EÉN SCENARIO, VELE LESSEN

DE HACK BIJ HET BEVOLKINGSONDERZOEK/ODIDO UITGEDIEPT VANUIT HET PERSPECTIEF VAN DE TOEZICHTHOUDER

5 MAART 2026

WIE BEN IK?

Melanie van den Berg

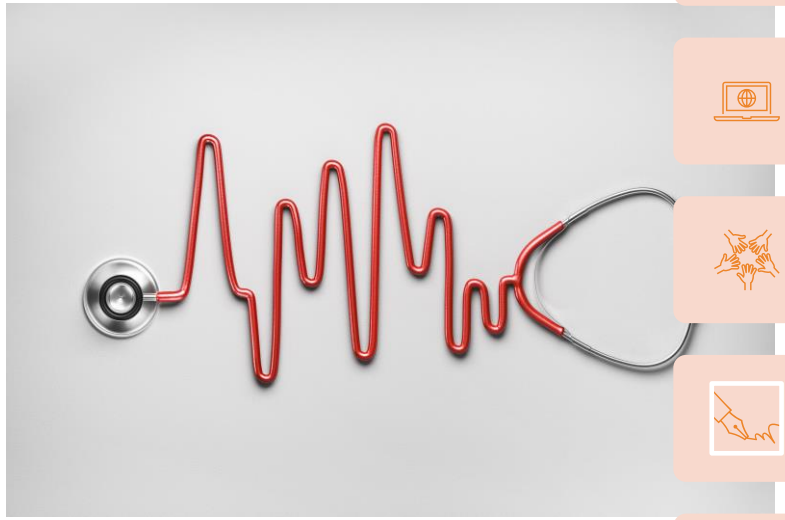
BergLegal & Trust

1. Expert op het gebied van risicomanagement, compliance en kwaliteit (van zorg & onderwijs)
2. Interim manager/directeur
3. Executive vertrouwenspersoon & coach
4. Toezichthouder in en buiten de zorg
5. Trainer

Linkedin

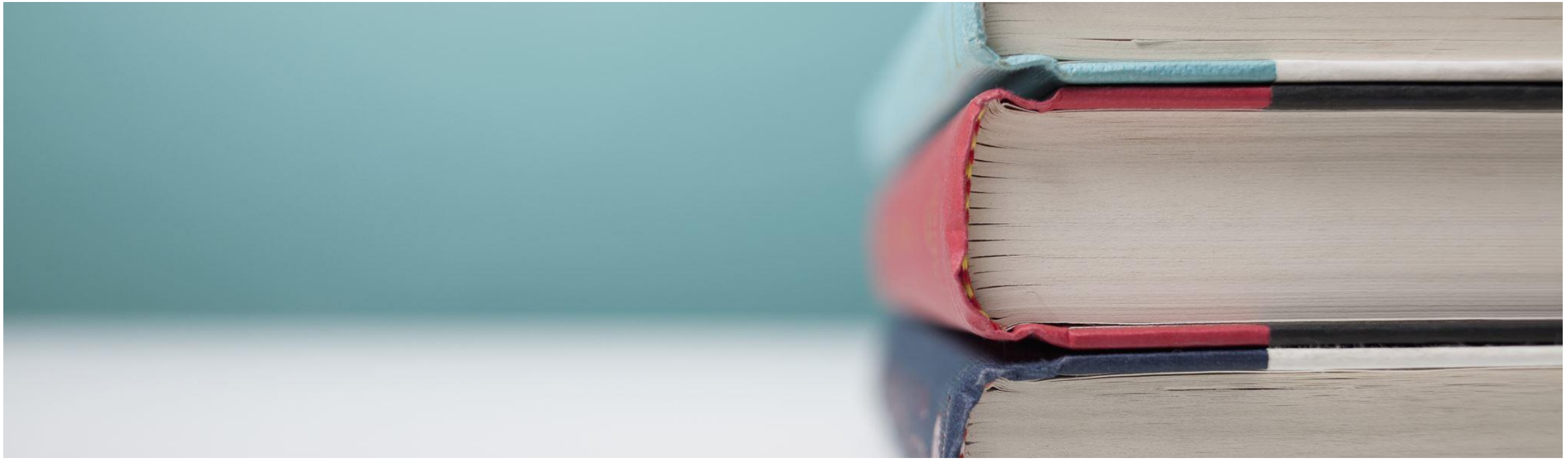
WAT WAS JE EERSTE REACTIE - ALS TOEZICHTHOUDER - TOEN DEZE HACK BIJ HET BEVOLKINGSONDERZOEK BEKEND WERD?

ONDERDELEN WORKSHOP



- Korte theorie
- Hacked
- Aan de slag
- Checklist
- Welke lessen neem je mee?

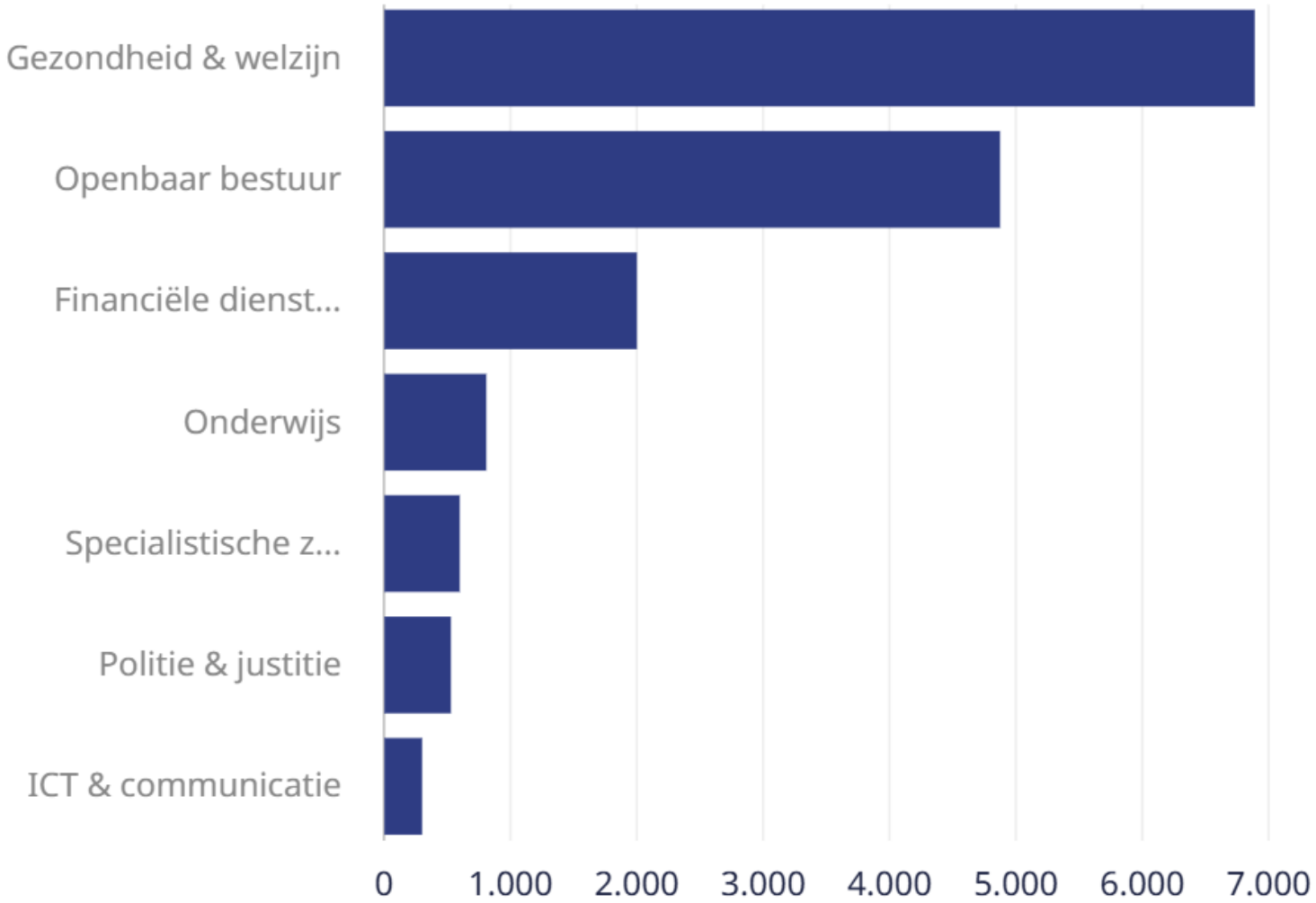
KORTE THEORIE



WEET JE WAAR DE DATA STAAT VAN DE ORGANISATIE WAAROP JE TOEZICHT HOUDT?

Gezondheidssector vaakst doelwit van datalekken

Totaal aantal meldingen van datalekken bij de Autoriteit Persoonsgegevens (AP) in 2024, uitgesplitst naar sector



NIS2 EN CBW IN EEN NOTENDOP

- Vanaf 17 oktober 2024 geldt NIS2 (Network and Information Systems Security Directive) in Nederland.
- In Nederland geïmplementeerd in de vorm van de Cyberbeveiligingwet (Cbw) – verwachting inwerking Q2 2026
- Zorg- en welzijnsinstellingen kunnen worden aangemerkt als 'essentiële' of 'belangrijke' entiteiten.
- De meeste middelgrote en grote zorginstellingen vallen hieronder.
- NIS2 Zelfevaluatie NL via https://regelhulpenvoorbedrijven.nl/NIS-2-NL/
- Essentiële en belangrijke entiteiten moeten maatregelen nemen om hun netwerk- en informatiesystemen tegen incidenten te beschermen. Hetzelfde geldt voor de fysieke omgeving waarin de systemen zich bevinden.
- De Cbw schrijft drie verplichtingen voor: zorgplicht, registratieplicht en meldplicht.
- Dit betekent o.a.:
  - Invoeren van technische en organisatorische risicobeheermaatregelen
  - Melding van ernstige incidenten binnen 24 uur
  - Aansprakelijkheid van bestuurders bij grove nalatigheid
  - Aantoonbare betrokkenheid van de raad van toezicht bij cyberrisicobeheer!

AANTOONBARE BETROKKENHEID RVT

Praktische minimumnorm voor RvT

Een RvT is aantoonbaar betrokken als:

📌 Cybersecurity gekoppeld is aan kwaliteit & veiligheid
📌 Jaarlijks informatiebeveiligingsbeleid en risicoanalyse formeel zijn besproken
📌 Incidenten geëvalueerd worden
📌 Scholing is gevolgd
📌 Alles schriftelijk is vastgelegd (notulen)

→Self-assessment RvT Cbw.

Welke maatregelen moet ik nemen om aan de zorgplicht te voldoen?

Onder de zorgplicht vallen ten minste:

1. Een risicoanalyse en beveiliging van informatiesystemen
2. (Beleid en procedures over) incidentenbehandeling
3. Maatregelen op het gebied van bedrijfscontinuïteit, zoals back-upbeheer en noodvoorzieningenplannen
4. Beveiliging van de toeleverancierssketen
5. Beveiliging bij het verwerken, ontwikkelen en onderhouden van netwerk- en informatiesystemen, inclusief de respons op en bekendmaking van kwetsbaarheden
6. Beleid en procedures om de effectiviteit van beheers-maatregelen van cyberbeveiligingsrisico's te beoordelen
7. Basis cyberhygiëne en trainingen op het gebied van cyberbeveiliging
8. Beleid en procedures over het gebruik van cryptografie en encryptie
9. Beveiligingsaspecten op het gebied van personeel, toegangsbeleid en beheer van activa
10. Het gebruik van multifactorauthenticatie, beveiligde spraak-, video- en tekstcommunicatie en beveiligde nood-communicatiesystemen binnen de entiteit

Zijn alle maatregelen van toepassing op mijn organisatie?

De NIS2-richtlijn schrijft voor dat de maatregelen passend en evenredig moeten zijn. Bij de beoordeling van de evenredigheid kunt u kijken naar de mate waarin uw organisatie is blootgesteld aan risico's, de omvang van de organisatie, de kans dat zich incidenten voordoen en de mogelijke impact op de maatschappij en economie.

Wie is verantwoordelijk voor het naleven van de zorgplicht?

Het bestuur van de NIS2-entiteit is eindverantwoordelijk voor het naleven van de zorgplicht. Zij kunnen voor het niet naleven aansprakelijk worden gesteld. Er ligt een actieve rol voor hen weggelegd in het goedkeuren van de voorgenomen maatregelen, het houden van toezicht op de implementatie, het volgen van training om kennis te vergroten en het aanbieden van trainingen aan medewerkers.

Houd voor meer informatie www.ncsc.nl in de gaten.

Nationaal Cyber Security Centrum

CYBER RESILIENCE ACT

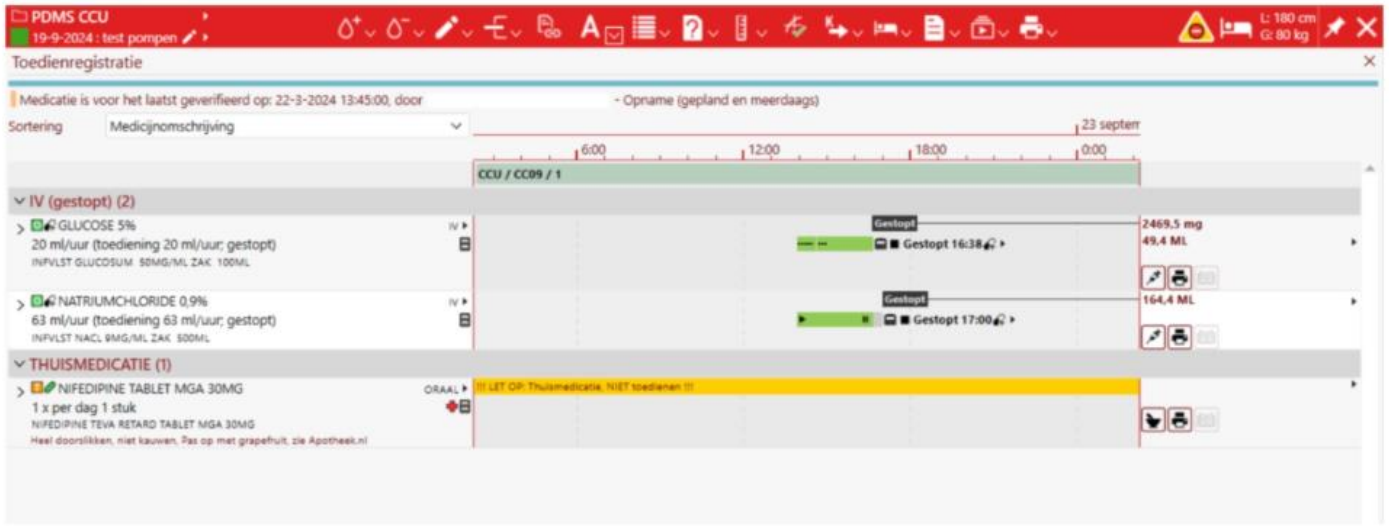
De Cyber Resilience Act (CRA) is een Europese verordening (EU) die eind 2023 is vastgesteld en de komende jaren gefaseerd in werking treedt. Het doel is om de cyberveiligheid van digitale producten en de software die daarin draait structureel te verbeteren binnen de hele EU.

Kernpunten van de Cyber Resilience Act

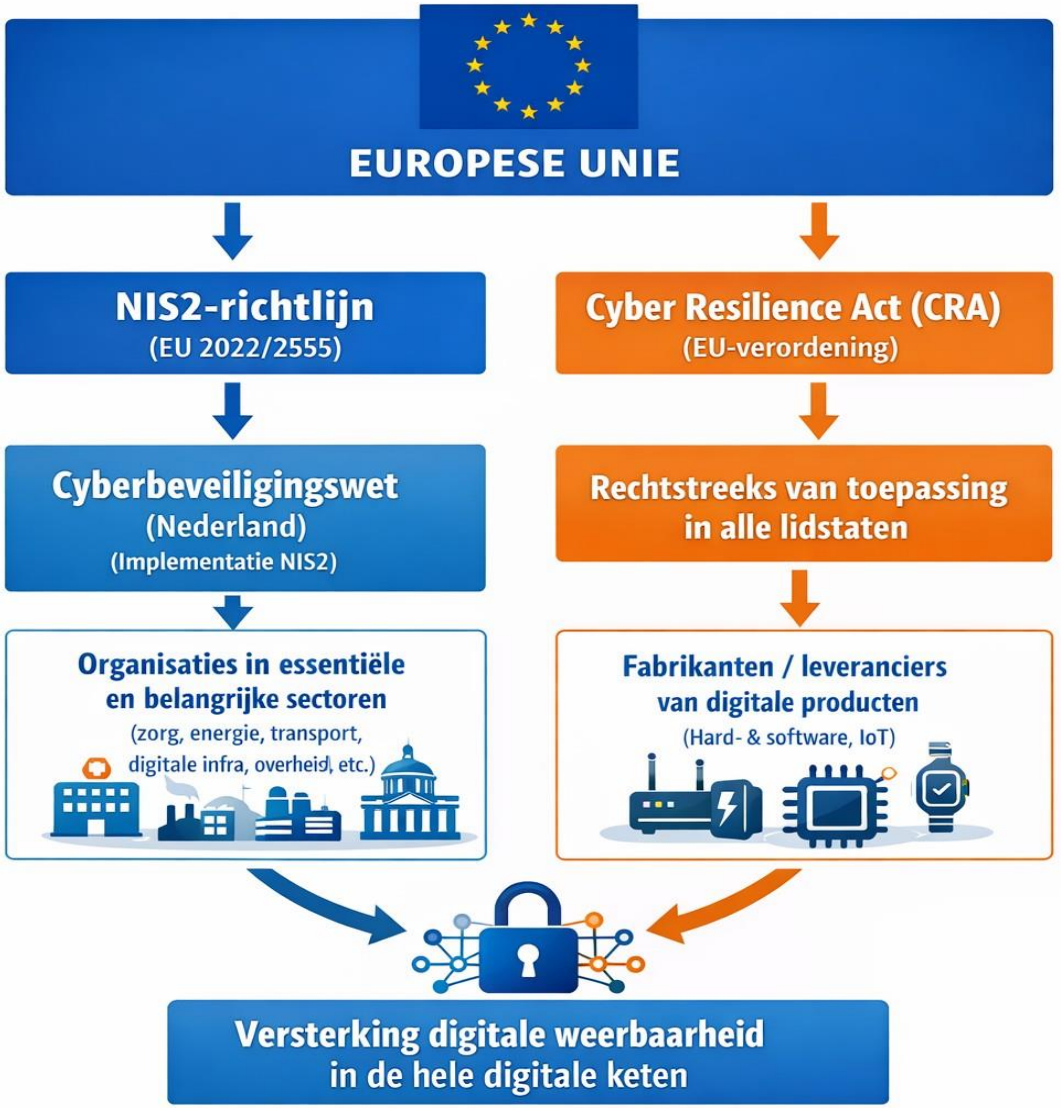
Toepassingsgebied: alle producten met digitale elementen (hardware en software) die op de EU-markt worden gebracht. Denk aan medische apparatuur met software, apps, industriële systemen, netwerkapparatuur, etc.

- Verplichtingen voor fabrikanten en leveranciers:
  - Beveiliging moet standaard ingebouwd zijn (“security by design”).
  - Producten moeten veilig zijn gedurende de gehele levenscyclus (dus ook updates en patches na verkoop).
  - Fabrikanten moeten bekende kwetsbaarheden melden en updates uitrollen binnen een redelijke termijn.
  - Transparantie naar gebruikers over beveiligingsondersteuning (bijv. hoe lang een apparaat beveiligingsupdates krijgt).
  - Risicogebaseerde aanpak: producten worden ingedeeld in risicocategorieën. Hoe kritieker het product voor veiligheid of infrastructuur, hoe strenger de eisen.

Rijnmondse primeur voor Maasstad Ziekenhuis met gebruik ‘slimme’ infuuspompen



OKTOBER 3, 2024


EUROPESE UNIE
NIS2-richtlijn
(EU 2022/2555)
Cyber Resilience Act (CRA)
(EU-verordening)
Cyberbeveiligingswet
(Nederland)
(Implementatie NIS2)
Rechtstreeks van toepassing
in alle lidstaten
Organisaties in essentiële
en belangrijke sectoren
(zorg, energie, transport,
digitale infra, overheid, etc.)
Fabrikanten / leveranciers
van digitale producten
(Hard- & software, IoT)
Versterking digitale weerbaarheid
in de hele digitale keten

Maastricht University

HACKED

https://www.hoppenbrouwerstechniek.nl/boek-hack/

hoppenbrouwers

Particulier Zakelijk Werken bij

Download 'Hack'

De impact van cybercrime

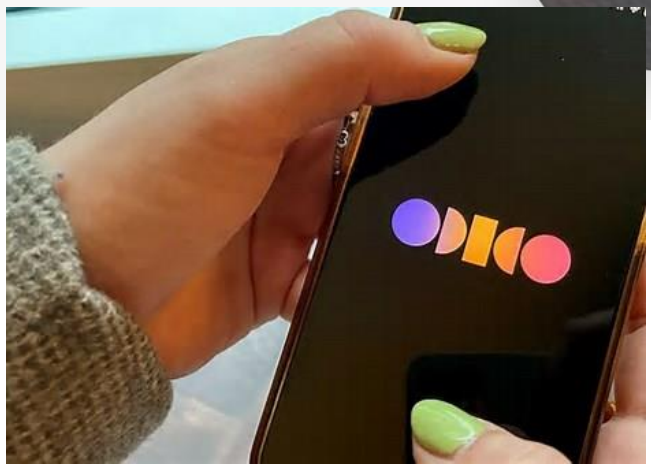
De kans dat bedrijven te maken krijgen met een brand is 1 op de 8.000, de kans op een inbraak is 1 op de 250 en de kans op een cyberaanval bij bedrijven is 1 op de 5. Uit een recent onderzoek van ABN AMRO onder 233 bedrijven blijkt zelfs dat bijna de helft afgelopen jaar te maken had met cybercriminaliteit.

Download het boek › Luister de podcast ›

REDACTIE - 02 MAART 2026 Deel dit artikel

Hack bij AkzoNobel: Paspoorten en NDA's gelekt op darknet

De beursgenoteerde verfgigant AkzoNobel is getroffen door een ingrijpende cyberaanval. De beruchte ransomware-groepering Anubis claimt de verantwoordelijkheid voor de hack en heeft inmiddels een grote hoeveelheid buitgemaakte data op het darknet gepubliceerd.



Dit is waarom hackers Nederlandse medische data stelen | RTL Nieuws

YouTube | RTL Nieuws | 6,2K weergaven | 1 maand geleden

AAN DE SLAG


bevolkingsonderzoek
nederland
Voor vroege opsporing van kanker
Retouradres: Postbus 91163, 3007

AANTAL FEITEN HACK LABORATORIUM

- Criminele hackers zijn begin juli 2025 binnengedrongen in de systemen van het laboratorium Clinical Diagnostics NMDL in het Zuid-Hollandse Rijswijk. Dat is een van de instanties die de monsters (in dit geval baarmoederhalskanker) beoordelen voor het Bevolkingsonderzoek Nederland.
- In eerste instantie leken de persoonsgegevens van 485.000 deelnemers te zijn gestolen.
- Naast persoonlijke informatie zoals namen, adressen en BSN zijn van een deel van de deelnemers ook de testuitslagen van uitstrijkjes en zelftests gestolen.
- Bevolkingsonderzoek Nederland heeft melding gedaan (van het datalek) bij de Inspectie Gezondheidszorg en Jeugd (IGJ), de Autoriteit Persoonsgegevens (AP) en bij het Nationaal Cyber Security Centrum (NCSC).
- De IGJ en het Openbaar Ministerie hebben bekend gemaakt dat zij een onderzoek starten bij Clinical Diagnostics NMDL.
- Onduidelijk of losgeld betaald is.
- Collectieve schadeclaim opgestart.
- Schatting is dat claimschade hack kan oplopen tot 2,3 miljard euro.

WORKSHOP

- Doel: Lessen leren van het incident en oefenen met toezicht houden onder onzekerheid

- Break-out sessie (7 groepen van 4 personen)

Beantwoording van de vragen:

- Wat zou jullie eerste reactie zijn als Raad van Toezicht?
- Welke risico's prioriteren jullie?
- Welke lessen trekken jullie voor het toezicht?

TWIST: GROTERE OMVANG VAN DE HACK

In eerste instantie leken de persoonsgegevens van 485.000 deelnemers te zijn gestolen. Dit is echter opgelopen tot **941.000 deelnemers**. Ook interne notities blijken door de hack buitgemaakt.

Vragen voor de discussie:

- Verandert dit jullie prioriteiten als toezichthouder? En hoe?
- Welke extra acties moet de organisatie en/of de Raad van Toezicht ondernemen?

PLENAIRE TERUGKOPPELING

- Elke groep deelt de initiële beslissingen
- Hoe de twist de besluitvorming (mogelijk) heeft beïnvloed
- Een belangrijke les voor toekomstige incidenten

CHECKLIST RAAD VAN TOEZICHT (PREVENTIE & RESPONS)

PREVENTIE

5 kernvragen voor de toezichthouder

Wat zijn onze top-3 cyberrisico's?

Wanneer hebben wij voor het laatst een cyberoefening gedaan?

Zijn wij aantoonbaar NIS2/Cbw-compliant?

Hoe afhankelijk zijn wij van kritieke ICT-leveranciers?

Wat gebeurt er als onze systemen 5 dagen uitvallen?

RESPONS (1)

Fase 1: Direct na de aanval – Informatie en eerste duiding

• Is de Raad van Toezicht onmiddellijk geïnformeerd over de aanval?

• Zijn de aard, omvang en impact van de aanval helder toegelicht?

• Is duidelijk of de aanval effect heeft op:

  • Continuïteit

  • Patiënt/cliëntveiligheid

Fase 2: Crisisaanpak en risicobeheersing

• Is het crisismanagementteam geactiveerd?

• Wordt er samengewerkt met externe specialisten (bijv. Z-CERT, forensisch IT)?

• Zijn meldingen gedaan aan relevante instanties:

Autoriteit Persoonsgegevens, IGJ, NCSC (Nationaal Cyber Security Centrum) of politie (indien relevant)

• Is er zicht op de werking van:

  • Het incident response-plan

  • Beveiligingsmaatregelen (segmentatie, back-ups, toegangsbeheer)

  • Herstelstrategie (recovery)

RESPONS (2)

Fase 3: Communicatie en reputatie

- Is er een communicatieplan geactiveerd?
- Worden patiënten/cliënten, medewerkers, vrijwilligers en pers adequaat geïnformeerd?
- Wordt reputatieschade proactief beheerst?
- Is de communicatie afgestemd op wet- en regelgeving (zoals AVG)?

Fase 4: Evaluatie en structurele verbetering

- Is er een evaluatieverslag van de aanval opgesteld?
- Zijn oorzaken, gebreken in beleid of techniek benoemd?
- Is er een verbeterplan voor:
  - IT-infrastructuur en software
  - Training van personeel/vrijwilligers (cyberbewustzijn)
  - Testen van back-ups en responscapaciteit
- Wordt het informatieveiligheidsbeleid aangepast waar nodig?

RESPONS (3)

Fase 5: Governance, toezicht en verantwoording

- Heeft de RvT gesproken over de strategische lessen uit de aanval?
- Is de cybergang van zaken vastgelegd in het jaarverslag?
- Is cyberbeveiliging structureel onderdeel van de RvT-agenda?
- Wordt de rol van de CIO/CISO voldoende ondersteund en gecontroleerd?
- Zijn er periodieke interne of externe audit op cybersecurity?

WELKE LESSEN NEEM JE MEE?

INTERESSE IN EEN VERDIEPING?

ONAFHANKELIJK INZICHT IN (CYBER)RISICO'S, COMPLIANCE EN BEHEERSING – AANTOONBAAR EN MET VERTROUWEN BESTUREN & TOEZICHT HOUDEN

Melanie van den Berg

Melanievdnberg@hotmail.com

06 11 22 3992