Het IT-landschap in beweging

Trendrapport IT-kanaal · Q4 2026

Wat er dit kwartaal speelt voor IT-partners en hun mkb-klanten: wet- en regelgeving, soevereiniteit, dreiging, de markt en wat je er nu mee kunt.

IMMYTEC DATA PROTECTION & CYBERSECURITY

Inhoud

1	**Dit kwartaal in het kort**	Waarom dit trendrapport · Vijf ontwikkelingen · Kwartaalradar
2	**Wet- en regelgeving**	Cyberbeveiligingswet (NIS2) · Europese regelgeving · Keten
3	**Soevereiniteit en cloud**	Beleid en overheid · Markt en aanbod
4	**Dreiging en weerbaarheid**	Dreigingsbeeld · Incidenten · Mkb-weerbaarheid · Cyberverzekering
5	**De markt voor IT-dienstverleners**	Markt in cijfers · Vendors en prijzen · Arbeidsmarkt · Klant · Vraagstukken
6	**Verdieping**	Sector in de spotlight · Technologie op de radar
7	**Aan de slag**	Regelingen · Agenda · Deadlines · Gespreksvragen

Waarom dit trendrapport

Informatie over wetgeving, dreiging en de markt is er genoeg. Het probleem is dat ze versnipperd is.

Wie als IT-partner wil bijblijven, zoekt op tientallen plekken: bij overheid en toezichthouders, in Europese regelgeving, in vakmedia, onderzoeksrapporten en bij vendors. Elk met een eigen tempo en invalshoek. Daardoor weet je niet meer goed waar wat staat. We zien een groeiende behoefte aan één plek waar het samenkomt.

Dit trendrapport bundelt elk kwartaal wat er speelt, ordent het in vaste delen en noemt bij elk feit de bron. Zo zie je in één keer wat er veranderd is, wat eraan komt en wat je ermee kunt in gesprekken met klanten.

- Overheid en toezichthouders
- Europese regelgeving
- Dreigingsbeelden
- Onderzoeksrapporten
- Vakmedia
- Vendors en distributeurs
- Brancheverenigingen
- Events en beurzen

Eén overzicht

gebundeld, geordend en met bron, elk kwartaal

Vijf ontwikkelingen sinds juli 2026

01 **Cyberbeveiligingswet van kracht**
Sinds 15 augustus 2026 gelden registratie-, zorg- en meldplicht voor ruim 8.000 organisaties. Via de keten merkt ook het mkb dat.

02 **Overheid kiest maximale soevereiniteit**
Het Rijk scherpte het cloudbeleid aan en bouwt een eigen overheidscloud. De overname van DigiD-beheerder Solvinity ging niet door.

03 **Dreiging groeit sneller dan weerbaarheid**
Het Cybersecuritybeeld 2026: AI versnelt aanvallen en kwetsbaarheden worden binnen uren misbruikt.

04 **Cyberaanval raakt de retailketen**
Ahold Delhaize verwacht door het incident van oktober € 200–250 miljoen minder omzet in het vierde kwartaal.

05 **Licenties en hardware duurder**
Microsoft verhoogde per 1 juli meerdere 365-prijzen; geheugenprijzen stegen sterk door de vraag naar AI.

8.000+
organisaties vallen onder de Cyberbeveiligingswet (NCSC)

84%
van Nederlandse IT-beslissers vindt datasoevereiniteit belangrijk of topprioriteit (Leaseweb)

136
ransomware-aanvallen zag de Autoriteit Persoonsgegevens in 2025

Periode: juli tot half november 2026

Wat is nieuw, wat loopt en wat komt eraan

De radar zet de ontwikkelingen op een tijdlijn: wat dit kwartaal is ingegaan, wat nog doorloopt en waar je de komende maanden rekening mee houdt.

Nieuw	Cyberbeveiligingswet van kracht (15 augustus) · Meldplicht Cyber Resilience Act gestart (11 september) · Cybersecuritybeeld Nederland 2026 verschenen (6 november)
Loopt	Registratie van organisaties bij het NCSC · Overgang naar het strengere Rijkscloudbeleid · Stijgende prijzen voor geheugen en hardware
Komt eraan	Subsidie voor kleine bedrijven sluit 30 november · Eerste applicaties op de overheidscloud eind 2026 · Cyber Resilience Act volledig van toepassing op 11 december 2027

02

Wet- en regelgeving

Welke regels gelden nu, wat vragen ze en hoe werken ze door in de keten, ook bij organisaties die er zelf niet onder vallen.

2.1 Cyberbeveiligingswet (NIS2)

2.2 Europese regelgeving: CRA en AI

2.3 Doorwerking in de keten

IMMTEC DATA PROTECTION & CYBERSECURITY

De Cyberbeveiligingswet is van kracht

Sinds 15 augustus 2026 gelden de Cyberbeveiligingswet (Cbw), de Nederlandse uitwerking van de Europese NIS2-richtlijn, en de Wet weerbaarheid kritieke entiteiten (Wwke). De wet legt vier plichten op.

- **Registratie:** in het entiteitenregister van het NCSC. Organisaties bepalen zelf of ze onder de wet vallen.
- **Zorgplicht:** passende en evenredige maatregelen op basis van een risicoanalyse.
- **Meldplicht:** vroegtijdige waarschuwing binnen 24 uur, melding binnen 72 uur en een eindverslag binnen een maand.
- **Bestuur:** keurt de maatregelen goed, houdt toezicht en volgt een training.
- **Wie valt eronder?** Organisaties in een aangewezen sector met 50 of meer medewerkers, of met een omzet of balanstotaal boven € 10 miljoen.

8.000+
organisaties onder de Cbw

±500
organisaties onder de Wwke

18
sectoren

24 uur
voor de eerste waarschuwing

Bron: Rijksoverheid (15-08-2026); NCSC, Cyberbeveiligingswet: meldplicht en 'Valt mijn organisatie onder de Cbw?'

Cyber Resilience Act en AI: de volgende golf

Naast NIS2, dat over organisaties gaat, komt er Europese regelgeving voor producten en voor AI. Beide raken IT-partners: als leverancier van hardware en software, en als adviseur bij de invoering van AI.

CYBER RESILIENCE ACT (CRA)

- Sinds 11 september 2026 melden fabrikanten actief misbruikte kwetsbaarheden en ernstige incidenten: binnen 24 uur, 72 uur en met een eindrapport.
- Vanaf 11 december 2027 gelden de meeste verplichtingen. Boetes tot € 15 miljoen of 2,5% van de wereldwijde omzet.
- Wie producten onder eigen naam verkoopt of wezenlijk aanpast, kan de plichten van een fabrikant krijgen. Dat kan ook een reseller zijn.

AI: GEBRUIK LOOPT VOOR OP BELEID

De AI-omnibus wijzigt de Europese AI Act sinds 27 juli 2026. In het mkb is AI al dagelijkse praktijk, maar afspraken ontbreken vaak:

8 op 10
mkb'ers gebruikt AI in enige mate

1 op 3
is bang dat gevoelige data in AI-tools belandt

9%
van het mkb heeft formeel AI-beleid

Bron: Jones Day (07-2026); Integrity360 (31-08-2026); Europese Commissie, AI Office; AI-cijfers uit het Cybersecuritybeeld 2026 zoals weergegeven door ICT Magazine (10-11-2026)

Ook wie niet onder de wet valt, merkt hem

Het grootste deel van het mkb valt niet onder de Cyberbeveiligingswet. Maar organisaties die dat wel doen, moeten hun risico's beheersen, en daar horen hun leveranciers bij. Zo komen de vragen bij het mkb terecht, en bij hun IT-partner.

Het Cybersecuritybeeld 2026 zegt het zo: kleine organisaties en het mkb kunnen hun weerbaarheid niet zelfstandig verhogen. Leveranciers, toezichthouders en overheid zijn medeverantwoordelijk.

VRAGEN DIE MKB-KLANTEN VAKER GAAN KRIJGEN

1. Heeft u een actueel overzicht van uw systemen en wie er toegang toe heeft?
2. Hoe snel en via welk kanaal meldt u een incident aan ons?
3. Zijn uw back-ups getest, en staan ze buiten bereik van een aanvaller?
4. Onder welk recht valt uw cloudleverancier?
5. Is uw continuïteitsplan ook echt geoefend?

Bron: NCSC (06-11-2026) over het Cybersecuritybeeld 2026; vragen afgeleid van de zorgplicht in de Cyberbeveiligingswet

03

Soevereiniteit en cloud

Waarom de overheid kiest voor maximale controle over data en infrastructuur, en hoe het onderwerp het mkb bereikt.

3.1 Beleid en overheid

3.2 Markt en aanbod

IMMTEC DATA PROTECTION & CYBERSECURITY

De overheid kiest het hoogste soevereiniteitsniveau

Op 3 juli 2026 scherpte het kabinet het cloudbeleid van het Rijk aan. Het geldt formeel alleen voor de Rijksoverheid, maar het zet de toon voor wat grote opdrachtgevers van hun leveranciers gaan vragen.

- Vooraf een cloudstrategie met de risico's, zoals afhankelijkheid van één leverancier en niet-Europees recht
- Een verplicht exitplan voor belangrijke clouddiensten
- E-mail en documenten: publieke cloud afgeraden
- Kritieke organisaties: aanbieders onder niet-EU-recht afgeraden voor kerntaken
- Een eigen overheidscloud op het hoogste niveau (SEAL-4) van het EU Cloud Sovereignty Framework; eerste applicaties eind 2026
- Vier jaar om bestaande diensten aan te passen

CASUS: SOLVINITY EN DIGID

nov 2025	Het Amerikaanse Kyndryl wil Solvinity overnemen, het bedrijf achter de infrastructuur van DigiD
26 mei 2026	De staatssecretaris verbiedt de overname op advies van het Bureau Toetsing Investeringen
aug 2026	Kyndryl ziet af van de overname
2028	Het kabinet wil dan een Nederlandse of Europese partij voor DigiD

Bron: Rijksoverheid (03-07-2026); Computable (03-07-2026); NOS (26-05-2026); MSP Business (27-08-2026)

Van overheidsdossier naar gesprek in het mkb

Soevereiniteit is niet langer alleen een onderwerp voor de overheid. Onderzoek onder Nederlandse organisaties laat zien dat het de IT-strategie begint te sturen. Klanten stappen niet massaal over, maar willen wel weten waar ze staan.

84%
van 383 Nederlandse IT-beslissers noemt datasoevereiniteit belangrijk (61%) of topprioriteit (23%). Leaseweb, 2026

37%
van grote organisaties zegt dat soevereiniteit de IT-strategie beïnvloedt. Dutch IT Sourcing Study 2026

26%
wil minder afhankelijk worden van de grote cloudaanbieders; in de publieke sector 45%. Dutch IT Sourcing Study 2026

SOEVEREINITEIT OF AUTONOMIE?

Soevereiniteit gaat over jurisdictie: onder welk recht vallen je gegevens? Autonomie gaat over keuzevrijheid: weet je waar je data staat en kun je weg als het moet?

WAT EEN IT-PARTNER ERMEE KAN

Begin met inzicht: waar staat welke data, welke afhankelijkheden zijn er en wat is het exitscenario per kritieke dienst? Dat gesprek kan ook binnen een Microsoft-omgeving.

Bron: Leaseweb/Blauw via Accountant.nl (10-06-2026); Eraneos en Whitelane, Dutch IT Sourcing Study 2026; Computable (21-04-2026)

04

Dreiging en weerbaarheid

Hoe ontwikkelt de dreiging zich, welke incidenten vielen op, en hoe weerbaar is het mkb echt?

4.1 Dreigingsbeeld
4.2 Incidenten en cijfers
4.3 Mkb-weerbaarheid
4.4 Cyberverzekering

IMMTEC DATA PROTECTION & CYBERSECURITY

De dreiging groeit sneller dan de weerbaarheid

Op 6 november 2026 verscheen het Cybersecuritybeeld Nederland 2026 van NCTV en NCSC. De kernboodschap is ‘scheefgroei’: aanvallers worden capabeler, terwijl de digitale weerbaarheid van organisaties achterblijft.

AI in elke fase

Aanvallers gebruiken AI in alle fasen van een aanval. Breed beschikbare modellen volstaan voor malware en overtuigende phishing.

Van maanden naar uren

De tijd tussen ontdekking en misbruik van een kwetsbaarheid: in 2024 maanden, in 2025 weken, in 2026 nog maar enkele uren.

Afpersing via datadiefstal

Criminelen richten zich meer op het stelen van data. Er waren meer incidenten met grote maatschappelijke impact.

Ga uit van een inbraak

Buiten houden is niet genoeg. Het gaat erom indringers snel op te sporen en te stoppen.

Advies van NCSC en NCTV: bestuurlijk eigenaarschap · snel patchen · back-ups en geteste continuïteit · 24/7 logging en detectie · inzicht in het eigen IT-landschap

Bron: NCTV en NCSC, Cybersecuritybeeld Nederland 2026 (06-11-2026); Computable (06-11-2026)

Ransomware in cijfers en de casus van het kwartaal

De Autoriteit Persoonsgegevens (AP) telt jaarlijks de ransomware-aanvallen die tot een datalek leidden. Daarnaast lichten we elk kwartaal één incident uit dat laat zien wat een aanval in de praktijk betekent.

AUTORITEIT PERSOONSGEGEVENS OVER 2025

136
ransomware-aanvallen (2024: 127)

283
gemelde datalekken als gevolg: één aanval raakt vaak meerdere organisaties

Aanvallen met alleen datadiefstal, zonder versleuteling, stegen van 15 naar 32. Advies van de AP: niet betalen, en zorg voor recente back-ups die de aanval niet hebben geraakt.

CASUS: AHOLD DELHAIZE, OKTOBER 2026

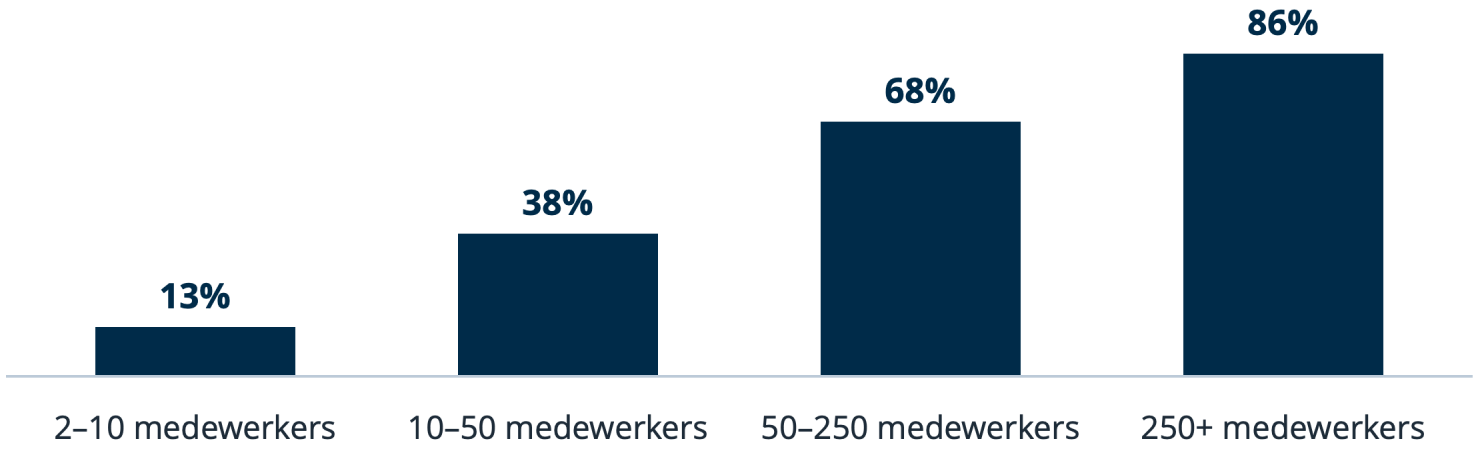
- Op 12 oktober meldde het concern een cyberincident; systemen gingen uit voorzorg offline
- Websites, apps en thuisbezorging van onder meer Albert Heijn lagen stil, bezorging circa twee weken
- Verwachte impact in Q4: € 200–250 miljoen omzet
- Volgens het bedrijf geen aanwijzingen dat klant- of partnerdata is buitgemaakt

Bron: AP, Rapportage ransomware 2025 (07-2026) via ICT Magazine en AG Connect; Ahold Delhaize (13-10-2026); ICT Magazine (04-11-2026)

Hoe kleiner het bedrijf, hoe minder maatregelen

Het CBS meet jaarlijks welke van twaalf beveiligingsmaatregelen bedrijven nemen, zoals back-ups, versleuteling en tweestapsverificatie. De grafiek laat per bedrijfsgrootte zien welk deel tien of meer van die maatregelen heeft.

Aandeel bedrijven met tien of meer van de twaalf beveiligingsmaatregelen



WAT DIT LAAT ZIEN

Van de kleinste bedrijven heeft 13% de basis breed op orde, tegenover 86% van de grote. Juist de groep waar de meeste mkb-klanten in zitten, is het kwetsbaarst.

33%
van bedrijven met 2–10 medewerkers versleutelt data

91%
van bedrijven met 250+ medewerkers doet dat

Bron: CBS, Cybersecuritymonitor 2025 (28-05-2026)

De verzekeraar bepaalt steeds vaker de basis

Verzekeraars stellen eisen voordat ze een cyberrisico dekken, en gaan bij een claim na of de maatregelen er echt waren. Voor IT-partners worden die eisen daarmee een herkenbare basislijn in gesprekken met klanten.

19%

van de Nederlandse bedrijven is verzekerd voor cyberincidenten; in de ICT-sector 35% (CBS)

–4%

daling van cyberpremies wereldwijd in Q2 2026, het twaalfde kwartaal op rij (Marsh)

Premies dalen, maar de eisen worden niet soepeler. Dat maakt dit een goed moment om met klanten te bespreken of ze verzekerd zijn, en of ze aan de voorwaarden voldoen.

WAT VERZEKERAARS MEESTAL VRAGEN

- Tweestapsverificatie (MFA) op e-mail, toegang op afstand en beheeraccounts
- Detectie op werkplekken (EDR), bij grotere polissen met 24/7 monitoring
- Offline of onveranderbare back-ups met getest herstel
- Vaste termijnen voor updates
- Een incidentresponsplan en bewustwordingstraining

Let op: een onjuist ingevulde vragenlijst kan de dekking kosten.

Bron: CBS, Cybersecuritymonitor 2025 (28-05-2026); Marsh Global Insurance Market Index Q2 2026 (23-07-2026); eisen volgens MSP Business (01-10-2026) en Q-Cyber (commercieel)

05

De markt voor IT-dienstverleners

Hoe verandert de markt voor MSP's en IT-resellers: consolidatie, vendors, mensen en wat klanten verwachten.

5.1 Markt in cijfers
5.2 Vendors, prijzen en licenties
5.3 Arbeidsmarkt en capaciteit
5.4 De klant in beeld
5.5 Vraagstukken voor IT-partners

IMMTEC DATA PROTECTION & CYBERSECURITY

Consolidatie zet door

De Nederlandse markt voor managed services consolideert in hoog tempo. Investeerders bouwen platforms door MSP's samen te voegen. De cijfers komen van overnameadviseur Hogenhouck m&a, die zelf MSP-overnames begeleidt.

219
overnames in het Nederlandse MSP-segment van 2023 tot en met 2025

88%
van die overnames had een investeerder aan boord

±6
transacties per maand in 2025 en 2026

$1 mln
CSP-omzet per jaar die Microsoft nu vraagt van partners die rechtstreeks afnemen

WAAR KOPERS OP LETTEN

- Terugkerende omzet en lange contracten
- Spreiding over klanten
- Specialisatie in security, cloud of een sector

AI: ANGST ÉN VERSNELLER

Op MSP Global (oktober 2026, ruim 2.000 bezoekers) was AI het hoofdthema. MSP's zijn er volop mee bezig, maar de uitrol naar klanten blijft achter.

Bron: Hogenhouck m&a via TBM (12-02-2026) en Consultancy.nl (05-05-2026); Microsoft Partner Center; c't (27-10-2026)

Licenties en hardware worden duurder

Twee kostenposten stegen dit jaar tegelijk: Microsoft-licenties en hardware. Voor IT-partners betekent dat lastige gesprekken over prijzen, maar ook een reden om licenties en vervanging met klanten door te lichten.

MICROSOFT 365 PER 1 JULI 2026 (LIJSTPRIJS IN USD)

Licentie	Oud	Nieuw
Business Basic	$6,00	**$7,00**
Business Standard	$12,50	**$14,00**
Business Premium	$22,00	**$22,00**
Office 365 E3	$23,00	**$26,00**
Microsoft 365 E3	$36,00	**$39,00**
Frontline F3	$8,00	**$10,00**

Per gebruiker per maand, varianten met Teams. De nieuwe prijs geldt bij verlenging; prijzen in euro's kunnen afwijken.

HARDWARE: AI VRAAGT HET GEHEUGEN OP

+90–95%

verwachte stijging van contractprijzen voor werkgeheugen in het eerste kwartaal van 2026 (TrendForce)

Fabrikanten leveren eerst aan AI-datacenters. Pc's, laptops en servers werden daardoor duurder. Advies: leg vervangingsplanning en offertes vroeg vast.

Bron: Microsoft, 2026 M365 Packaging and Pricing Updates (16-02-2026); TrendForce (02-02-2026)

De krapte neemt af, maar niet voor specialisten

Jarenlang was personeel de grootste rem op groei in de IT. Dat beeld kantelt: het aantal vacatures daalt en werkgevers ervaren minder tekort. Voor specialistische functies blijft het zoeken.

589.000
mensen werken in een ICT-beroep; het aantal stijgt sinds 2023

18.900
openstaande ICT-vacatures in het tweede kwartaal van 2026; dalend sinds 2023

29%
van de werkgevers in informatie en communicatie noemt personeelstekort een belemmering (2022: 53%)

WAT ER VERANDERT

- Het aantal WW-uitkeringen vanuit de ICT stijgt, deels door reorganisaties
- AI automatiseert taken en vraagt meer specialistische kennis

WAT EEN IT-PARTNER ERMEE KAN

Minder krapte geeft ruimte om gericht te werven en eigen mensen op te leiden in security en AI: de kennis waar klanten om vragen.

Bron: UWV, Arbeidsmarktinformatie ICT-beroepen (10-2026) en Werkgeversonderzoek 2025 (02-2026)

Wat klanten van IT-dienstverleners verwachten

De Dutch IT Sourcing Study 2026 van Eraneos en Whitelane ondervroeg ruim 350 grote Nederlandse organisaties over hun IT-leveranciers. Het gaat om grote organisaties, maar de kritiek is ook voor mkb-dienstverleners herkenbaar.

WAAR LEVERANCIERS VOLGENS KLANTEN TEKORTSCHIETEN

45% daagt de klant te weinig uit

30% begrijpt het bedrijf van de klant onvoldoende

25% gedraagt zich niet als echte partner

VERDER OPVALLEND

- Gemiddelde tevredenheid over leveranciers: 75%
- 26% wil meer zelf gaan doen; vijf jaar geleden was dat 12 tot 13%
- 15% ziet al aanzienlijke impact van AI op het bedrijf; een jaar eerder 2%
- Belangrijkste reden om uit te besteden: schaalbaarheid (53%)

Bron: Eraneos en Whitelane Research, Dutch IT Sourcing Study 2026 (03-2026); Computable (21-04-2026)

Zes strategische vragen

Geen antwoorden, wel denkrichtingen. Elke vraag volgt uit de ontwikkelingen in dit rapport.

Schaal of specialisatie?

Consolidatie beloont schaal, maar klanten en kopers zoeken specialisten. Waar zit jullie onderscheid?

Compliance als dienst?

De Cbw, de CRA en ISO 27001 vragen om aantoonbaarheid. Kan dat een vaste dienst worden in plaats van een project?

Hoe soeverein is het portfolio?

Weet je per dienst waar klantdata staat, onder welk recht, en wat het exitscenario is?

Wie bewaakt AI-gebruik?

De meeste mkb'ers gebruiken AI, weinig hebben beleid. Wie helpt met afspraken, rechten en bewustzijn?

Hoe bewijs je continuïteit?

Herstel aantoonbaar en periodiek testen is een gesprek voor de directie, niet alleen voor IT.

Welke partners vullen aan?

Niemand hoeft alles zelf te bouwen. Verantwoordelijkheid spreiden verkleint ook het risico voor de klant.

06

Verdieping

Elk kwartaal één sector in de spotlight en de technologieën die IT-partners de komende jaren gaan raken.

6.1 Sector in de spotlight: handel, groothandel en automotive

6.2 Technologie op de radar

IMMTEC DATA PROTECTION & CYBERSECURITY

Handel, groothandel en automotive

Handel en autobranche horen volgens de AP bij de drie sectoren met de meeste datalekken door ransomware. Bedrijven in deze sector draaien op systemen die altijd beschikbaar moeten zijn, en zitten midden in een keten.

Top 3
handel en autobranche bij datalekken door ransomware in 2025, na zorg en voor ICT (AP)

6 op 10
groot- en detailhandelsbedrijven kende in 2025 de eigen NIS2-plichten niet (ABN AMRO)

WAAROM KWETSBAAR

- ERP, magazijn en webshop moeten continu draaien
- Veel koppelingen met leveranciers en vervoerders
- Stilstand werkt direct door: van distributiecentrum tot schap

RECENTE VOORBEELDEN

- Ahold Delhaize (oktober 2026): online en distributie deels stil
- Ceva Logistics (augustus 2026): klantgegevens van minstens twaalf opdrachtgevers gelekt
- Blue Yonder (november 2024): ketensoftware plat, supermarkten geraakt

Bron: AP, Rapportage ransomware 2025 via AG Connect (30-07-2026); ABN AMRO (14-07-2025); ICT Magazine (04-11 en 10-11-2026)

Wat de sector van IT-partners vraagt

VALT DE KLANT ONDER DE CYBERBEVEILIGINGSWET?

Levensmiddelen is een van de aangewezen sectoren. Een bedrijf in zo'n sector valt onder de wet bij 50 of meer medewerkers, of bij een omzet of balanstotaal boven € 10 miljoen. Twijfel? De zelfevaluatie van het NCSC geeft uitsluitsel. Handelsbedrijven die er niet onder vallen, krijgen wel vragen van klanten die er wel onder vallen.

Wat kost een dag stilstand?

Omzet per dag + loonkosten van medewerkers die niet kunnen werken + herstel + contractschade. Een concreet bedrag maakt continuïteit bespreekbaar bij de directie.

GESPREKSONDERWERPEN VOOR DEZE SECTOR

1. Hoe lang kan het magazijn draaien zonder ERP?
2. Zijn alle koppelingen met leveranciers en de webshop in beeld?
3. Is het herstel van het ERP-systeem ooit getest?
4. Wie meldt een incident aan klanten in de keten, en hoe snel?
5. Voldoen de maatregelen aan de eisen van de verzekeraar?

Bron: NCSC, 'Valt mijn organisatie onder de Cyberbeveiligingswet?'

Vier ontwikkelingen om te volgen

Niet elke technologische ontwikkeling vraagt nu om actie. De radar verdeelt ze in wat nu speelt, wat binnenkort komt en wat later relevant wordt, zodat je weet waar je kennis voor opbouwt.

NU

AI-assistenten

15% van de grote organisaties ziet al aanzienlijke impact van AI, tegen 2% een jaar eerder. Beleid, rechten en datalabeling worden basiswerk bij elke uitrol.

NU

24/7 detectie en respons

NCSC en NCTV adviseren continue logging, monitoring en detectie. Verzekeraars vragen er bij grotere polissen ook om.

BINNENKORT

Afscheid van Windows 10

De ondersteuning stopte in oktober 2025. Verlengde updates kosten $61 per apparaat in het eerste jaar en verdubbelen elk jaar, maximaal drie jaar.

LATER

Quantumveilige versleuteling

Volgens de Europese roadmap moeten toepassingen met een hoog risico eind 2030 zijn overgezet. Het NCSC adviseert nu te inventariseren.

Bron: Eraneos en Whitelane (03-2026); NCTV (06-11-2026); Microsoft Learn, Extended Security Updates; NCSC, Quantumveilige cryptografie

07

Aan de slag

Regelingen, events, deadlines en vragen om het gesprek met klanten te openen.

7.1 Regelingen en hulpmiddelen
7.2 Agenda
7.3 Deadlines en ijkmomenten
7.4 Gespreksvragen

IMMTEC DATA PROTECTION & CYBERSECURITY

Wat nu beschikbaar is voor het mkb

Voor kleine bedrijven is er subsidie en gratis hulp om de basis op orde te brengen. Een concrete aanleiding om nog dit jaar met kleine klanten in gesprek te gaan.

AANVRAGEN TOT EN MET 30 NOVEMBER 2026

Subsidie Mijn Cyberweerbare Zaak

50%
van de kosten van maatregelen

€ 1.250
maximaal per aanvrager

€ 1 mln
beschikbaar in 2026

Voor kleine bedrijven en zzp'ers. Doe de CyberVeilig Check, schaf de maatregelen aan, bewaar de facturen en vraag aan bij RVO.

VERDER BESCHIKBAAR

- CyberVeilig Check: het startpunt voor de subsidie
- NCSC: basisprincipes voor digitale weerbaarheid
- NCSC-zelfevaluatie: valt mijn organisatie onder de Cbw?
- Actieprogramma Toekomstbestendige Digitale Weerbaarheid van het kabinet, met onder meer betere voorbereiding van het mkb

Bron: NCSC, ncsc.nl/subsidie; NCTV (06-11-2026)

Agenda: MSP’s, cloud en security

Datum	Event	Locatie	Wat is het
2–3 dec 2026	Cloud Expo	Expo Houten	Beurs over cloud, AI en data
11 dec 2026	Making CRA a Reality	ENISA / Europese Commissie	Toelichting op de Cyber Resilience Act
19 jan 2027	Yellowhat	Almere	Microsoft Security-event voor SOC-analisten en MSSP’s
1–3 mrt 2027*	IT Nation Connect Europe	Londen	Event voor MSP’s van ConnectWise
15–18 mrt 2027	CloudFest	Rust (Duitsland)	Internationaal event voor cloud en hosting
17 mrt 2027	NLdigital Ondernemersdag	Woerden	Jaarlijkse dag van de brancheverenigingvoor IT-bedrijven
26–27 mei 2027	Cybersec Europe	Brussel	Securitybeurs met onder meer OT- en AI-security
31 mei–1 jun 2027	Experts Live Netherlands	Nieuwegein	Microsoft-community-event voor IT-professionals
8–10 jun 2027	Infosecurity Europe	Londen	Grote Europese securitybeurs
22–24 jun 2027	Kaseya Connect Europe	nog niet bekend	Event voor MSP’s van Kaseya
14 sep 2027	MSP Show NL en SITS	Jaarbeurs Utrecht	Beurs en seminars voor MSP’s, gratis toegang
15–16 sep 2027	Cybersec Netherlands	Jaarbeurs Utrecht	Securitybeurs voor experts en start-ups
5–6 okt 2027	ONE Conference	nog niet bekend	Cybersecurityconferentie van onder meer het NCSC
5–7 okt 2027	it-sa Expo&Congress	Neurenberg	Europese beurs voor IT-security

* Datum uit een overzicht van derden; de site van de organisator was niet te controleren.
Bron: websites van de organisatoren en it-agenda.nl, gecontroleerd op 12-11-2026; IT Nation: nuoptima.com (08-2026)

Agenda: andere vakgebieden en sectoren

Datum	Event	Locatie	Wat is het
19–23 jan 2027	NOT	Jaarbeurs Utrecht	Onderwijs: vakbeurs voor onderwijs en kinderopvang
28 jan 2027	Nationale Privacy Conferentie	Den Haag	Privacy: conferentie van ECP
2–5 feb 2027	Integrated Systems Europe (ISE)	Barcelona	AV en systeemintegratie
16–17 feb 2027	Kickstart Europe	Amsterdam	Datacenters en cloudinfrastructuur
16 mrt 2027	Security Leadership	Utrecht	Voor CISO's en IT-management
13–15 apr 2027	Zorg & ict	Jaarbeurs Utrecht	Zorg: grootste healthtech-beurs van Nederland
13 apr 2027	IT Asset Management	Vianen	Licentie- en assetbeheer
21 apr 2027	Cloud & AI in de Publieke Sector	Utrecht	Overheid: digitalisering en infrastructuur
20 mei 2027	Identity & Access Management	Den Bosch	Toegangsbeheer, voor IAM-managers en CISO's
2 jun 2027	Cyberweerbare Overheid	Den Haag	Overheid: voor CISO's en ICT-managers
15–16 sep 2027	Data Expo	Jaarbeurs Utrecht	Data, AI en business intelligence
9 nov 2027	AI & Automation Day	Utrecht	AI en automatisering in de bedrijfsvoering
25 nov 2027	Cyber Security Experience	Utrecht	Voor security- en ICT-managers

Events buiten de eigen bubbel: hier kom je de IT-verantwoordelijken van klanten in zorg, onderwijs, overheid en industrie tegen.

Bron: Jaarbeurs, zorg-en-ict.nl, data-expo.nl, iseurope.org, heliview.com en it-agenda.nl, gecontroleerd op 12-11-2026

Data om in de gaten te houden

De belangrijkste data uit dit rapport op een rij, in volgorde van tijd.

30 nov 2026	**Laatste dag voor de subsidie Mijn Cyberweerbare Zaak**
eind 2026	Eerste applicaties op de soevereine overheidscloud
eind 2026	Nationale quantum-roadmap per EU-lidstaat
11 dec 2027	Cyber Resilience Act volledig van toepassing
2028	Het kabinet wil een Nederlandse of Europese partij voor DigiD
2030	Einde van de overgangstermijn van vier jaar voor het Rijkscloudbeleid
eind 2030	Toepassingen met hoog risico quantumveilig (EU-roadmap)

Bron: NCSC; Rijksoverheid (03-07-2026); Computable (03-07-2026); Jones Day (07-2026); MSP Business (27-08-2026)

Tien vragen om met klanten te bespreken

Elke ontwikkeling in dit rapport laat zich vertalen naar een eenvoudige vraag aan een klant. Geen verkooppraatje, wel een opening voor een goed gesprek.

01 Levert u aan organisaties die onder de Cyberbeveiligingswet vallen?

02 Wat kost één dag stilstand, in euro's?

03 Wanneer is het herstel van uw systemen voor het laatst getest?

04 Zijn uw back-ups bereikbaar voor een aanvaller die al binnen is?

05 Onder welk recht vallen uw belangrijkste clouddiensten?

06 Heeft u een exitscenario voor uw kritieke diensten?

07 Welke AI-tools gebruiken uw medewerkers, en met welke data?

08 Wie in de directie is eigenaar van cyberrisico's?

09 Voldoet u aan de eisen van uw cyberverzekering?

10 Is uw incidentresponsplan ooit geoefend?

Over dit trendrapport

Het Trendrapport IT-kanaal verschijnt elk kwartaal en bundelt wat er speelt voor IT-partners en hun mkb-klanten. De inhoud is gebaseerd op openbare bronnen en geeft de stand van zaken bij publicatie. Dit rapport is geen juridisch advies.

VOLGENDE EDITIE

Q1 2027

IMMUTEC is een Europese Managed Service Provider voor data protection en cybersecurity. Delen en verder gebruiken mag, met bronvermelding. De bronnen staan per pagina vermeld; ‘via’ betekent dat een cijfer uit een tussenbron is overgenomen.

immutec.eu · info@immutec.eu · +31 (0)85 482 3400

Trendrapport IT-kanaal Q4 2026 · NL V0.5 · Druk- en zetfouten voorbehouden.

IMMUTEC DATA PROTECTION & CYBERSECURITY