GIDS

De complete gids voor managed backup as a service

3-2-1 regel, immutable backups, kosten, NIS2-compliance, ransomware-bescherming en selectiecriteria. Met actuele Nederlandse marktdata en bronvermelding.

Maart 2026

IBGIDS NL

INHOUDSOPGAVE

Kerncijfers op een rij

Managed backup is geen luxe -- het is een zakelijke noodzaak. Deze cijfers laten zien waarom.

85%
van MKB-bedrijven ondervindt problemen met backup en recovery
Veeam SMB Survey [1]

96%
van ransomware-aanvallen richt zich specifiek op backup repositories
Veeam Ransomware Trends Report 2024 [2]

17%
van het Nederlandse MKB maakt nooit een backup -- complete blootstelling aan dataverlies
Digital Trust Center [3]

93%
van bedrijven met meer dan 10 dagen dataverlies gaat binnen 1 jaar failliet
Boston Computing [4]

EUR 100K+
Gemiddelde schade per ransomware-incident in Nederland
Autoriteit Persoonsgegevens [5]

6 dagen
Gemiddelde downtime na een succesvolle ransomware-aanval
NCSC Jaarbeeld Ransomware 2024 [6]

EUR 26 mrd
Wereldwijde BaaS-marktomvang (2024), verwacht EUR 69 mrd in 2030
Business Research Insights [7]

Q2 2026
Verwachte inwerkingtreding Cyberbeveiligingswet (NIS2) -- backup expliciet verplicht
Digitale Overheid [8]

1. Wat is managed backup as a service?

Bij managed backup as a service (BaaS) neemt een externe partij het volledige backup-beheer van je bedrijfsdata over. Jij bepaalt wat er gebackupt wordt -- de provider regelt de rest.

DEFINITIE

Managed Backup as a Service is een dienst waarbij een gespecialiseerde IT-provider je data automatisch kopieert, opslaat en bewaakt in een extern datacenter. In tegenstelling tot een doe-het-zelf backup draag je het technische beheer, de monitoring en het herstel uit aan specialisten [9].

VERSCHIL MET EIGEN BACKUP

KENMERK	EIGEN BACKUP	MANAGED BAAS
Beheer	Intern IT-team of systeembeheerder	Externe provider, 24/7 monitoring
Verantwoordelijkheid	Volledig bij jou	Gedeeld: provider beheert, jij bepaalt beleid
Kosten	Hoge upfront investering (hardware, licenties)	Maandelijks abonnement, voorspelbare kosten
Schaalbaarheid	Beperkt door eigen hardware	Direct op- en afschaalbaar
Expertise	Zelf bijhouden	Specialisten met certificeringen
Testen	Vaak vergeten of handmatig	Automatische restore-verificatie

CLOUD VS HYBRID VS ON-PREMISES

MODEL	HOE HET WERKT	GESCHIKT VOOR
Cloud-only	Alle backups naar extern datacenter via internet	Bedrijven zonder eigen serverruimte, SaaS-omgevingen
Hybrid	Lokale kopie voor snel herstel + cloud kopie voor offsite bescherming	MKB met eigen servers, snelle RTO nodig
On-premises managed	Hardware bij jou, beheer door externe provider	Strenge data-soevereiniteit, lage latency vereisten

Kort samengevat: bij managed BaaS huur je niet alleen opslagruimte -- je huurt expertise, monitoring en de garantie dat je data er is wanneer je het nodig hebt.

2. Waarom is het belangrijk?

Data is het fundament van je bedrijfsvoering. Zonder werkende backup kan een enkel incident je bedrijf stilleggen -- of erger.

DE 3-2-1 REGEL

De 3-2-1 regel is de gouden standaard voor dataprotectie [10]:

- **3 kopieeen** van je data (origineel + twee backups)
- **2 verschillende mediatypen** (bijv. lokale schijf + cloud)
- **1 kopie offsite** (fysiek gescheiden locatie)

De moderne uitbreiding is de **3-2-1-1-0 regel**: voeg 1 immutable of air-gapped kopie toe, en zorg voor 0 fouten bij hersteltests [11].

RANSOMWARE VERSLEUTELT BACKUPS

96% van ransomware-aanvallen richt zich specifiek op backup repositories [2]. Aanvallers weten dat bedrijven zonder backup eerder losgeld betalen. In Nederland had 58% van de ransomware-slachtoffers in 2023 geen werkende backup [12].

> **ALARMEREND**
> Slechts 8% van bedrijven die losgeld betalen herstelt uiteindelijk al hun data. Betalen is geen oplossing -- een geteste backup wel [13].

DE CIJFERS LIEGEN NIET

STATISTIEK	WAARDE	BRON
MKB slecht voorbereid op dataverlies	39%	Digital Trust Center [3]
Bedrijven zonder noodplan	21%	Veeam SMB Survey [1]
Failliet na >10 dagen dataverlies	93%	Boston Computing [4]
Heropent nooit na dataverlies	43%	Invenioit [14]
Data recovery rate (dalend)	66,3% (was 87,4% in 2021)	Go Beyond [15]

HET MKB IS EXTRA KWETSBAAR

Grote bedrijven hebben dedicated IT-teams, budgetten voor disaster recovery en redundante systemen. Als MKB-ondernemer heb je die luxe vaak niet. Juist daarom is een managed backup-dienst logisch: je krijgt enterprise-niveau bescherming zonder een eigen IT-afdeling op te bouwen.

3. Hoe werkt het?

Van installatie tot herstel: zo verloopt het backup-proces bij een managed dienst.

HET BACKUP-PROCES IN 5 STAPPEN

1 Inventarisatie en configuratie

De provider brengt je IT-omgeving in kaart: servers, werkstations, cloud-applicaties, databases. Samen bepaal je wat gebackupt wordt, hoe vaak en hoelang backups bewaard blijven.

2 Automatische backup

Software maakt op vastgestelde tijden incrementele of volledige backups. Data wordt versleuteld (AES-256) en verstuurd naar een extern datacenter. Bij een hybride setup blijft ook een lokale kopie beschikbaar voor snel herstel.

3 Monitoring en alerting

De provider bewaakt 24/7 of backups succesvol verlopen. Bij fouten, mislukte jobs of afwijkend datavolume krijg je direct een melding.

4 Restore-verificatie

Periodiek worden backups automatisch getest door een proefherstel uit te voeren. Zo weet je zeker dat je data daadwerkelijk herstelbaar is -- niet pas bij een incident.

5 Herstel bij incident

Bij dataverlies, ransomware of hardwarefalen start de provider het herstelproces. Afhankelijk van je SLA kan dat variieren van minuten (instant VM recovery) tot uren (cold restore).

RPO EN RTO UITGELEGD

BEGRIP	BETEKENIS	VRAAG
RPO (Recovery Point Objective)	Maximaal acceptabel dataverlies in tijd	"Hoeveel data mag ik kwijtraken?"
RTO (Recovery Time Objective)	Maximale tijd om systemen te herstellen	"Hoe lang mag ik plat liggen?"

Richtwaarden per bedrijfstype

BEDRIJFSTYPE	RPO	RTO
Webshop / e-commerce	< 10 minuten	< 1 uur
Financiele dienstverlening	< 1 uur	< 1 uur
Zorginstelling	< 1 uur	< 2 uur
Productiebedrijf	1--4 uur	< 4 uur
Standaard kantoor	4--12 uur	< 8 uur

Bronnen: Combell [16], Zmanda [17], Outvie [18]

IMMUTABLE BACKUPS

Immutable (onveranderbare) backups gebruiken WORM-technologie (Write Once, Read Many). Na het schrijven kan niemand -- ook geen administrator -- de data wijzigen, versleutelen of verwijderen [19]. Dit is je laatste verdedigingslinie tegen ransomware.

TIP

Vraag je provider altijd of immutable backups standaard zijn inbegrepen. Bij sommige aanbieders is dit een optie met meerkosten (10--30% boven standaardopslag).

4. Wat kost het?

De kosten van managed backup variieren sterk per model, datavolume en SLA-niveau. Hieronder vind je realistische indicaties voor de Nederlandse markt.

PRIJSMODELLEN

MODEL	PRIJSRANGE	TOELICHTING
Per gebruiker/maand	EUR 5--50	Afhankelijk van datavolume, retentie en SLA
Per TB/maand (self-service)	EUR 7--25	Puur opslag, zelf beheer via portal
Per TB/maand (managed)	EUR 25--75	Inclusief monitoring, herstel-support en rapportage
Per TB/maand (enterprise)	EUR 75--150+	Inclusief immutable storage, DR-testen, compliance

Bron: E-Storage [9], Truehost [20]

MKB-INDICATIES

BEDRIJFSGROOTTE	TYPISCH DATAVOLUME	INDICATIE PER JAAR
ZZP / micro (1--5 pers.)	100 GB -- 1 TB	EUR 600--1.800
Klein MKB (5--25 pers.)	1--5 TB	EUR 1.800--6.000
Middelgroot MKB (25--100 pers.)	5--25 TB	EUR 6.000--18.000
Groot MKB (100--250 pers.)	25--100 TB	EUR 18.000--60.000

WAT BEPAALT DE PRIJS?

FACTOR	IMPACT
Datavolume	Primaire prijsdriver -- meer TB = hogere kosten (vaak met volumekorting)
Retentieperiode	Langer bewaren = meer opslag = hogere kosten
RTO/RPO vereisten	Kortere RTO/RPO = duurdere infrastructuur
Compliance-eisen	NIS2, AVG, branchespecifiek = extra rapportage en audit-kosten

FACTOR	IMPACT
Immutability	WORM/immutable storage kost 10--30% meer
Datacenter locatie	Nederlands datacenter ~10--20% duurder dan buitenland

Bron: E-Storage [9]

KOSTEN VAN GEEN BACKUP

- Downtime kost MKB gemiddeld meer dan EUR 40.000 per jaar [21]
- Ransomware-schade in Nederland: gemiddeld meer dan EUR 100.000 per incident [5]
- NIS2-boetes bij niet-naleving: tot EUR 10 miljoen of 2% van de jaaromzet
- 93% van bedrijven met meer dan 10 dagen dataverlies gaat failliet binnen 1 jaar [4]

Een managed backup van EUR 6.000--18.000 per jaar weegt niet op tegen EUR 100.000+ potentiele schade.

5. Waar moet je op letten?

Niet elke backup-dienst is gelijk. Gebruik deze selectiecriteria om aanbieders objectief te vergelijken.

SELECTIECRITERIA

CRITERIUM	WAAROM BELANGRIJK	WAAR OP LETTEN
Immutability	Ransomware-bescherming	WORM-technologie, retentielock, niet uitschakelbaar
Offsite opslag	Bescherming tegen lokale rampen	Datacenter in NL, geografisch gescheiden
Encryptie	Data-integriteit en vertrouwelijkheid	AES-256 in transit en at rest, jij beheert de sleutel
Restore-snelheid	Minimale downtime	RTO in SLA vastgelegd, instant VM recovery optie
SLA met garanties	Afdwingbare afspraken	Uptime-garantie, herstelgarantie, compensatie bij falen
Compliance-rapportage	Bewijs voor toezichthouder	NIS2-ready rapporten, audit-trail, AVG-documentatie
Backup-verificatie	Zekerheid dat herstel werkt	Automatische restore-tests, rapportage van resultaten
SaaS-backup	M365/Google Workspace valt buiten standaard licentie	Specifieke ondersteuning voor cloud-applicaties
Schaalbaarheid	Meegroeien met je bedrijf	Pay-per-use model, geen lock-in contracten
Transparante prijzen	Geen verrassingen	Geen verborgen kosten voor egress, restores of support

10 VRAGEN VOOR JE PROVIDER

1. Zijn backups standaard immutable? Zo niet, wat kost het extra?
2. Waar staat het datacenter en is mijn data gegarandeerd in Nederland?
3. Wat is de gegarandeerde RTO en RPO in jullie SLA?
4. Hoe vaak worden restore-tests uitgevoerd en kan ik de rapporten inzien?
5. Wat gebeurt er als een backup faalt -- hoe snel word ik geinformeerd?
6. Zijn er kosten voor data-egress bij een restore?
7. Ondersteunen jullie backup van M365, Google Workspace en SaaS-applicaties?
8. Hoe ziet jullie NIS2-compliance rapportage eruit?
9. Wat is de minimale contractduur en zijn er uitstapkosten?
10. Wat is jullie procedure bij een ransomware-incident?

6. Veelgemaakte fouten

Deze fouten komen keer op keer terug bij Nederlandse bedrijven. Herken je er een? Dan is het tijd om actie te ondernemen.

#	FOUT	GEVOLG
1	Backups nooit testen	Pas bij een incident ontdek je dat restore niet werkt. 77% van tape-backups bevat fouten bij test [22].
2	Geen offsite kopie	Brand, diefstal of wateroverlast vernietigt productie en backup tegelijk.
3	Alleen cloud, geen lokale kopie	Herstel via internet is traag. Bij grote datasets kan restore dagen duren.
4	Geen immutable backup	Ransomware versleutelt je backups mee. 96% van aanvallen richt zich op backup repositories [2].
5	Ransomware al in de backup	Zonder retentiebeleid zit de ransomware in al je herstelpunten. Je herstelt het probleem mee.
6	SaaS-data niet gebackupt	M365 en Google Workspace zijn geen backup-diensten. Het gedeeld verantwoordelijkheidsmodel wordt niet begrepen [1].
7	Backup op hetzelfde netwerk	Ransomware beweegt lateraal door je netwerk en versleutelt alles wat bereikbaar is.
8	Geen retentiebeleid	Te kort: ransomware zit overal. Te lang: onnodige opslagkosten.
9	Geen noodplan / DR-plan	21% van bedrijven heeft geen noodplan. Bij een incident is het paniek [1].
10	Helemaal geen backup	17% van het Nederlandse MKB maakt nooit een backup [3]. Volledige blootstelling.

Bronnen: Veeam [1], COIN BV [23], Switch.be [24], Digital Trust Center [3]

GROOTSTE MISVATTING

"Wij werken in de cloud, dus onze data is veilig." Cloud-providers bieden infrastructuur, geen backup. Microsoft's eigen serviceovereenkomst adviseert expliciet om een backup-oplossing van een derde partij te gebruiken.

7. Compliance: NIS2 en AVG

Met de Cyberbeveiligingswet in aantocht wordt een professionele backup-strategie niet langer optioneel -- het wordt wettelijk verplicht.

NIS2 EN DE CYBERBEVEILIGINGSWET

De Cyberbeveiligingswet (Cbw) -- de Nederlandse implementatie van de Europese NIS2-richtlijn -- staat gepland voor Q2 2026 [8]. Artikel 21 noemt 14 verplichte beveiligingsmaatregelen, waarvan backup een expliciet onderdeel is.

Backup-relevante NIS2-vereisten

VEREISTE	ART. 21 ONDERDEEL	RELATIE MET BAAS
Back-upbeheer	Bedrijfscontinuiteit	Gestructureerd backup-beleid verplicht
Noodvoorzieningenplannen	Bedrijfscontinuiteit	Herstelplannen met geteste RTO/RPO
Crisisbeheer	Bedrijfscontinuiteit	Incidentrespons inclusief data-herstel
Risicoanalyse	Zorgplicht	Analyse welke data kritiek is
Incidentmelding	Meldplicht	Binnen 24 uur melden bij CSIRT

Bronnen: NCTV [25], NLdigital [26], NBA [27]

Wie valt onder NIS2?

CATEGORIE	VOORBEELDEN	BACKUP-IMPACT
Essentieel	Energie, transport, zorg, financieel, water	Strengste eisen, actief toezicht
Belangrijk	Post, afval, voedsel, chemie, productie	Zorgplicht, toezicht na incidenten
Ketenpartners	Leveranciers van bovenstaande	Indirect verplicht via supply chain

Bronnen: SPS [28], WaveSec [29]

AVG EN BACKUP

De AVG vereist "passende technische en organisatorische maatregelen" voor persoonsgegevens, waaronder [30]:

- **Beschikbaarheid en veerkracht** van verwerkingssystemen
- Vermogen om bij een incident de **toegang tot persoonsgegevens tijdig te herstellen**
- Een **procedure voor regelmatig testen** van de doeltreffendheid van maatregelen

Dit maakt een geteste backup-strategie een impliciete AVG-vereiste. Managed BaaS biedt hier een aantoonbare invulling van.

TIP

Vraag je provider om een NIS2-compliance rapport en een verwerkersovereenkomst (AVG). Een professionele provider heeft deze documenten standaard beschikbaar.

8. Managed backup vs alternatieven

Managed backup is niet de enige optie. Begrijp de verschillen zodat je de juiste keuze maakt voor jouw situatie.

KENMERK	MANAGED BAAS	EIGEN BACKUP	DRAAS	BCP
Wat het is	Externe partij beheert je backups	Je regelt alles zelf intern	Disaster Recovery as a Service: volledige omgeving repliceren	Business Continuity Plan: organisatorisch raamwerk
Focus	Data beschermen en herstellen	Data beschermen	Hele IT-omgeving overeind houden	Bedrijfsprocessen draaiend houden
Kosten	EUR 500--5.000/ maand (MKB)	Hoge upfront, variabele onderhoudskosten	EUR 2.000--15.000+/ maand	Consultancy + interne tijd
Complexiteit	Laag (provider regelt het)	Hoog (eigen expertise nodig)	Middel (provider regelt techniek)	Hoog (organisatie-breed)
RTO	Uren tot minuten	Afhankelijk van eigen capaciteit	Minuten (failover)	N.v.t. (geen technische oplossing)
Geschikt voor	MKB zonder dedicated IT-team	Bedrijven met sterke IT-afdeling	Bedrijven waar downtime direct omzet kost	Elke organisatie (aanvullend)

Managed BaaS en DRaaS zijn geen concurrenten -- ze vullen elkaar aan. BaaS beschermt je data, DRaaS beschermt je hele omgeving. Een BCP is het organisatorische kader daaromheen. Voor de meeste MKB-bedrijven is managed BaaS de logische eerste stap.

WANNEER KIES JE WAT?

SITUATIE	AANBEVELING
Geen IT-afdeling, beperkt budget	Start met managed BaaS
Eigen IT-team, controle belangrijk	Eigen backup met extern advies
Elke minuut downtime kost omzet	DRaaS + managed BaaS
NIS2-plichtig, compliance-eisen	Managed BaaS + BCP

9. Trends en ontwikkelingen

De backup-markt ontwikkelt zich snel. Deze trends bepalen waar de sector naartoe gaat in 2026 en daarna.

IMMUTABLE BACKUP ALS STANDAARD

Waar immutable backups eerder een premium optie waren, wordt het steeds vaker de standaard. De ransomware-dreiging is zo groot dat providers die geen immutable storage bieden marktaandeel verliezen [19].

AIR-GAPPED BACKUPS

Fysiek of logisch geisoleerde backups die niet via het netwerk bereikbaar zijn. De 3-2-1-1 regel (met de extra "1" voor air-gapped) wint terrein als best practice [11].

AI-DETECTIE VAN RANSOMWARE IN BACKUPS

Moderne backup-oplossingen gebruiken AI en machine learning om ongebruikelijke patronen in backup-data te detecteren. Denk aan massale bestandswijzigingen, encryptie-patronen of verdachte metadata-veranderingen. Het doel: ransomware identificeren voordat je een besmette backup herstelt [31].

CLOUD-NATIVE BACKUP

Steeds meer bedrijven werken volledig in de cloud (M365, Google Workspace, SaaS-applicaties). Cloud-native backup-oplossingen zijn specifiek ontworpen om deze omgevingen te beschermen -- zonder dat je lokale infrastructuur nodig hebt [7].

MARKTGROEI

METRIC	2024	2030 (VERWACHT)	CAGR
BaaS markt (wereldwijd)	~EUR 26 miljard	~EUR 69 miljard	17,5%
Cloud Backup markt	~EUR 7,1 miljard	~EUR 21,6 miljard	24,8%

Bronnen: Business Research Insights [7], IMARC Group [32], Research and Markets [33]

WAT BETEKENT DIT VOOR JOU?

- De markt groeit, dus er komen meer aanbieders en scherpere prijzen
- Immutable en air-gapped worden standaard -- kies een provider die dit biedt
- AI-detectie wordt een onderscheidend kenmerk -- vraag ernaar bij selectie
- SaaS-backup is niet langer optioneel nu bedrijven volledig in de cloud werken

10. Aan de slag

Je weet nu wat managed backup inhoudt, wat het kost en waar je op moet letten. Tijd voor actie.

STAPPENPLAN

1 **Inventariseer je data**

WEEK 1

Breng in kaart welke data kritiek is: servers, werkstations, e-mail, cloud-applicaties, databases. Bepaal voor elk systeem hoeveel dataverlies (RPO) en downtime (RTO) acceptabel is.

2 **Bepaal je eisen**

WEEK 1--2

Gebruik de selectiecriteria uit hoofdstuk 5. Heb je NIS2-verplichtingen? Dan zijn immutable backups, compliance-rapportage en geteste restores verplicht.

3 **Vergelijk aanbieders**

WEEK 2--3

Vraag offertes op bij minimaal 3 aanbieders. Stel de 10 vragen uit hoofdstuk 5. Let op verborgen kosten voor egress en restores.

4 **Start met een pilot**

WEEK 3--6

Begin met je meest kritieke systemen. Valideer de backup-kwaliteit en herstelsnelheid voordat je de hele omgeving migreert.

5 **Test, test, test**

DOORLOPEND

Plan maandelijkse restore-tests. Documenteer de resultaten. Dit is niet alleen een best practice -- het is een NIS2-vereiste.

Bronnenlijst

[1] **Veeam** -- 85% of SMBs Experiencing Problems with Backup and Recovery. https://www.veeam.com/news/85-percents-of-smbs-experiencing-problems-with-backup-and-recovery-veeam-survey-finds.html

[2] **Veeam** -- Ransomware Encryption: Prevention and Response. https://www.veeam.com/blog/ransomware-encryption.html

[3] **Digital Trust Center** -- Back-ups. https://www.digitaltrustcenter.nl/back-ups

[4] **Boston Computing** -- Data Backup Statistics. https://www.bostoncomputing.net/consultation/databackup/statistics/

[5] **Techzine** -- Dutch Authority: Data theft via ransomware doubles in one year. https://www.techzine.eu/news/security/132719/dutch-authority-data-theft-via-ransomware-doubles-in-one-year/

[6] **NCSC** -- Jaarbeeld Ransomware 2024. https://www.ncsc.nl/actueel/nieuws/2025/02/17/jaarbeeld-ransomeware-2024

[7] **Business Research Insights** -- BaaS Market Trends 2025--2035. https://www.businessresearchinsights.com/market-reports/backup-as-a-service-market-121898

[8] **Digitale Overheid** -- Cyberbeveiligingswet. https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/cyberbeveiligingswet/

[9] **E-Storage** -- Wat zijn de kosten van een backup and recovery as a service oplossing? https://www.e-storage.nl/blog/wat-zijn-de-kosten-van-een-backup-and-recovery-as-a-service-oplossing/

[10] **Veeam** -- 3-2-1 Backup Rule. https://www.veeam.com/blog/321-backup-rule.html

[11] **TechTarget** -- How the 3-2-1-1-0 backup rule reflects modern needs. https://www.techtarget.com/searchdatabackup/tip/How-the-3-2-1-1-0-backup-rule-reflects-modern-needs

[12] **Computable** -- Meeste ransomware-slachtoffers laks met backup. https://www.computable.nl/2024/02/23/meeste-ransomware-slachtoffers-laks-met-backup/

[13] **CrashPlan** -- 75+ Data Loss Statistics 2026: The Complete Guide. https://www.crashplan.com/blog/75-data-loss-statistics-for-2026-the-complete-guide/

[14] **Invenioit** -- 15 Data Loss Statistics. https://invenioit.com/continuity/data-loss-statistics/

[15] **Go Beyond** -- Backup Statistics 2025. https://www.go-beyond.biz/resources/backup-statistics

[16] **Combell** -- De juiste RPO en RTO bepalen. https://www.combell.com/nl/blog/hoe-bepaal-je-de-juiste-rpo-en-rto-voor-jouw-disaster-recovery/

[17] **Zmanda** -- RTO versus RPO: begrijpen hun verschillen. https://www.zmanda.com/nl/blog/rto-vs-rpo-begrijpen-hun-verschillen/

[18] **Outvie** -- Back-upafspraken in een IT-contract: RPO en RTO. https://outvie.nl/kennisbank/back-upafspraken-in-een-it-contract-hoe-gaat-u-om-met-rpo-en-rto/

[19] **ConnectWise** -- What is Immutable Backup. https://www.connectwise.com/blog/what-is-immutable-backup

[20] **Truehost** -- Cloud Backup Costs 2026. https://truehost.com/cloud-backup-costs/

[21] **Beschermheren** -- Wat zijn de kosten van downtime voor bedrijven? https://www.beschermheren.nl/wat-zijn-de-kosten-van-downtime-voor-bedrijven/

[22] **TrueList** -- Data Loss Statistics 2025. https://truelist.co/blog/data-loss-statistics/

[23] **COIN BV** -- Veel voorkomende fouten bij backup en disaster recovery. https://www.coinbv.nl/blog/veel-voorkomende-fouten-bij-back-up-en-disaster-recovery/

[24] **Switch.be** -- 5 veelgemaakte fouten bij backups. https://www.switch.be/blog/backupfouten/

[25] **NCTV** -- Vragen en antwoorden Cyberbeveiligingswet. https://www.nctv.nl/onderwerpen/c/cyberbeveiligingswet/vragen-en-antwoorden

[26] **NLdigital** -- Stappenplan Cyberbeveiligingswet NIS2. https://www.nldigital.nl/kennis-producten/stappenplan-cyberbeveiligingswet-nis2-richtlijn/

[27] **NBA** -- Cyberbeveiligingswet: nieuwe verplichtingen voor bedrijven. https://www.nba.nl/nieuws/2025/maart/cyberbeveiligingswet-nieuwe-verplichtingen-voor-bedrijven-onder-nis2-richtlijn/

[28] **SPS** -- Cyberbeveiligingswet 2026: val je eronder? https://sps.nl/inspiratie/cyberbeveiligingswet-2026-nis2-val-je-eronder/

[29] **WaveSec** -- NIS2-richtlijn uitgelegd. https://wavesec.nl/nis2-richtlijn/

[30] **Storware** -- Role of Immutability and Air-Gapping in European Data Protection. https://storware.eu/blog/the-role-of-immutability-and-air-gapping-in-european-data-protection-strategies/

[31] **ObjectFirst** -- Ransomware Backup Protection. https://objectfirst.com/guides/ransomware/ransomware-backup-protection/

[32] **IMARC Group** -- Cloud Backup Market. https://www.imarcgroup.com/cloud-backup-market

[33] **Research and Markets** -- BaaS Market Forecast to 2030. https://www.researchandmarkets.com/report/backup-as-a-service