cuccibu
Reduce Risk, Create Value

CUCCIBU'S
INSIGHT OF THE WEEK

Een terugblik op het nieuws van de afgelopen week:

- IT wordt vaak vergeten in de duurzaamheidsstrategie
- Air France-KLM getroffen door datalek: klantgegevens gestolen
- OM na cyberaanval weer bereikbaar per mail
- Veiligheidsregio's onvoldoende voorbereid op landelijke stroomuitval

QHSE

IT wordt vaak vergeten in de duurzaamheidsstrategie

30 juli 2025 - Steeds meer organisaties zijn actief bezig met duurzaamheid. Ze vergroenen hun wagenpark, stappen over op groene energie en herzien hun leverancierskeuzes. Maar opvallend genoeg blijft één belangrijke categorie vaak buiten beeld: IT-hardware.

Juist in IT schuilt een grote, vaak onzichtbare milieu-impact. De meeste CO_2-uitstoot van een laptop, tablet of smartphone ontstaat niet tijdens het gebruik, maar al vóór het apparaat is ingeschakeld - tijdens de productie, het transport en door de korte levensduur. Toch vervangen veel bedrijven hun apparatuur al na drie tot vijf jaar, terwijl deze technisch vaak nog prima functioneert. Dit lineaire patroon van kopen, gebruiken, weggooien is niet langer houdbaar.

Tijd om circulair te denken. Wat kun je doen?

1. **Investeer in circulaire hardware.** Kies voor pre-owned, refurbished of modulair ontworpen apparatuur. Zo verleng je de levensduur én verklein je de CO_2-impact.
2. **Verleng wat je al hebt.** Zorg voor tijdig onderhoud en hergebruik apparaten binnen andere afdelingen. Wat voor de één verouderd is, kan voor de ander nog prima werken.
3. **Integreer lifecycle management.** Denk bij je IT-beleid niet alleen aan aanschaf, maar ook aan onderhoud, hergebruik en verantwoorde afvoer. Werk bijvoorbeeld met terugnameprogramma's of sociale ondernemingen voor de herbestemming van oude apparatuur.
4. **Maak duurzaamheid onderdeel van inkoop.** Kies leveranciers die transparant zijn over hun milieu-impact en aantoonbaar duurzaam handelen.

Een circulaire IT-strategie is niet alleen goed voor het milieu, maar bespaart ook kosten én sluit aan bij ESG-, CSRD- en VSME-rapportageverplichtingen. Kortom: **wil je écht duurzaam ondernemen? Vergeet dan je IT niet.**

Bron: duurzaam-actueel

Data Privacy

Air France-KLM getroffen door datalek: klantgegevens gestolen

6 augustus 2025 - Luchtvaartmaatschappij Air France-KLM is getroffen door een datalek. Aanvallers wisten toegang te krijgen tot, een niet nader genoemd, extern platform dat de luchtvaartmaatschappij voor de klantenservice gebruikt. Daarbij zijn persoonlijke gegevens zoals namen, contactinformatie, Flying Blue-nummers en onderwerpregels van e-mails gestolen. Hoeveel klanten zijn gedupeerd, laat KLM niet weten.

Datalek gemeld en beveiligingsmaatregelen getroffen
Er zijn beveiligingsmaatregelen genomen om ongeautoriseerde toegang te stoppen en herhaling te voorkomen. De interne systemen van KLM en Air France zijn niet geraakt. Gevoelige gegevens zoals wachtwoorden, reisgegevens of paspoort- en creditcardinformatie zijn volgens de luchtvaartmaatschappij niet gestolen.

Klanten zijn gewaarschuwd en geadviseerd alert te blijven voor phishingpogingen. Het incident is gemeld bij de Nederlandse Autoriteit Persoonsgegevens (AP) en de Franse privacytoezichthouder CNIL.

Wat kunnen we hiervan leren?
Dit voorval laat zien hoe kwetsbaar externe platforms in de keten kunnen zijn, zelfs wanneer de interne systemen goed beveiligd zijn. Voor organisaties is het cruciaal om ook derde partijen te onderwerpen aan strenge beveiligingseisen en monitoring.

Voor klanten geldt: wees extra alert op verdachte e-mails of communicatie die namens KLM lijkt te komen, vooral als daarin om persoonlijke gegevens wordt gevraagd. Controleer altijd het e-mailadres van de afzender en klik niet zomaar op links.

Bron: NOS, KLM en Security.nl

Data Security

OM na cyberaanval weer bereikbaar per mail

7 augustus 2025 - Drie weken nadat het Openbaar Ministerie (OM) zijn systemen deels offline haalde vanwege een cyberdreiging, is de organisatie inmiddels weer bereikbaar via e-mail voor externe partijen. De maatregel werd op 17 juli genomen na een waarschuwing van het Nationaal Cyber Security Centrum (NCSC) over mogelijk misbruik van een kwetsbaarheid in Citrix NetScaler – software die gebruikt wordt voor externe toegang tot het netwerk.

Kwetsbaarheid ondanks updates misbruikt
Hoewel het OM de door Citrix verstrekte beveiligingsupdates op tijd had geïnstalleerd, blijkt nu dat aanvallers toch toegang hebben gekregen tot de Citrix-servers. Daarmee is het lek (CVE-2023-3519), waarvoor al sinds juni werd gewaarschuwd, daadwerkelijk benut.

Omvang van de schade nog onbekend
Hoe diep de hackers in de systemen zijn binnengedrongen en of er informatie is buitgemaakt, is vooralsnog onduidelijk. Volgens voormalig AIVD-toezichthouder Bert Hubert is het risico groot, omdat Citrix directe toegang biedt tot alle gegevens die medewerkers op afstand kunnen inzien. Het is dus aannemelijk dat de aanvallers konden meekijken met deze gegevens.

E-mail weer in de lucht, met beperkingen
Het OM heeft inmiddels extra beveiligingsmaatregelen getroffen en de e-mailfunctionaliteit hersteld. Wel vraagt de organisatie om terughoudendheid: grote bestanden kunnen nog niet worden ontvangen en het e-mailverkeer wordt beperkt verwerkt.

Dit incident onderstreept het belang van het in kaart brengen van kwetsbaarheden en het minimaliseren van risico’s. Niet alleen binnen de eigen IT-omgeving, maar ook in systemen van leveranciers of externe toegangspunten.

Bron: BNR en Security.nl

QHSE

Veiligheidsregio's onvoldoende voorbereid op landelijke stroomuitval

7 augustus 2025 - Volgens onderzoek van de Inspectie Justitie en Veiligheid zijn de Nederlandse veiligheidsregio's niet goed voorbereid op een grootschalige of langdurige landelijke stroomuitval. Hoewel veel regio's oefenen met stroomstoringen, gebeurt dat vooral op lokaal niveau en bij kortdurende uitval. In maar liefst 15 van de 25 regio's ontbreekt zelfs een concreet noodplan om als crisisorganisatie operationeel te blijven zonder stroom. De Inspectie noemt dit zorgwekkend en roept op tot het treffen van maatregelen.

Als concreet voorbeeld wordt verwezen naar de recente stroomuitval in Spanje en Portugal, waar mobiele netwerken uitvielen, ziekenhuizen overgingen op noodaggregaten, het Openbaar Vervoer (OV) stilviel en elektronische betalingen onmogelijk werden. Zulke scenario's zijn ook in Nederland reëel. De Inspectie pleit dan ook voor grootschalige, gezamenlijke oefeningen tussen de veiligheidsregio's.

Zorg voor integrale bedrijfscontinuïteit
Dit rapport benadrukt dat continuïteit niet alleen een technisch of operationeel vraagstuk is, maar ook strategisch bekeken moet worden. Het vereist een goed doordacht noodplan, inzicht in kwetsbaarheden binnen én buiten de organisatie, en samenwerking met externe partners. Bedrijfscontinuïteit vraagt om realistische scenario-oefeningen, duidelijke afspraken en een integrale aanpak waarbij risico's structureel worden meegenomen in de besluitvorming.

Bron: Inspectie Justitie en Veiligheid en NOS