

Zo bouwt u een toekomstbestendige backupstrategie

Op basis van Veeam-technologie
| Nederlandse dataopslag | AVG & NIS2-compliant

75%

75% van alle organisaties werd in 2023 getroffen door ransomware

€540.000

De gemiddelde kosten per uur downtime bedragen €540.000

€4.500.000

De gemiddelde kosten per ransomware-incident bedragen €4,5 miljoen

59%

59% van alle organisaties laat cloud- en SaaS-data onbeschermd

De Microsoft 365-valkuil die veel organisaties over het hoofd zien

Veel organisaties gaan ervan uit dat Microsoft hun data volledig beschermt. Dat is een misvatting. Microsoft beheert de infrastructuur, maar u bent zelf verantwoordelijk voor databescherming, retentie en herstel.

Geo-redundantie is replicatie, geen backup. Wanneer data wordt verwijderd of versleuteld door ransomware, wordt die fout meegekopieerd naar alle locaties. Exchange Online, SharePoint, OneDrive en Teams zijn kwetsbaar zonder een externe backupoplossing.

Het 3-2-1-1-0 principe: de moderne backupstandaard

3

Drie kopieën van uw data

Eén productiekopie en twee backups. Nooit afhankelijk van één bron.

Productie

Backup 1

Backup 2

2

Twee verschillende opslagmedia

Spreiding voorkomt dat één defect alle kopieën treft.

Disk / NAS

Cloud / Tape

1

Eén kopie offsite opgeslagen

Gescheiden van uw productieomgeving, in een extern datacenter.

Primair datacenter

Remote / Cloud

1

Eén immutable (onwijzbare) kopie

Niet aan te passen of te versleutelen door ransomware.

Air-gap systeem

Object Lock

Offline tape

0

Nul fouten na herstelverificatie

Een backup is pas een backup als u hem kunt terugzetten. Test regelmatig.

Test restore

Valideer data

Documenteer

Wat te doen na een incident? Vier herstelstappen



Stap 1: Isoleer het systeem

Verbreek direct de netwerkverbinding om verdere verspreiding te voorkomen.



Stap 2: Meld het incident

NIS2 verplicht melding binnen 24 uur. Informeer uw BaaS-partner direct.



Stap 3: Herstel via immutable backup

Zet terug vanuit de onwijzbare kopie. Nooit vanuit een mogelijk besmette bron.



Stap 4: Valideer en documenteer

Verifieer de data-integriteit en leg het herstelproces vast voor audits en compliance.

Is uw backupstrategie toekomstbestendig? Controleer het zelf

3-2-1-1-0 ingericht

Heeft u drie kopieën, op twee media, waarvan één offsite en één immutable?

Restore-tests uitgevoerd

Wanneer heeft u voor het laatst een herstel getest en gedocumenteerd?

Data op Nederlands grondgebied

Staat uw backupdata in een Nederlands datacenter, buiten het bereik van de Amerikaanse CLOUD Act?

AVG en NIS2-compliant

Kunt u bij een incident binnen 24 uur rapporteren aan de toezichthouder?

1. Fortinet Ransomware Report
2. Veeam Data Protection Trends Report
3. IBM Cost of a Data Breach Report 2023
4. Veeam Cloud Protection Trends Report 2023

Wilt u uw backupstrategie laten toetsen?

Plan een vrijblijvend adviesgesprek met een SLTN-specialist. Wij analyseren uw huidige situatie, brengen de risico's in kaart en stellen een oplossing op maat voor.

Bel ons op
(0031) 35 - 688 84 00

Mail naar
info@sltn.nl

Bezoek de site
sltn.nl

Plan een kennismaking →