IRON MOUNTAIN®

UW SUCCESVOLLE STRATEGIE VOOR GEGEVENSBESCHERMING: 3-2-1-1-0

Wanneer u uw organisatie voorbereidt op het voorkomen van cyberaanvallen, is het ook belangrijk om na te denken over hoe te herstellen als het worstcasescenario zich toch voordoet.

Voor het back-uppen van gegevens werd altijd de strategie 3-2-1 geadviseerd. Dat wil zeggen drie kopieën van uw gegevens op twee verschillende media waarvan één kopie extern opgeslagen. Maar dit is aan het verschuiven. De beste strategie is nu **3-2-1-1-0** en we leggen u uit waarom.

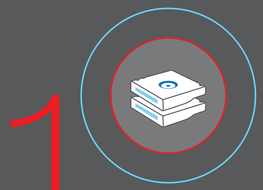
Gartner voorspelt dat ten minste **75%** van de IT-bedrijven tegen 2025 te maken krijgt met een of meer ransomware-aanvallen.

› *Bron*

3 Meerdere kopieën van uw data

2 Verschillende opslagmedia

1 Extern bewaarde kopie



1 Offline bewaarde kopie

0 Foutloze backup

WAAROM 3 KOPIEËN?

De drie kopieën van uw gegevens omvatten uw primaire data plus twee reservekopieën. Naast een snel herstelbare failover-kopie, moeten er ook echte back-ups zijn.

WAAROM MEERDERE MEDIA?

De drie kopieën moeten op ten minste twee verschillende soorten opslagmedia worden bewaard. Met zoveel applicaties, gegevens en opslag in de cloud is het belangrijk om de opslag te spreiden over cloud- en on-premises opslag.

39% van de mkb-bedrijven heeft geen calamiteitenplan om te reageren op cyberaanvallen en datalekken.

› *Bron*

WAAROM EXTERN?

Hoe uw back-ups worden opgeslagen, hangt vaak samen met de gegevensbeschermingsstrategie van uw cloudleverancier. Het is het beste om een kopie van de gegevens virtueel te isoleren van het productienetwerk. Als u zich voorbereidt op een waterramp, storm of andere natuurramp is het slim om minimaal één back-upkopie fysiek van de hoofdlocatie te verwijderen en in een andere regio op te slaan.

WAAROM OFFLINE?

Wanneer een back-up fysiek geïsoleerd is, kan ransomware er niet bij. Uw air-gapped back-up is gescheiden van het netwerk waar uw primaire kopie is opgeslagen. Als de primaire kopie of de back-up op locatie wordt beschadigd of in gevaar komt, kan de offline back-up worden gebruikt voor een herstel. Dit is vaak een back-up op tape. De softwarematige air-gaps die gebruikelijk zijn bij objectopslag doen al veel, maar er gaat niets boven een letterlijke air-gap wanneer u gegevens wilt beschermen.

WAAROM NO-ERRORS?

Kopie 0 is een no-errors back-up, die onveranderbaar is en op geen enkele manier kan worden gewijzigd. Deze wordt meestal offline gehouden en kan worden gebruikt om te herstellen van een ransomware-aanval. Om foutenvrij te blijven is er dagelijkse gegevenscontrole nodig en correctie van fouten zodra ze worden ontdekt.

Een 3-2-1-1-0 back-upstrategie beperkt de impact van een Single Point of Failure. Ransomware-aanvallen blijven toenemen, dus plan vooruit om te zorgen dat het met uw gegevensbescherming wel snor zit.

ONTDEK DE DIENSTEN VAN IRON MOUNTAIN

Iron Cloud® Data Protection
Om bedrijven van elke omvang uitgebreide gegevensbescherming te bieden heeft Iron Mountain de krachten gebundeld met cloud backup-leveranciers Carbonite en Veeam.

- **Iron Cloud® Data Protection samen met Carbonite**
- **Iron Cloud Backup and Replication Powered by Veeam**
- **Iron Cloud Secure Offline Storage (SOS) with Vault Lock**