cuccibu
Reduce Risk, Create Value

CUCCIBU'S
INSIGHT OF THE WEEK

Een terugblik op het nieuws van de afgelopen week:

- Google waarschuwt voor telefonische phishing van Salesforce-klanten
- UWV lekte door fout bij versturen van e-mail gezondheidsgegevens cliënten
- Schepen Nederlands offshorebedrijf Allseas gaan op kernenergie varen
- Meer dan 150 Nederlandse gemeenten betrokken bij ransomware-incidenten
- Grondrechten burgers onvoldoende beschermd bij AI-gebruik door politie

Data Security

Google waarschuwt voor telefonische phishing van Salesforce-klanten

4 juni 2025 - Google slaat alarm over een gerichte phishing tegen organisaties die gebruikmaken van Salesforce. Aanvallers, bekend als UNC6040, maken gebruik van telefonische social engineering om toegang te krijgen tot bedrijfsdata.

Ze doen zich voor als helpdeskmedewerkers van Salesforce en weten zo medewerkers te overtuigen om: inloggegevens te delen, toegang te verlenen of een gemanipuleerde versie van Salesforce Data Loader te installeren.

De risico's van phishing
Telefonische phishing – ook wel voice pishing of spoofing genoemd – is steeds geavanceerder geworden. Aanvallers gebruiken geloofwaardige scripts, valse telefoonnummers en social engineeringtechnieken om hun doel te bereiken. De gevolgen van een succesvolle phishing aanval zijn enorm:

- Infiltratie van het netwerk via kwaadaardige malware;
- Diefstal of versleuteling van gegevens (ransomware);
- Financiële of reputatieschade door afpersing;
- Laterale bewegingen richting andere systemen;
- Verstoring van de bedrijfscontinuïteit.

Bescherming tegen phishing
Effectieve bescherming vraagt om een combinatie van technische én menselijke maatregelen. Naast de technische beheersmaatregelen is het vergroten van bewustwording binnen de organisatie minstens zo belangrijk. Train medewerkers om verschillende vormen van phishing herkennen én om gepast te reageren.

Bron: Security.nl

Data Privacy

UWV lekte door fout bij versturen van e-mail gezondheidsgegevens cliënten

4 juni 2025 - In Q1-2025 heeft het UWV in totaal 216 datalekken gemeld bij de Autoriteit Persoonsgegevens (AP). Dit blijkt uit de recent gepubliceerde rapportage Stand van de uitvoering sociale zekerheid. Twee incidenten ontstonden door menselijke fouten bij het verzenden van e-mails.

Incident 1 - januari: interne e-mail met persoonsgegevens naar cliënt
Een interne e-mail met een bijlage die persoons- en gezondheidsgegevens van cliënten bevatte, werd per ongeluk naar een cliënt gestuurd. De ontvanger gaf aan de e-mail ongeopend te hebben verwijderd. Het UWV heeft zowel de betrokken cliënten als de AP geïnformeerd en is een onderzoek gestart naar de mogelijkheid om dit soort documenten via een centrale, veilige omgeving te delen — zodat verzending via e-mail in de toekomst niet meer nodig is.

Incident 2 - februari: mail met persoonsgegevens naar verkeerde afnemer
Een e-mail met twee bestanden, met persoonsgegevens van 158 personen, werd naar een verkeerde afnemer verstuurd. Ook dit datalek is gemeld bij de AP. Volgens het UWV bieden contractuele afspraken en gedragscodes voldoende bescherming voor de betrokkenen. Daarom is besloten hen niet persoonlijk te informeren. De ontvanger heeft bevestigd dat de bestanden direct zijn verwijderd.

Lessen voor organisaties
Deze incidenten onderstrepen het belang van:

- Veilige communicatiekanalen voor het delen van gevoelige informatie.
- Training en bewustwording bij medewerkers over privacy
- Implementatie van technische maatregelen
- Heldere datalekprocedures.

Door deze maatregelen te nemen, verklein je niet alleen het risico op datalekken, maar zorg je er ook voor dat je als organisatie snel en adequaat kunt reageren wanneer het toch misgaat.

Bron: Security.nl

QHSE

Schepen Nederlands offshorebedrijf Allseas gaan op kernenergie varen

5 juni 2025 - Het Nederlandse offshorebedrijf Allseas heeft aangekondigd dat zijn grote installatieschepen vanaf 2030 op kernenergie zullen varen. In samenwerking met de Technische Universiteit Delft ontwikkelt het bedrijf een kleine modulaire kernreactor (SMR) op basis van hoge temperatuur-gasgekoelde technologie. Deze reactoren zijn speciaal ontworpen voor langdurige en intensieve operaties op zee, waar het bijtanken van duurzame brandstoffen vaak een uitdaging is.

Met deze innovatie wil Allseas zijn CO2-uitstoot in 2030 met 30% reduceren en in 2050 volledig klimaatneutraal opereren. De keuze voor kernenergie komt voort uit de beperkte beschikbaarheid en hoge kosten van andere schone brandstoffen zoals waterstof, methanol en ammoniak.

Een noodzakelijke stap richting verduurzaming
Allseas is de eerste grote reder ter wereld die een overstap naar kernenergie aankondigt. De stap komt op een moment dat de druk op de scheepvaartsector toeneemt: de Internationale Maritieme Organisatie (IMO) heeft recent de emissienormen aangescherpt. Niet voor niets, want de internationale zeevaart is verantwoordelijk voor ongeveer 3% van de wereldwijde uitstoot van broeikasgassen.

Verduurzaming is daarmee geen keuze meer, maar een noodzaak. Door te investeren in kernenergie als emissievrije oplossing, levert Allseas een krachtige bijdrage aan het Nederlandse Klimaatakkoord en de Europese Green Deal.

Koploper in schone zeevaart
Volgens Annet Koster (directeur Koninklijke Vereniging van Nederlandse Reders) kan de techniek van Allseas Nederland een koppositie geven in duurzame zeevaart. Bovendien versterkt kernenergie de Europese energiezekerheid en vermindert het de afhankelijkheid van buitenlandse brandstoffen.

Bron: NOS

Data Security

Meer dan 150 Nederlandse gemeenten betrokken bij ransomware-incidenten

5 juni 2025 - Uit het Dreigingsbeeld Informatiebeveiliging 2025–2026 van de Informatiebeveiligingsdienst (IBD) van de VNG blijkt dat ruim 150 Nederlandse gemeenten in de periode 2023–2024 direct of indirect betrokken zijn geweest bij ransomware-incidenten. Ook datalekken door phishing en menselijke fouten zijn een groeiende bedreiging.

Toenemende afhankelijkheid van toeleveranciers
De IBD merkt op dat steeds meer gemeentelijke ICT als dienst wordt afgenomen, wat de kwetsbaarheid in de keten vergroot. Ransomware of phishing bij leveranciers leidt regelmatig tot grootschalige incidenten, met uitval van essentiële gemeentelijke processen als gevolg. Deze toenemende ketenafhankelijkheid benadrukt de noodzaak voor gemeenten om duidelijke beveiligingseisen te stellen aan leveranciers, en actief regie te voeren op continuïteit bij uitbestede diensten.

Aanbevelingen voor versterking digitale weerbaarheid
Het rapport benadrukt dat digitale veiligheid niet alleen een technische, maar ook een bestuurlijke verantwoordelijkheid is. Met de komst van de NIS2 wordt dit zelfs een expliciete verplichting. Bestuurders worden dan ook opgeroepen om digitale risico’s structureel te integreren in hun beleid en besluitvorming. Om de digitale weerbaarheid te vergroten, worden de volgende maatregelen aanbevolen:

- **Implementatie van basismaatregelen**: zoals multifactorauthenticatie, netwerksegmentatie, monitoring, strikte toegangsrechten en regelmatige back-ups.
- **Veilig opdrachtgeverschap**: maak duidelijke afspraken met leveranciers over beveiliging, incidentrespons en dataminimalisatie.
- **Collectieve samenwerking**: bundel kennis, capaciteit en inkoopkracht tussen gemeenten.
- **Voorbereid crisisteam**: zorg voor continuïteitsscenario’s en een doordacht communicatieplan om de dienstverlening snel te herstellen.

Bron: Security.nl en Dreigingsbeeld Informatiebeveiliging 2025-2026 (IBD)

Data Privacy

Grondrechten burgers onvoldoende beschermd bij AI-gebruik door politie

5 juni 2025 - De Wetenschappelijke Adviesraad Politie (WARP) luidt in het rapport “Navigeren in Niemandsland” de noodklok over het gebruik van AI door de politie. Door de razendsnelle technologische ontwikkeling en het ontbreken van een adequaat wettelijk kader zijn de grondrechten van burgers onvoldoende beschermd bij datagedreven politiewerk. De balans tussen veiligheidsbelangen en burgerrechten is zoek.

Aanbevelingen voor verantwoord AI-gebruik.
De WARP doet concrete aanbevelingen om de inzet van AI ethisch en effectief te laten verlopen:

- **Ontwikkel passend wettelijk kader**: herzie wet- en regelgeving rondom datagedreven politiewerk om privacy en andere grondrechten beter te waarborgen.
- **Stel een onafhankelijke evaluatiecommissie in**: voor toezicht op de toepassing van de Wet politiegegevens en AI-toepassingen.
- **Zorg voor transparantie**: hanteer het principe 'openbaar, tenzij' voor het gebruik van AI binnen de politie. Communiceer actief en transparant over de inzet van AI, binnen een ethisch en juridisch raamwerk.
- **Formuleer strikte voorwaarden voor samenwerking met private partijen**: inclusief een toetsings- en samenwerkingskader dat publieke waarden beschermt en afhankelijkheid beperkt.
- **Investeer in een digitale mindset**: een kritische digitale houding en AI-geletterdheid moeten basisvaardigheden zijn binnen de politieorganisatie.
- **Breng de interne datahuishouding op orde**: Goed databeheer is essentieel om fouten, vooroordelen en misbruik te voorkomen. AI-governance moet integraal onderdeel zijn van de bredere organisatie-governance.
- **Versterk vertrouwen via ‘positieve veiligheid’**: stimuleer AI-toepassingen die de relatie met burgers verbeteren en bijdragen aan maatschappelijke legitimiteit.
- **Onderzoek effectiviteit van AI-toepassingen**: meer empirisch (kwalitatief én kwantitatief) onderzoek is nodig naar de werkelijke impact van AI binnen de politiepraktijk.
- **Neem publieke afstand van voorspellende AI op persoonsniveau**: vermijd algoritmes die crimineel gedrag proberen te voorspellen per individu, en communiceer dit expliciet.

Bron: Security.nl, NieuwRechts en Navigeren in niemandsland (WARP)