CHECKLIST · BCP VAULT

Is uw data veilig opgeborgen? 3-2-1-1-0 in de praktijk

De 3-2-1-1-0-regel is een eenvoudige maatstaf voor een backup waar u écht op kunt terugvallen: **3** kopieën van uw data, op **2** soorten opslag, waarvan **1** buiten de deur, **1** onveranderbaar, en **0** fouten bij het terugzetten.[1] Loop de vijf punten hieronder langs en kruis aan wat bij u geregeld is. Elk "nee" of "weet ik niet" is een punt om aandacht aan te geven.

3 Heeft u minimaal drie kopieën van uw belangrijke data?

Het origineel plus ten minste twee backups. Eén kopie is kwetsbaar: als die mislukt of beschadigd raakt, heeft u niets meer.

☐ **Ja** ☐ **Nee** ☐ **Weet ik niet**

2 Staan die kopieën op twee verschillende soorten opslag?

Bijvoorbeeld lokaal op schijf én in de cloud. Zo treft één storing of één type fout niet al uw kopieën tegelijk.

☐ **Ja** ☐ **Nee** ☐ **Weet ik niet**

1 Staat er minstens één kopie buiten uw eigen netwerk en locatie?

Een backup op hetzelfde netwerk of in dezelfde beheeromgeving als het origineel kan bij brand, een storing of een aanval samen met de rest getroffen worden. Een offsite kopie staat daar los van.

☐ **Ja** ☐ **Nee** ☐ **Weet ik niet**

1 Is er minstens één kopie onveranderbaar (immutable)?

Ransomware probeert steeds vaker eerst de backups te wissen of te versleutelen.[1] Een onveranderbare kopie kan na het wegschrijven door niemand worden aangepast of verwijderd, ook niet met beheerdersrechten of gestolen inloggegevens.

☐ **Ja** ☐ **Nee** ☐ **Weet ik niet**

0 Weet u zeker dat het terugzetten werkt, zonder fouten?

Een backup is pas waardevol als u er ook een restore mee kunt doen. Test u het terugzetten regelmatig, en weet u hoe lang het duurt voordat uw systemen weer draaien?[1]

☐ **Ja** ☐ **Nee** ☐ **Weet ik niet**

Uw uitkomst

- **5 × ja:** uw backup volgt de 3-2-1-1-0-regel. Blijf het terugzetten periodiek testen.
- **3 tot 4 × ja:** een goede basis, met een paar aandachtspunten.
- **0 tot 2 × ja:** bij een aanval of calamiteit is uw data waarschijnlijk minder goed beschermd dan u denkt.

Extra aandachtspunt: veel organisaties vallen sinds 15 augustus 2026 onder de Cyberbeveiligingswet (de Nederlandse invulling van NIS2). De NIS2-richtlijn noemt bedrijfscontinuïteit, "zoals back-upbeheer en noodherstel", uitdrukkelijk als onderdeel van de zorgplicht.[2] Een aantoonbaar geteste backup helpt u om dat te laten zien.

Hoe Business Continuity Partners hierin zorgt

Met **BCP Vault** zorgen wij voor de "1 buiten de deur" én de "1 onveranderbaar":[3]

- een onveranderbare kopie die vanaf het wegschrijven niet te wijzigen of te verwijderen is;
- volledig los van uw eigen netwerk en beheeromgeving, opgeslagen in Microsoft Azure in Nederland (Ierland mogelijk), versleuteld met AES-256;
- sluit rechtstreeks aan op uw bestaande Veeam Backup & Replication-omgeving: geen nieuwe software, geen migratie;
- bewaakt door onze engineers, met een periodieke restoretest vanuit de vault: zo werken we samen naar de "0".

Twijfelt u bij één van de punten? Wij beoordelen kosteloos uw huidige backupopzet en laten zien welke kopie een aanvaller met beheerdersrechten wel en niet zou kunnen bereiken.

sales@businesscontinuitypartners.nl · +31 320 799 360 · businesscontinuitypartners.nl/diensten/offsite-backup.html

1. Veeam, 3-2-1 Backup Rule Explained (bijgewerkt 3 juli 2026), veeam.com/blog/321-backup-rule.html · 2. Richtlijn (EU) 2022/2555 (NIS2), art. 21 lid 2 sub c, eur-lex.europa.eu/eli/dir/2022/2555/oj; Cyberbeveiligingswet in werking 15-08-2026 (Stb. 2026, 187 en 189) · 3. BCP Vault-productinformatie, businesscontinuitypartners.nl/diensten/offsite-backup.html