cuccibu
Reduce Risk, Create Value

CUCCIBU'S
INSIGHT OF THE WEEK

Een terugblik op het nieuws van de afgelopen week:

- Misleidende duurzaamheidsclaims op koffie- en cacaoproducten
- Dataveiligheid in de zorg: Tweede Kamer wil technische briefing
- Handreiking weerbaarheid bereidt gemeenten voor op crisis
- NCSC waarschuwt voor malwarecampagne via onschuldig lijkende tools
- Demissionair kabinet voor invoering van Europese bewaarplicht

QHSE

Misleidende duurzaamheidsclaims op koffie- en cacaoproducten

14 augustus 2025 - Steeds meer bedrijven willen laten zien dat ze duurzame en ethisch verantwoorde producten verkopen. Maar volgens de Autoriteit Consument & Markt (ACM) gaat dat vaak mis. Uit recent onderzoek naar duurzaamheidsclaims in de levensmiddelensector blijkt dat vooral bij koffie- en cacaoproducten veel gebruik wordt gemaakt van vage of misleidende claims. Denk aan termen als “duurzaam” of “verantwoord geteeld”, zonder dat wordt uitgelegd wat dit inhoudt.

Waarom is dat een probleem?
Claims zijn vaak dubbelzinnig. “Verantwoord geteeld” kan slaan op de manier van verbouwen, maar ook op een hoger loon voor boeren. Ook werken veel koffie- en cacaoboeren in tropische gebieden, waardoor zij kampen met o.a. armoede, gebrek aan sociale bescherming, verlies van biodiversiteit, bodemuitputting en ontbossing. Daar wordt meestal niets over gezegd. Transparantie en eerlijkheid zijn cruciaal om duurzame keuzes mogelijk te maken.

Wat doet de ACM?
De toezichthouder intensifieert het toezicht op deze sector en is gestart met gerichte onderzoeken bij grote spelers.

- De levensmiddelen sector wordt opgeroepen om hun claims te controleren aan de hand van de door de ACM opgestelde richtlijnen.
- Bedrijven worden aangesproken bij misleidende duurzaamheidsclaims en geacht hun verpakkingen aan te passen.

Naast de levensmiddelensector deed de ACM al eerder onderzoek naar duurzaamheidsclaims in de sectoren voor energie, kleding en vervoer.

Conclusie
Duurzaamheidsclaims zijn waardevol, maar alleen als ze juist, eerlijk en goed onderbouwd zijn. Alleen zo kunnen consumenten een weloverwogen en écht duurzame keuze maken.

Bron: NOS

Data Security

Dataveiligheid in de zorg: Tweede Kamer wil technische briefing

22 augustus 2025 - De Tweede Kamer maakt zich zorgen over de veiligheid van persoonsgegevens in de zorg. Aanleiding is het grote datalek bij Clinical Diagnostics, waarbij gegevens van ruim een half miljoen Nederlanders zijn buitgemaakt. Het gaat om zeer gevoelige medische informatie die in handen kwam van cybercriminelen, die nu opnieuw dreigen de data openbaar te maken als er niet betaald wordt. Dit incident roept vragen op over hoe veilig persoonlijke gegevens bij andere laboratoria en zorginstellingen werkelijk zijn.

Reactie van de Tweede Kamer
Een brede Kamermeerderheid heeft daarom aangedrongen op een technische briefing door de ministeries van Volksgezondheid en Justitie en Veiligheid. Ambtenaren van deze ministeries en de vaste commissie voor Volksgezondheid gaven op 4 september een update over de laatste stand van zaken rond dataveiligheid in de zorg.

Aantoonbaar voldoen aan NEN 7510
Voor zorginstellingen is er al een duidelijke standaard: NEN 7510, de norm voor informatiebeveiliging in de zorg. Deze norm schrijft voor hoe organisaties zorgvuldig met medische gegevens moeten omgaan en passende technische en organisatorische maatregelen moeten nemen. Incidenten zoals bij Clinical Diagnostics laten zien dat aantoonbare naleving en handhaving van deze norm urgenter zijn dan ooit.

Waarom is dit urgent
Deze stap benadrukt de urgentie: gezondheidsdata behoren tot de meest gevoelige persoonsgegevens. Incidenten als dit datalek ondermijnen niet alleen het vertrouwen van burgers, maar leggen ook pijnlijke kwetsbaarheden bloot in de digitale weerbaarheid van de zorgsector. Meer transparantie en concrete maatregelen zijn onmisbaar om de sector structureel beter te beschermen.

Bron: Security.nl en Tweede Kamer

Data Security

Handreiking weerbaarheid bereidt gemeenten voor op crisis

24 augustus 2025 - Geopolitieke spanningen, klimaatverandering en de kwetsbaarheid van vitale voorzieningen vragen om versterking van de maatschappelijke weerbaarheid en veerkracht. Gemeenten spelen hierin een sleutelrol. Een crisis, van stroomuitval tot hybride dreiging, heeft namelijk in de eerste plaats lokaal impact.

Daarom presenteerde de Vereniging van Nederlandse Gemeenten (VNG) op 28 augustus 2025 de handreiking “Weerbaarheid en veerkracht op lokaal niveau”. Deze biedt gemeenten een praktisch kader om zich organisatiebreed beter voor te bereiden op langdurige crises en verstoringen.

41 maatregelen per crisisfase

De kern van de handreiking is een lijst met 41 concrete maatregelen, ingedeeld naar zes pijlers, zoals eigen continuïteit en crisisorganisatie. De maatregelen zijn uitgewerkt per fase van een crisis: de koude fase, de warme fase binnen 72 uur, de warme fase na 72 uur en de nafase. Daarbij staat steeds aangegeven wie verantwoordelijk is en welke partners – zoals veiligheidsregio’s, ministeries en, maatschappelijke organisaties, woningcorporaties of vrijwilligers – betrokken kunnen zijn.

Lokale vertaling en innovatieve tools

Gemeenten worden aangemoedigd de handreiking te vertalen naar hun eigen context, prioriteiten te stellen en gebruik te maken van innovatieve instrumenten zoals scenario-studies, impactanalyses en digital twins. Deze tools maken kwetsbaarheden inzichtelijk en versterken de gemeentelijke responsvaardigheid.

Koppeling met ISO 22301

De handreiking sluit nauw aan bij principes uit de internationale norm ISO 22301, gericht op Business Continuity Management (BCM). Deze norm helpt organisaties te anticiperen op verstoringen en processen in te richten voor herstel en continuïteit.

Bron: VNG

Data Security

NCSC waarschuwt voor malware campagne via onschuldig lijkende tools

29 augustus 2025 - Recentelijk is een wereldwijde malwarecampagne aan het licht gekomen, waarbij Windows-computers geïnfecteerd raakten via ogenschijnlijk onschuldige software. Het Nationaal Cyber Security Centrum (NCSC) waarschuwt dat programma's als "PDF-editor" en "ManualFinder" – vaak hoog in zoekresultaten of aangeboden via advertenties – na installatie kwaadaardig gedrag vertonen.

Gebruikers installeerden deze tools massaal om handleidingen te downloaden of PDF-bestanden te bewerken. Pas na verloop van tijd bleek dat de applicaties malware-activiteiten uitvoerden, wat leidde tot een golf aan alarmeringen bij SOC's en cybersecuritybedrijven wereldwijd.

Apparaten ingezet als residential proxies
Na installatie worden de systemen misbruikt als residential proxies. Daarmee maskeren criminelen hun eigen activiteiten door deze via de computers van slachtoffers te laten lopen. Zo lijkt het alsof het slachtoffer zelf de kwaadaardige acties uitvoert.

Het verkeer wordt via deze proxies omgeleid, bijvoorbeeld om een IP-adres in een specifiek land te gebruiken bij een aanval. Door middel van browserscripts en geplande taken behouden aanvallers blijvende toegang via command-and-control (C2)-servers.

Handelingsperspectief volgens NCSC
Het NSCS geef organisaties en gebruikers een aantal adviezen, waaronder:

- Blokkeer de toegang tot verdachte C2-domeinen.
- Controleer systemen op aanwezigheid van applicaties als "ManualFinder" en "PDF-editor", en op verdachte JavaScript-bestanden.
- Waarschuw eindgebruikers voor de risico's van het installeren van externe, onbetrouwbare tools.

Bron: Security.nl en NCSC

Data Privacy

Demissionair kabinet voor invoering van Europese bewaarplicht

1 september 2025 - Het demissionaire kabinet staat positief tegenover de plannen van de Europese Commissie om een Europese bewaarplicht in te voeren.

Elf jaar geleden verklaarde het Europese Hof van Justitie de toenmalige richtlijn dataretentie ongeldig, omdat telecomgegevens van burgers maanden- tot jarenlang mochten worden opgeslagen. Nu onderzoekt Brussel of een nieuwe, Europabrede bewaarplicht juridisch houdbaar kan worden ingevoerd.

Rol van de High-Level Group “Going Dark”
Het vernieuwde voorstel werd mede geadviseerd door de High-Level Group (HLG) "Going Dark": een samenwerkingsverband van nationale opsporingsdiensten dat pleit voor verbeterde toegang tot (versleutelde) data voor rechtshandhaving. De adviesgroep publiceerde vorig jaar een rapport waarin zij onder andere pleiten voor het invoeren van encryptie-backdoors en een nieuwe Europese bewaarplicht.

Fiche aan de Tweede Kamer
De Tweede Kamer ontving hierover een fiche met de titel “Routekaart rechtmatige en effectieve toegang tot data ten behoeve van de opsporing”. Het kabinet benadrukt dat geharmoniseerde regelgeving binnen de EU noodzakelijk is voor rechtsgelijkheid & kwaliteit en beschikbaarheid van data. Tegelijkertijd stelt het dat een nieuwe bewaarplicht zorgvuldig moet worden getoetst en volledig in lijn moet zijn met grondrechten en jurisprudentie van het Europees Hof van Justitie.

Kritiek vanuit burgerrechten
Burgerrechtenorganisaties zoals EDRi waarschuwen dat een hernieuwde bewaarplicht privacyfundamenten onder druk zet. Denk aan beperking van anonieme meningsuiting, persvrijheid en politiek activisme. Ze noemen de voorgestelde strategie een stap richting surveillance à la “digitale dystopie”.

Bron: Security.nl