rules in place governing software installation by users.

12.7 Information systems audit considerations

IT audits should be planned and controlled to minimize adverse effects on production systems, or inappropriate data access.

https://www.iso27001security.com/html/27002.html