Backup

Hvor godt er du egentligt beskyttet

75 53 35 00 // salg@scannet.dk

Indhold

Spørgsmål til overvejelse

Backup strategi – Best practices

- Placering af data

- Hvem har adgang

- Scope på din backup – hvad er med?

Skal du stole på din leverandør?

Hvor godt beskyttet er din backup (hvordan beskytter man sin backup)

Disaster recovery eller backup

Opsummering - Hvad er dit problem?

Til overvejelse

Har I bevidst valgt en backup strategi?

Stoler I 100% på jeres leverandør?

Hvor ligger jeres backup(s)?

Hvem har adgang til jeres backup?

Hvor godt beskyttet er jeres backup?

Har I en Disaster recovery strategi eller en backup strategi?

Placering af Data

Backup-lokation
– og hvem der egentlig ejer den

- On-prem, cloud eller hybrid?
- Er den placeret i EU?
- Har I fuld adgang til jeres backup?

⚠ Tænk over det her:

- Økonomisystemet – kan I tage backup af det selv?
- Microsoft 365 – har I en ekstern backup?
- SaaS-platforme – hvem er ansvarlig; jer eller leverandøren

Hvem har adgang

- Begræns adgangen med rollebaseret adgang
- Adskil drift og backup roller
- Log og overvåg hvem der tilgår backup-data
- Hvem kan i dag slette eller ændre backup?

- Tænk i scenarier

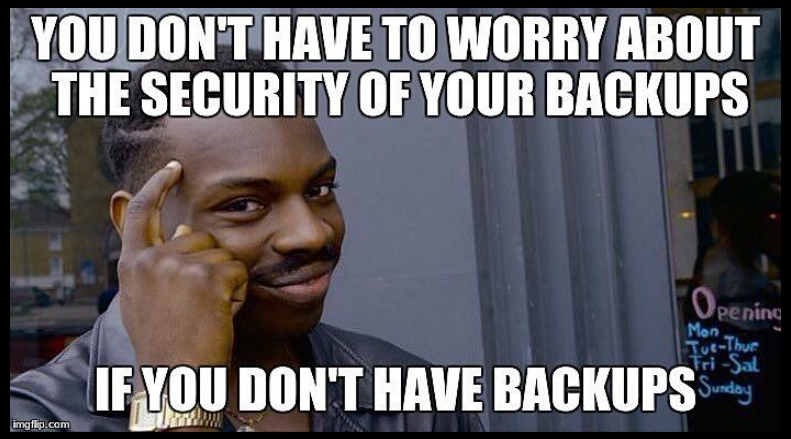
Backup scope

- Forretningskritiske systemer og data
- Konfigurationer og SaaS
- Retention og restore punkter
- Alt data er ikke ens

⚠ Tænk over det her:

- Hvilke data lever din forretning på? Hvis I mister dem, hvad så?
- Hvor længe skal data gemmes – og er der lovkrav, fx fra GDPR, bogføringsloven eller ISO-certificeringer?
- Er din backup application-aware?

Stoler I på jeres leverandør?



Stoler I på jeres leverandør?

Hvordan tager I selv kontrollen?

RPO – Hvor meget data kan vi miste?
RTO – Hvor hurtigt skal vi kunne restore?

Er det dokumenteret? Og er der en plan for udførelse?

Restore Point Objective - RPO

Hvor mange minutters data kan I tåle at miste?

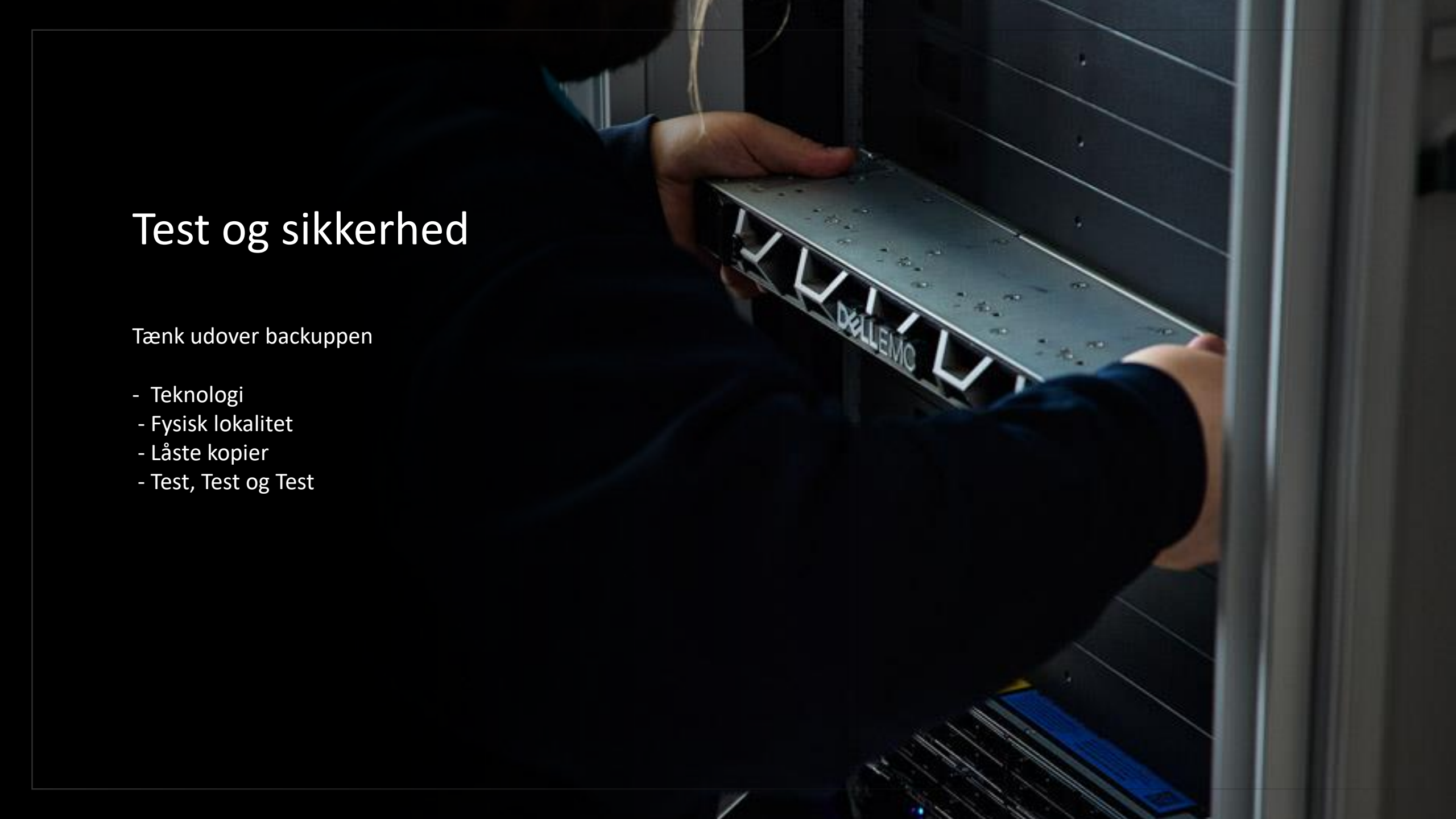
Restore Time Objective - RTO

Hvor lang nedetid kan I tåle?

Test og sikkerhed

Tænk udover backuppen

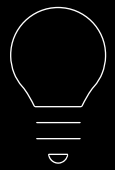
- Teknologi
- Fysisk lokalitet
- Låste kopier
- Test, Test og Test



Hvor godt beskyttet er din backup?

- Backup på flere lokationer
- Immutable backup
- Rollebaserede adgange
- Logging/overvågning
- Application-aware backup
- Restore-test
- Kryptering af transporten og gerne indholdet

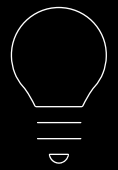
Disaster recovery
- Eller backup?



Backup & recovery politik

- Din data krypteres
- Gendannelse af data
- Compliance krav

= Løses med forskellige former for backup og/eller låste backups



Disaster recovery politik

- Tab af primære infrastruktur/produktionsdata

= Løses med Disaster recovery løsninger, som består af passiv hardware og storage i et andet datacenter og replikering af data

Hvorfor er det vigtigt?
- Scenarie 1
Backup uden disaster recovery

Primære datacenter

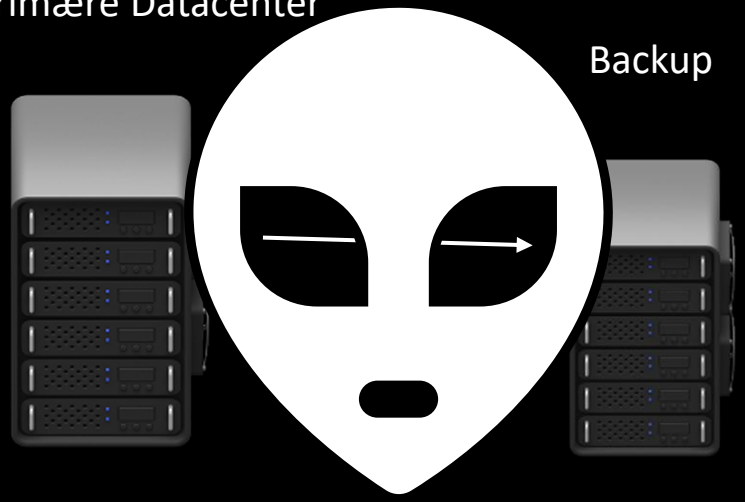
Backup

Hvilket system gendanner vi til?

Hvorfor er det vigtigt?
- Scenarie 2
Backup uden låste kopier

Primære Datacenter

Backup



Hvor er vores backup?

*Ved 93% af alle ransomware angreb går hackerne bevidst efter at slette eller låse backups
-*Veeam ransomware rapport fra 2023*

Opsummering

Har I bevidst valgt en strategi?	→	Nej? Prøv 3-2-1 og husk scenarier
Stoler I 100% på jeres leverandør?	→	Sørg for at tage kontrollen, start med RPO og RTO
Hvor ligger jeres backup(s)?	→	Tænk fysisk lokation, men også entitet
Hvem har adgang til jeres backup?	→	Tænk ikke kun internt, også eksternt
Hvor godt beskyttet er jeres backup?	→	Tænk ud over backup – teknologi, låste kopier
Har I en disaster recovery strategi eller en backup strategi?	→	Brug de rigtige værktøjer, undgå katastrofen

Få svar på, om din backup er en illusion

→ GAP-analyse

Få et hurtigt og effektivt overblik via denne GAP analyse. Det tager 1–2 minutter og du får svar med det samme.
Foretag din GAP analyse her: https://info.curanet.dk/backupgapanalyse