cuccibu
Reduce Risk, Create Value

CUCCIBU'S
INSIGHT OF THE WEEK

Een terugblik op het nieuws van de afgelopen week:

- Naam NCSC misbruikt in phishingcampagne
- 23andMe boete van €2,7 miljoen voor datalek afstammingsgegevens
- Nederlandse implementatie NIS2 opnieuw uitgesteld
- Bouwbedrijf vervolgd wegens blootstelling werknemers aan asbest

Data Security

Naam NCSC misbruikt in phishingcampagne

13 juni 2025 - Op 13 juni 2025 waarschuwt het Nationaal Cyber Security Centrum (NCSC) dat kwaadwillenden zich via e-mail uitgeven voor hun directeur Matthijs van Amelsfort. Ontvangers krijgen zogenaamd een “dagvaarding” toegestuurd met als doel persoonlijke gegevens te stelen. Dit is een typisch voorbeeld van een phishingcampagne. Het NCSC benadrukt dat zij nooit rechtstreeks contact opnemen met burgers, en roept op om verdachte berichten direct te verwijderen en te melden bij de Fraudehelpdesk. De herkomst van deze e-mails wordt onderzocht.

Hoe herken je een phishingmail?
Je denkt misschien: "Ik trap daar niet in." Maar phishingmails worden steeds geavanceerder en realistischer. Let op de volgende signalen:

- Dringende toon of gezaghebbende afzender.
- Ongebruikelijke afzender of e-mailadres. Eén verkeerd teken of afwijkend domein is al verdacht.
- Algemene aanhef. Betrouwbare partijen (of waar je klant bent) gebruiken meestal je naam in plaats van termen als “Geachte heer/mevrouw” of “Beste klant”.
- Verdachte bijlagen of bestandsformaten. Open nooit bijlagen van onbekende afzenders – zeker geen .zip- of .rar-bestanden.
- Onlogische verzoeken om persoonsgegevens. Word je gevraagd om je gegevens ‘bij te werken’ via een link? Trap er niet in.
- Links die leiden naar onbekende of onbetrouwbare sites. Zet je cursor op de link zonder te klikken: komt het webadres je vreemd voor, klik dan niet. Let extra op verkorte links
- Taalgebruik en opmaak. Foutieve spelling, rommelige opmaak of vreemd taalgebruik zijn duidelijke rode vlaggen.

Blijf alert, meld verdachte berichten en deel je twijfels intern. Bewustzijn is het krachtigste wapen tegen cyberdreigingen. Eén klik kan genoeg zijn om schade aan te richten – voorkomen begint bij herkennen.

Bron: Nationaal Cyber Security Centrum, Digital trust center

Data Privacy

23andMe boete van €2,7 miljoen voor datalek afstammingsgegevens

17 juni 2025 - De Britse privacytoezichthouder ICO heeft dna-testdienst 23andMe een boete opgelegd van €2,7 miljoen wegens een grootschalig datalek in 2023. Bij dit incident werden de gevoelige gegevens van 6,9 miljoen gebruikers buitgemaakt. Het ging onder meer om genetische profielen, adressen, etnische afkomst en familieverbanden.

Beveiliging ernstig tekortgeschoten
De ICO stelde vast dat 23andMe op meerdere punten ernstig tekort was geschoten in de bescherming van deze persoonsgegevens:

- Er was geen verplichte multi-factorauthenticatie (MFA).
- De gebruikte wachtwoordprotocollen waren onvoldoende veilig.
- Gebruikersnamen waren voorspelbaar en daardoor kwetsbaar.
- Er ontbraken systemen om cyberdreigingen te monitoren, detecteren en blokkeren.
- Toegang tot ruwe genetische data was onvoldoende beperkt en slecht beveiligd.

De aanval vond plaats via een zogenaamde **credential stuffing-aanval**, waarbij eerder gestolen inloggegevens van andere websites werden gebruikt om toegang te krijgen tot accounts bij 23andMe. Pas toen een medewerker ontdekte dat de gestolen data online werd verhandeld, startte het bedrijf een onderzoek en werd het datalek formeel erkend.

Overname en rechten van betrokkenen
Na faillissement is 23andMe, inclusief de dna-databank van miljoenen gebruikers, overgenomen door het TTAM Research Institute. Volgens de AVG hebben betrokkenen bepaalde rechten als organisaties hun persoonsgegevens verwerken. Zo hebben zij o.a. recht op informatie, inzage, rectificatie en gegevens verwijdering. Alle gebruikers van 23andME zullen 2 dagen voor de definitieve afronding van de verkoop informatie ontvangen over hoe zij zich kunnen afmelden voor onderzoeksdoeleinden en hun data definitief kunnen laten verwijderen.

Bron: Security.nl, autoriteit persoonsgegevens

Data Security

Nederlandse implementatie NIS2 opnieuw uitgesteld

17 juni 2025 - De invoering van de Europese NIS2-richtlijn in Nederland is opnieuw vertraagd. De Nederlandse Cyberbeveiligingswet, die de richtlijn moet omzetten in nationale wetgeving, zal naar verwachting pas in het tweede kwartaal van 2026 in werking treden — bijna twee jaar later dan de oorspronkelijke deadline van oktober 2024.

Oorzaken van vertraging
Het omzetten van NIS2 naar Nederlandse wetgeving blijkt een complex en omvangrijk proces. Daarnaast spelen ook politieke factoren een rol: het demissionaire kabinet en een traag wetgevingsproces zorgen mogelijk voor verdere vertraging.

Wacht niet af
Is dat goed nieuws voor organisaties die nog niet klaar zijn? Niet echt. Cyberdreigingen houden zich niet aan wetten of deadlines. Hoewel het uitstel tijdelijk lucht geeft, is het geen excuus om achterover te leunen.

De realiteit is dat cyberaanvallen in frequentie en impact toenemen. Daarom roept het NCSC op om niet te wachten met actie. Veel verplichtingen uit de NIS2 zijn nu al te vertalen naar concrete stappen: voer een risicoanalyse uit, implementeer passende beheersmaatregelen, stel een incident-response plan op en train bestuurders in digitale weerbaarheid.

Wie nu begint, is straks niet alleen compliant, maar vooral weerbaarder tegen de risico’s die vandaag al realiteit zijn. Kortom: wacht niet op wetgeving om in beweging te komen. Begin nu.

Bron: Nationaal Cyber Security Centrum, Binnenlands Bestuur

QHSE

Bouwbedrijf vervolgd wegens blootstelling werknemers aan asbest

17 juni 2025 - Het Openbaar Ministerie vervolgt het Twentse bouwbedrijf Eternit op verdenking van doodslag of dood door schuld. Werknemers die tussen 1937 en 1993 met asbest in aanraking kwamen, zouden jarenlang zijn blootgesteld aan gevaarlijke vezels. Volgens het OM leidde dit tot de dood van ten minste twee oud-medewerkers en een partner van hen.

Eternit produceerde sinds 1937 bouwmaterialen waarin fijne asbestvezels werden verwerkt. Pas in 1993 werd het gebruik van asbest in Nederland verboden. Volgens het OM heeft het bedrijf ondanks toenemende kennis over de risico's gehandeld in strijd met haar zorgplicht en werknemers opzettelijk blootgesteld aan de ernstige gezondheidsrisico's die blootstelling met zich meebrengt.

Dringend signaal voor arbobeleid
Het OM benadrukt dat bedrijven die werken met gevaarlijke stoffen, zoals asbest, een zware verantwoordelijkheid dragen. De Arbowet verplicht hen om de gezondheid van werknemers actief te beschermen en risico's te minimaliseren. Dit betekent onder andere:

- Een verplichte risico-inventarisatie & -evaluatie (RI&E) uitvoeren;
- Adequate beheersmaatregelen treffen, zoals persoonsbeschermingsmiddelen (PBM), goede ventilatie en veilige werkprocedures;
- Grondige documentatie van inspecties, incidenten en maatregelen.

De strafzaak tegen Eternit laat zien dat nalatigheid, ook uit het verleden, zwaar kan worden bestraft. Het is een harde herinnering dat arbo- en veiligheidsbeleid geen formaliteiten zijn, maar cruciaal voor de bescherming van je mensen én de organisatie.

Bron: NOS, Openbaar Ministerie