cuccibu
Reduce Risk, Create Value

CUCCIBU'S
INSIGHT OF THE WEEK

Een terugblik op het nieuws van de afgelopen weken:

- Koninkrijk der Nederlanden richt Cyberweerbaarheidsnetwerk op
- Europese Commissie wil cookiewetgeving versoepelen
- AI Governancekader voor gemeenten
- Cyberdreigingen en stilstand grootste risico's voor bedrijven
- Phishing en kwetsbaarheden vaakst gebruikt bij cyberaanvallen

Data Security

Koninkrijk der Nederlanden richt Cyberweerbaarheidsnetwerk op

10 september 2025 - De huidige cyberdreigingen zijn niet meer op te vangen met losse initiatieven. Daarom komt er een **Cyberweerbaarheidsnetwerk (CWN)**: een samenwerking tussen publieke én private organisaties om de digitale weerbaarheid in het Koninkrijk der Nederlanden te versterken.

Het NCSC heeft hiervoor samen met partners een bouwplan opgesteld, dat voortbouwt op de Toekomstvisie Cyberweerbaarheidsnetwerk (NCTB) en de Nederlandse Cybersecuritystrategie 2022–2028.

Wat zit in het bouwplan?
Het plan noemt vijf kernfuncties, inclusief concrete doelen, benodigde activiteiten en randvoorwaarden.

1. Informatiedeling
2. Doelwit- en slachtoffernotificatie
3. Incidentafhandeling
4. Kennisuitwisseling
5. Opleiden, trainen en oefenen

Het bouwplan fungeert als routekaart. Het groeit mee met de praktijk en nodigt uit tot verdere ontwikkeling.

Waarom is dit relevant?
Cyberweerbaarheid is een gedeelde verantwoordelijkheid. Dit netwerk brengt structuur, synergie en schaalbaarheid. Daarnaast biedt het publieke én private organisaties in het hele Koninkrijk, inclusief de overzeese gebieden, de kans om kennis te bundelen en samen op te trekken tegen digitale dreigingen. Want alleen samen worden we echt weerbaar.

Bron: Nationaal Cyber Security Centrum

Data Privacy

Europese Commissie wil cookiewetgeving versoepelen

22 september 2025 - De Europese Commissie overweegt de cookiewetgeving te versoepelen en vereenvoudigen. Brussel wil bepaalde lastige eisen schrappen en nieuwe uitzonderingen toestaan, zodat gebruikers niet op elke website afzonderlijk een cookiebanner hoeven te accepteren.

Wat verandert er mogelijk?
Volgens de plannen zouden bepaalde regels uit de huidige ePrivacy-richtlijn worden geschrapt of aangepast. Op dit moment moeten websites nog voor vrijwel alle cookies toestemming vragen (behalve strikt noodzakelijke cookies). De nieuwe aanpak zou bijvoorbeeld toestaan dat gebruikers hun voorkeuren centraal via hun browser kunnen instellen.

Wat is de status?
Het was de bedoeling dat de ePrivacy Richtlijn door de ePrivacy Verordening zou worden vervangen. Dit voorstel is al eerder ingetrokken. Brussel werkt nu aan een zogeheten “omnibus”-voorstel dat in december wordt verwacht. Hierin zouden meerdere verplichtingen voor bedrijven worden geschrapt. Concrete details zijn op dit moment nog niet bekend.

Kritiek vanuit privacyhoek
Privacyorganisaties zijn kritisch en waarschuwen dat deze versoepeling mogelijk de AVG-waarborgen onder druk zet. Zij vrezen dat de focus op gebruiksgemak en minder regeldruk ten koste kan gaan van fundamentele privacyrechten van gebruikers.

Bron: Security.nl

Data Privacy

AI Governancekader voor gemeenten

23 september 2025 - Gemeenten zetten steeds vaker AI en algoritmen in, bijvoorbeeld voor virtuele assistenten, transcriptietools of anonimiseringssoftware. Maar hoe doe je dat veilig en verantwoord?

Op 23 september lanceerde de VNG samen met diverse gemeenten een governancekader voor de ethische, transparante en veilige inzet van AI. Het biedt praktische handvatten voor het inkopen, ontwikkelen, beheren en implementeren van AI-toepassingen.

Via aigovernance.vng.nl vinden gemeenten een kennisbank met:

- Instrumenten, definities en kaders;
- Inzicht in rollen, taken en verantwoordelijkheden;
- Processtappen voor AI-ontwikkeling en -gebruik.

Doel is risico's zoals privacyschending of discriminatie te beperken, én gemeenten klaar te stomen voor de strengere Europese AI-regelgeving.

Belangrijk om te weten: dit kader is geen eindpunt, maar een groeimodel. Gemeenten worden actief uitgenodigd om mee te denken, te testen en te leren.

Waarom relevant?
AI is niet meer weg te denken, ook niet in het publieke domein. Maar zonder duidelijke governance lopen organisaties forse risico's. Dit kader biedt een waardevol startpunt om AI slim én verantwoord in te zetten, iets waar ook andere sectoren van kunnen leren.

Bron: VNG

Data Security

Cyberdreigingen en stilstand grootste risico's voor bedrijven

2 oktober 2025 - Bedrijven staan wereldwijd onder toenemende druk van een risicolandschap dat complexer en onvoorspelbaarder is dan ooit. Volgens de laatste Global Risk Management Survey van Aon blijkt dat cyberaanvallen opnieuw het grootste risico vormen, gevolgd door bedrijfsstilstand.

- **Cyberdreigingen** nemen niet alleen in aantal toe, maar ook in complexiteit. Waardoor de potentiële impact en risico ook blijft groeien.
- **Bedrijfsstilstand** ontstaat steeds vaker door verstoorde toeleveringsketens, klimaat gerelateerde incidenten, geopolitieke spanningen en uitval van personeel

Nieuwkomer: AI als toekomstig risico
Hoewel AI-incidenten nu nog schaars zijn, verwachten experts dat dit snel verandert. De bekendste risico's zijn privacy en dataveiligheid maar ook bias en transparantie. AI-systemen verwerken enorme hoeveelheden (gevoelige) data, nemen soms bestaande vooroordelen over en maken het moeilijk te herleiden hoe beslissingen tot stand komen.

Wat betekent dit voor organisaties?
Het huidige risicolandschap vraagt om een fundamenteel andere aanpak: niet langer focussen op beperking en beheersing, maar risicomanagement inzetten als motor voor innovatie en concurrentievoordeel.

Geen enkel bedrijf kan elk incident voorkomen. De sleutel ligt in wendbaarheid, robuuste respons en anticipatie. Bedrijven die risicomanagement koppelen aan strategie, samenwerking bevorderen en data slim gebruiken, bouwen aan echte veerkracht.

Bron: consultancy.nl, Global Risk Management Survey (Aon)

Data Security

Phishing en kwetsbaarheden vaakst gebruikt bij cyberaanvallen

2 oktober 2025 - Volgens het nieuwste Threat Landscape-rapport van ENISA zijn phishing en misbruik van kwetsbaarheden de meest gebruikte methoden bij cyberaanvallen op systemen in Europa.

- Bij 60% van de onderzochte incidenten bleek phishing de initiële aanvalsvector te zijn. Dit ging niet alleen om e-mail phishing maar ook telefonische phishing en e-mails met besmette bijlagen.
- Bij 21% van de incidenten werd misbruik van kwetsbaarheden vastgesteld als de oorzaak.
- De impact van phishing is vaak onbekend (73%). In 27% leidde de phishing wel tot een daadwerkelijke inbraak, en bij ongeveer een kwart werd daadwerkelijk malware geïnstalleerd.
- Wanneer kwetsbaarheden worden misbruikt, leidt dit in 70% van de gevallen tot een daadwerkelijke inbraak. Vaak gevolgd door malware zoals ransomware.

Bescherm je organisatie
Phishing en kwetsbaarheden blijven de favoriete aanvalsroutes, en ze zijn nog steeds effectief. Versterk daarom de weerbaarheid van je organisatie met een aantal impactvolle maatregelen.

- **Bewustwordingstraining**: leer medewerkers verdachte mails herkennen en melden.
- **Gebruik multifactor-authenticatie** (MFA): verklein de kans dat gestolen inloggegevens misbruikt worden.
- **E-mailfiltering**: voorkom dat phishingmails medewerkers bereiken.
- **Patch en update regelmatig**: los kwetsbaarheden snel op met automatische updates of patchmanagement.
- **Test je verdediging**: voer regelmatig phishing-simulaties en penetratietesten uit om zwakke plekken te ontdekken.

Kortom: de basis blijft bepalend. Door mens, proces en techniek te combineren, verklein je de kans op succesvolle aanvallen én beperk je de schade als het toch misgaat.

Bron: Security.nl