INTERSTELLAR

Checklist: Data Recovery Readiness

KUN JE HERSTELLEN ONDER DRUK?

*8 kritieke vragen die je **nu** moet kunnen beantwoorden om je weerbaarheid te garanderen.*

HOE DEZE CHECKLIST TE GEBRUIKEN

Een backup hebben is niet hetzelfde als herstellen. Deze lijst helpt je in 5 minuten in kaart te brengen hoe weerbaar jouw data-omgeving werkelijk is. Loop de 8 vragen langs en geef per controlepunt een score:

- Rood: Niet geïmplementeerd of niet aantoonbaar. Direct aandacht vereist.
- Oranje: Gedeeltelijk geregeld. Verbetering nodig.
- Groen: Volledig geïmplementeerd, getest en gedocumenteerd.

DE 8 CONTROLEPUNTEN

RTO EN RPO PER KRITISCH SYSTEEM

Weet je per kritisch systeem en dataset wat de maximaal acceptabele downtime (**RTO**) en dataverlies (**RPO**) is, en zijn die met de operatie afgestemd?

Waarom dit ertoe doet: Zonder concrete **RTO/RPO** is herstel een vorm van hoop. De business bepaalt wat acceptabel is, IT levert de oplossing. Bij een incident bepaalt deze afstemming of je beslissingen onder druk consistent kunt nemen.

- Rood: Geen RTO/RPO gedefinieerd of alleen op infrastructuurniveau
- Oranje: RTO/RPO bestaan op papier, maar hebben geen interne eigenaar
- Groen: Per kritisch systeem zijn RTO/RPO vastgelegd, ondertekend door verantwoordelijken en jaarlijks herzien

3–2–1–1 STRATEGIE MET IMMUTABLE COPY

Voldoet jouw backup-architectuur aan de **3-2-1-1** regel? 3 kopieën, op 2 verschillende media, 1 offsite én 1 immutable of offline copy die ransomware niet kan versleutelen?

Waarom dit ertoe doet: Moderne ransomware zoekt actief naar backup-omgevingen om die als eerste te versleutelen of te verwijderen. Een immutable of offline kopie is je laatste redmiddel. Het is ook een expliciete eis vanuit NIS2 en cyberverzekeraars.

- Rood: Backup staat op hetzelfde netwerk, geen onveranderlijke kopie aanwezig
- Oranje: Offsite backup aanwezig, maar geen aantoonbare immutability of air gap
- Groen: 3-2-1-1 volledig geïmplementeerd met immutable storage of offline tier, getest tegen ransomware-scenario

AANTOONBARE RESTORE–TESTS

Wanneer is voor het laatst een volledige restore-test uitgevoerd op kritische systemen, en is het resultaat gedocumenteerd?

Waarom dit ertoe doet: Een backup die nooit getest is, is geen backup. Dat is een aanname. Praktijk leert dat 1/3 restore-pogingen faalt of langer duurt dan verwacht. Restore-tests zijn het enige objectieve bewijs dat herstel werkt.

- Rood: Geen restore-tests uitgevoerd, of alleen incidentele file-level checks
- Oranje: Restore-tests uitgevoerd, maar onregelmatig en niet gedocumenteerd
- Groen: Minimaal halfjaarlijkse end-to-end restore-test op kritische workloads, met rapportage en opvolging

RANSOMWARE RECOVERY–SCENARIO GETEST

Is er een geoefend scenario voor herstel ná een ransomware-aanval, inclusief schone forensische uitgangspositie, gevalideerde restore-bron en duidelijke beslismomenten?

Waarom dit ertoe doet: Herstellen ná ransomware is fundamenteel anders dan herstellen na een schijfcrash. Je moet weten welke backup besmet is, wanneer de aanvaller binnenkwam, en hoe je herstelt zonder de aanvaller opnieuw te activeren. Dit oefen je niet tijdens een incident.

- Rood: Geen ransomware-specifiek herstelscenario aanwezig
- Oranje: Scenario bestaat op papier, maar is niet geoefend met IT en operatie samen
- Groen: Tabletop én technische oefening minimaal jaarlijks, inclusief beslissing om wel of niet te betalen en communicatieplan

DISASTER RECOVERY RUNBOOK EN ROLLEN

Is er een actueel Disaster Recovery-runbook waarin per scenario staat: wie doet wat, in welke volgorde, met welke tools en met welke fallback, en weten de betrokken mensen dat?

Waarom dit ertoe doet: Onder druk maken mensen fouten en zijn ze moeilijk bereikbaar. Een runbook zet de denkstappen vooraf op papier, zodat er tijdens een incident geen discussie is over wie de beslissing neemt of welk systeem als eerste online moet.

- Rood: Geen runbook, of een verouderd document dat niemand kent
- Oranje: Runbook bestaat, maar is niet actueel of niet recent geoefend
- Groen: Up-to-date runbook met rollen, escalatiepad en contactgegevens, minimaal jaarlijks geoefend

DATACLASSIFICATIE EN HERSTEL–PRIORITERING

Zijn data en applicaties geclassificeerd (bijvoorbeeld prio 1, 2, 3), en is duidelijk welke systemen eerst hersteld worden bij beperkte capaciteit of tijd?

Waarom dit ertoe doet: Bij een grote uitval kun je niet alles tegelijk herstellen. Zonder vooraf bepaalde herstelvolgorde wordt het ad-hoc, en daarmee chaotisch. Purview helpt bij classificatie binnen de Microsoft-omgeving, maar de business moet de prioriteit bepalen.

- Rood: Geen classificatie, alles wordt gelijk behandeld
- Oranje: Classificatie bestaat, maar is niet gekoppeld aan herstelvolgorde of -capaciteit
- Groen: Prio-classificatie bestaat, gekoppeld aan RTO/RPO en herstel-prioritering, jaarlijks herzien

TOEGANG TOT CREDENTIALS TIJDENS EEN INCIDENT

Zijn admin-credentials, encryptiesleutels en herstel-procedures beschikbaar als jouw primaire omgeving (incl. password manager, Entra ID, Teams) volledig onbruikbaar is?

Waarom dit ertoe doet: Een veelvoorkomende blokkade tijdens herstel: de wachtwoorden staan in een vault die in dezelfde omgeving draait die je probeert te herstellen. Out-of-band toegang is essentieel. Anders ben je afhankelijk van de aanvaller, of van geluk.

- Rood: Geen out-of-band toegang tot kritische credentials of recovery keys
- Oranje: Procedure bestaat, maar is nooit getest of credentials zijn niet up-to-date
- Groen: Break-glass procedure aanwezig, fysiek of in offline kluis, periodiek geverifieerd en geoefend

NIS2: AANTOONBAARHEID EN BESTUURLIJKE VERANTWOORDING

Kun je richting NIS2-auditors, toezichthouders én bestuur aantonen dat jouw herstelvermogen getest, geoefend en gedocumenteerd is, en is het bestuur betrokken bij beslissingen rondom RTO/RPO?

Waarom dit ertoe doet: Onder **NIS2** zijn bestuurders persoonlijk aansprakelijk voor de cyberweerbaarheid van de organisatie. Aantoonbaarheid is niet optioneel. Het gaat niet om wat je hebt, maar om wat je kunt laten zien.

- Rood: Geen documentatie of bestuurlijke betrokkenheid
- Oranje: Documentatie aanwezig, maar bestuur is niet aantoonbaar geïnformeerd of betrokken
- Groen: Volledige audit trail: testrapporten, RTO/RPO-besluiten en bestuurlijke goedkeuring vastgelegd

SCORINGSOVERZICHT

Nr	Controlepunt	Rood	Oranje	Groen
1.	RTO en RPO per kritisch systeem	☐	☐	☐
2.	3-2-1-1 strategie met immutable copy	☐	☐	☐
3.	Aantoonbare restore-tests	☐	☐	☐
4.	Ransomware recovery-scenario getest	☐	☐	☐
5.	DR-runbook en verantwoordelijkheden	☐	☐	☐
6.	Dataclassificatie en herstel-prioritering	☐	☐	☐
7.	Toegang tot credentials tijdens een incident	☐	☐	☐
8.	NIS2: aantoonbaarheid en bestuurlijke verantwoording	☐	☐	☐

Aantal rood	Aantal oranje	Aantal groen

WAT ZEGT JOUW SCORE?

7 – 8 groen

Sterke basis. Je hebt herstel niet alleen geregeld, je kunt het ook aantonen. Focus op continue verbetering, geautomatiseerde rapportage en jaarlijkse oefening van het volledige scenario.

4 – 6 groen

Redelijke basis met duidelijke verbeterpunten. Prioriteer de rode controlepunten en breng objectief in kaart wat de huidige hersteltijd is.

2 – 3 groen

Risicogebied. De kans is groot dat herstel onder druk niet binnen acceptabele tijd lukt. Een gestructureerde restore-test maakt de gap zichtbaar.

0 – 1 groen

Hoog risico. Bij een incident is de kans op significant dataverlies en langdurige uitval reëel. Acuut aandacht en een gerichte verbeterroad-map zijn noodzakelijk.

VAN INZICHT NAAR ACTIE

Zie je twee of meer rode of oranje scores? Dan is dat geen uitzondering, maar een signaal. Veel organisaties ontdekken met deze checklist waar het wringt. Maar missen een concrete aanpak om dit gericht op te lossen.

Wil je weten wat voor jouw omgeving de juiste volgende stap is? In de Data Security Engagement workshop brengen we jouw datarisico's scherp in kaart en vertalen we die direct naar een concreet plan van aanpak, afgestemd op jouw situatie.

Plan je Data Security workshop