cuccibu
Reduce Risk, Create Value

CUCCIBU'S
INSIGHT OF THE MONTH

Een terugblik op het nieuws van de afgelopen weken:

- Cybersecuritymonitor 2025: minder cyberaanvallen, weerbaarheidskloof blijft bestaan.
- Generatieve AI belangrijkste IT-trend voor 2026.
- Digitale soevereiniteit hoger op de agenda.
- Explosieve stijging van privacyklachten.
- Shadow AI vergroot risico op datalekken.

Information Security

Cybersecuritymonitor 2025: minder cyberaanvallen, weerbaarheidskloof blijft bestaan

28 mei 2026 - De Cybersecuritymonitor 2025 laat zien dat Nederlandse organisaties minder cyberaanvallen ervaren dan voorgaande jaren.

Het percentage bedrijven dat te maken kreeg met een cyberincident door een aanval van buitenaf daalde van 11% in 2016 naar 4% in 2024. Daarmee is sprake van het laagste incidentcijfer sinds de start van de metingen. Toch is er geen reden om achterover te leunen.

De kloof in cyberweerbaarheid tussen grote en kleine organisaties blijft bestaan. Grotere organisaties investeren vaker in cybersecuritymaatregelen, terwijl kleinere organisaties en zzp'ers hierin achterblijven. Hierdoor ontstaat een weerbaarheidskloof die cybercriminelen kunnen benutten.

Bovendien blijven phishing, spoofing en andere vormen van digitale fraude veelvoorkomende dreigingen.

Wat betekent dit voor jouw organisatie?
Cyberweerbaarheid is geen project, maar een continu proces. Investeer in een goede balans tussen technische, organisatorische en menselijke maatregelen. Juist voor kleinere organisaties is het belangrijk om cybersecurity structureel te verankeren binnen de organisatie.

Bron: NCSC

Information Security Privacy

Generatieve AI belangrijkste IT-trend voor 2026

3 juni 2026 - Generatieve AI wordt door organisaties gezien als de belangrijkste IT-trend voor 2026. Dat blijkt uit het jaarlijkse trendonderzoek van Supply Value onder IT-beslissers.

AI ontwikkelt zich daarmee verder van experimentele technologie naar een vast onderdeel van de bedrijfsvoering. Organisaties verwachten AI steeds vaker in te zetten voor automatisering, kennismanagement, productiviteitsverbetering en ondersteuning van medewerkers. Tegelijkertijd groeit de behoefte aan duidelijke governance, risicobeheersing en compliance rondom AI-toepassingen.

De rode draad dit jaar bestaat uit drie elementen die in vrijwel alle trends terugkeren: weerbaarheid, innovatie en digitale autonomie. Daarbovenop hebben geopolitieke ontwikkelingen en de snelle opmars van AI grote invloed op strategische keuzes.

Een belangrijk inzicht uit het onderzoek is dat organisaties deze ontwikkelingen niet langer los van elkaar kunnen benaderen. Succes vraagt om een samenhangende aanpak waarin technologie, governance, veiligheid en innovatie elkaar versterken.

Bron: Consultancy.nl

Information Security

Digitale soevereiniteit hoger op de agenda

3 juni 2026 - Digitale soevereiniteit staat steeds hoger op de politieke en bestuurlijke agenda. Geopolitieke spanningen, strengere regelgeving en de groeiende afhankelijkheid van Amerikaanse cloud- en technologiebedrijven maken het thema urgenter dan ooit.

Ook Aleid Wolfsen, voorzitter van de Autoriteit Persoonsgegevens (AP), waarschuwt dat Nederland voor essentiële digitale diensten te afhankelijk is geworden van Amerikaanse techbedrijven. Deze afhankelijkheid brengt risico's met zich mee op het gebied van privacy, continuïteit en controle over data.

In dit kader presenteerde de Europese Commissie in juni het langverwachte **EU Tech and Sovereignty Package**. Dit wetgevingspakket moet de digitale autonomie van Europa versterken en de afhankelijkheid van buitenlandse technologieaanbieders verminderen.

Een belangrijk onderdeel hiervan is de **Cloud and Data Center Act** (CADA). Deze wet moet de Europese digitale infrastructuur (in ongekend tempo) toekomstbestendig maken door onder andere:

- de afhankelijkheid van niet-Europese cloud-aanbieders te verminderen;
- de Europese datacentercapaciteit op een duurzame en energie-efficiënte manier uit te breiden;
- maatschappelijk verantwoorde innovatie op het gebied van AI te bevorderen en versnellen.

Daarnaast bevat het pakket maatregelen zoals een verplichte soevereiniteitsbeoordeling voor cloudtechnologie, een Europese open-source strategie en het principe 'publiek geld, publieke code'.

De Vereniging van Nederlandse Gemeenten (VNG) reageert positief op de plannen. Tegelijkertijd benadrukt zij dat de overgang naar meer digitale autonomie een grote verandering vraagt, waarbij aandacht voor uitvoerbaarheid en haalbaarheid essentieel is.

Bron: Security.nl, Dutch IT Leaders, VNG

Privacy

Explosieve stijging van privacyklachten

8 juni 2026 - De Autoriteit Persoonsgegevens ontving in 2025 ruim 13.500 klachten en signalen over mogelijke privacyschendingen. Dat is een stijging van maar liefst 75% ten opzichte van een jaar eerder.

Veel klachten gaan over organisaties die onvoldoende transparant zijn over het gebruik van persoonsgegevens of verzoeken van betrokkenen niet correct afhandelen. De stijging laat zien dat burgers zich steeds bewuster zijn van hun privacyrechten en sneller actie ondernemen wanneer zij vinden dat deze worden geschonden.

Ook over datalekken kwamen veel meldingen binnen. Meer dan de helft daarvan hield verband met het datalek bij Clinical Diagnostics. Daarna volgden klachten over zakelijke dienstverleners en de overheid.

Wat betekent dit voor jouw organisatie?
Controleer regelmatig of privacyprocessen nog effectief functioneren én voldoen aan de AVG. Denk hierbij aan het afhandelen van inzage-, correctie- en verwijderverzoeken en het transparant informeren van betrokkenen over het gebruik van persoonsgegevens.

Bron: Autoriteit Persoonsgegevens

Information Security | Privacy

Shadow AI vergroot risico op datalekken

15 juni 2026 - De Europese privacytoezichthouder waarschuwt voor de groei van Shadow AI: het gebruik van AI-tools door medewerkers zonder medeweten of goedkeuring van de organisatie.

Steeds meer werknemers ontdekken hoe generatieve AI hun werkzaamheden efficiënter kan maken. Daarbij worden regelmatig persoonsgegevens, vertrouwelijke informatie of bedrijfsgegevens ingevoerd in publieke AI-tools.

Het grootste risico zit vaak niet in onwil, maar in onbekendheid. Medewerkers willen AI gebruiken, maar weten niet altijd hoe dit veilig en verantwoord kan. Hierdoor ontstaan risico's op datalekken, verlies van controle over gegevens en overtredingen van privacywetgeving.

Daarnaast ontstaat een 'blinde vlek' voor organisaties. Zodra gegevens worden ingevoerd in een niet-goedgekeurd AI-systeem, is het vaak moeilijk te achterhalen waar deze informatie terechtkomt, hoe deze wordt gebruikt en of deze wordt ingezet voor het trainen van modellen.

Wat betekent dit voor jouw organisatie?
Het verbieden van AI-tools is meestal niet de oplossing. Medewerkers vinden vaak toch alternatieven. Effectiever is het om AI-gebruik actief te faciliteren en te begeleiden. Zorg voor duidelijke richtlijnen, bewustwording onder medewerkers en veilige, goedgekeurde AI-oplossingen die aansluiten bij de behoeften van medewerkers.

Bron: Security.nl, NOS