Webinar 2: cybersecurity en digitale weerbaarheid

19 juni

Praktische afspraken

1. We beginnen om 8 uur
2. Zet uw microfoon uit
3. De presentatie wordt opgenomen en u ontvangt deze, inclusief slides, na afloop
4. Vragen en reacties kunt u kwijt in de chat
5. Als we tijdens het webinar niet aan alle vragen toekomen, ontvangt u de antwoorden na afloop per e-mail

vgn vereniging gehandicaptenzorg nederland

Van overzicht naar uitvoering

Doel: kennis en betrokkenheid vergroten rond gegevensuitwisseling, databeschikbaarheid, privacy en cyberbeveiliging (en de bestuurlijke sturing daarop).

Wat (inhoud)

Hoe (implementatie)

Webinar 1
Scope & hoofdthema's
• Gezamenlijke taal/bestuurlijke agenda
• EHDS, Wegiz, NIS2

Webinar 2
Cybersecurity & digitale weerbaarheid
• Risico's/rol bestuur/crisisrespons
• Z-CERT/IVGZ + gedrag/normering

Webinar 3
Gegevensuitwisseling & stelsel
• GIS/LDN/LVS (bestuurlijk)
• Medicatieoverdracht, eOverdracht, PGO + EHDS/Wegiz

Webinar 4
Data & (gen)AI
• Data voor sturing
• (gen)AI: kansen/risico's + accountability

Webinar 5
Verandermanagement & digitale cultuur
• Veranderkracht/innovatie
• Prioriteiten + vervolgacties

vgn vereniging gehandicaptenzorg nederland

Welkom

1. Inleiding Suzanne Leijendekkers
2. Onno Theuvenet – Z-CERT
3. Bettine Pluut – Informatieveilig gedrag in de zorg (IVGZ)
4. Afsluitende vraag en afronding

vgn vereniging gehandicaptenzorg nederland

1

Z-CERT
wettelijke taak
en dreigingen zorg

Onno Theuvenet

19 juni 2026 – Webinar VGN

TLP: AMBER

Stichting Z-CERT

Over ons

Hét CERT voor de zorg

Wettelijke taak NIS2
(nationaal: Cyberbeveiligingswet (Cbw)

Oprichting

1 juni 2017

Private stichting

Geen winstoogmerk
Niet marktverstorend

Financiering

Deelnemersvergoedingen
Bekostiging vanuit VWS

380+ Deelnemers

Groei naar 1500+ deelnemers

De Nederlandse zorg digitaal veilig

Diensten	Deelnemers	Entiteiten
Waarschuwingsdienst	✓	✓
Bewakingsdienst (buitenkant IT-infra)	✓	✓
Zorg Detectie Netwerk (digitale voetsporen)	✓	✗
Coördinatie bij incidenten – 24/7 bereikbaar	✓	✓
Coördinatie meldingen ethisch hackers (CVD)	✓	✗
Kennisdeling en communities (chatplatform)	✓	✗
Dreigingsinformatie	✓	✗
Opleiden Trainen Oefenen en testen	✓	✗

Kennisdeling en communities – benut elkaars kennis!

Samenbrengen van mensen en kennis voor de zorg.

We hebben een uitgebreid netwerk in de zorg en hebben zelf ook veel kennis in huis.

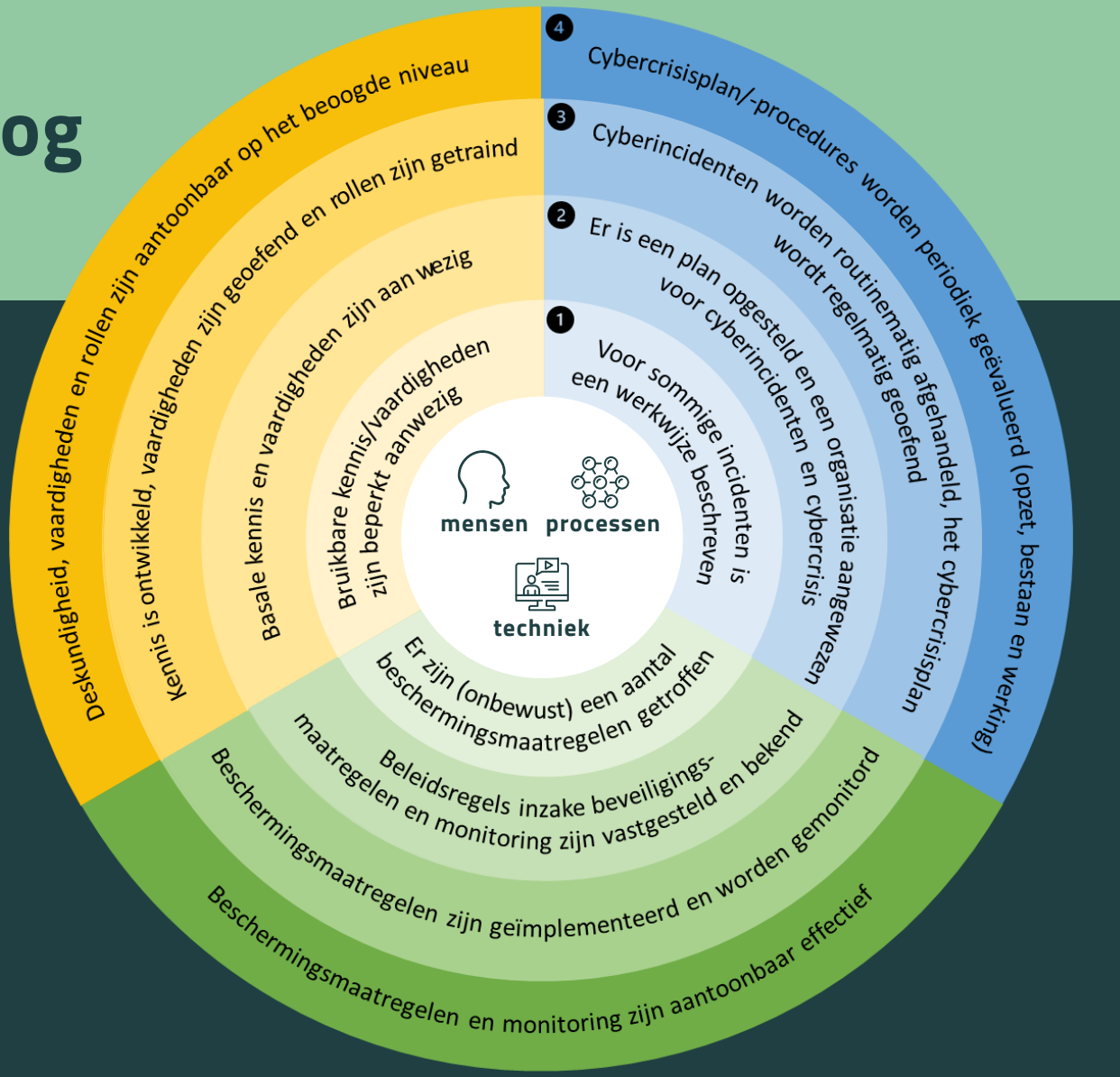
Dat zetten we in om mensen bij elkaar te brengen en een uitgebreid kennisplatform op te bouwen.

Community en relatiebeheer | **Kennisplatform** | **Samenwerken** | **End of Month**

Diensten

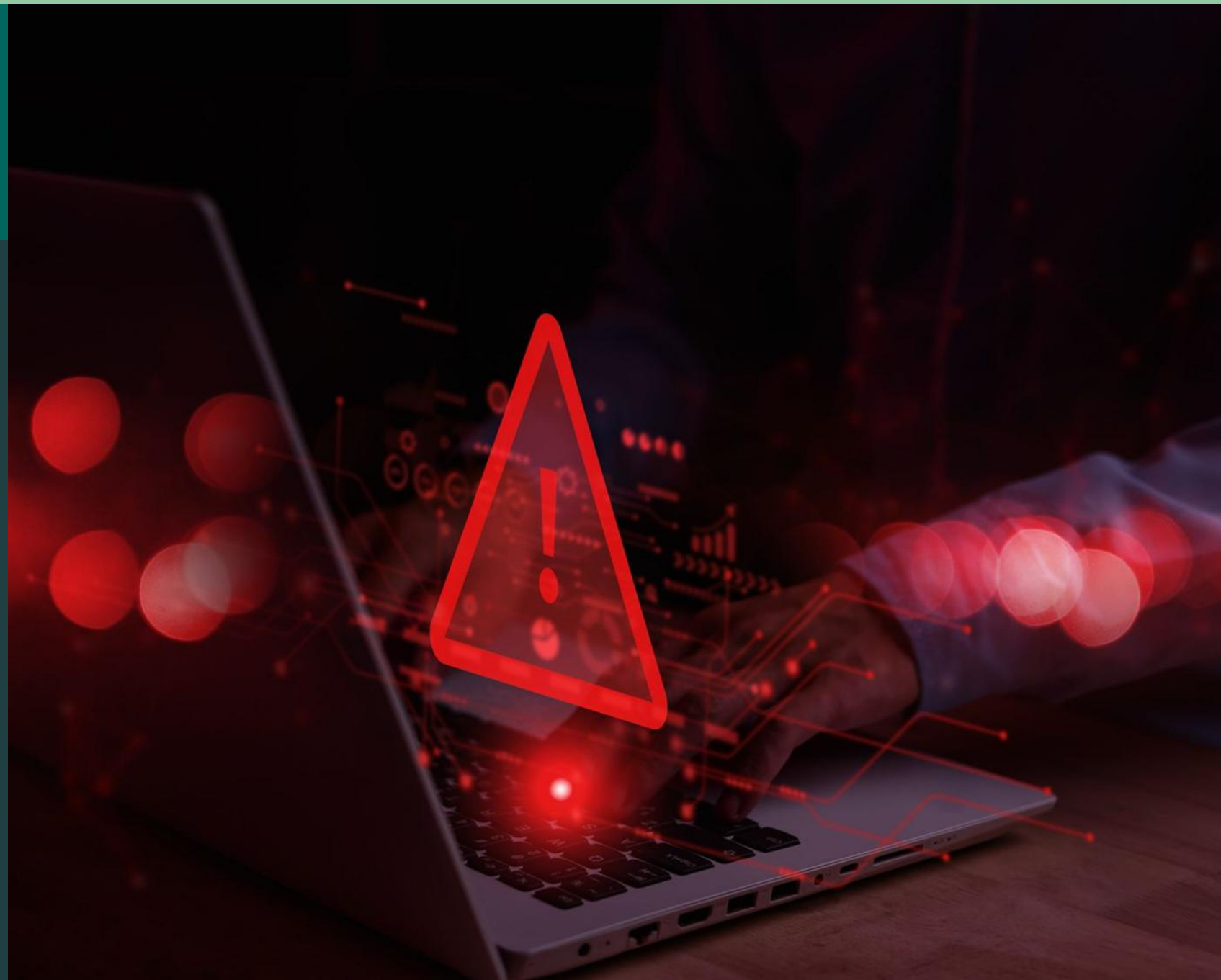
Oefenen, oefenen en nog eens oefenen!

Naast het op orde hebben van cybersecurity is het noodzaak om voor te bereiden op situaties waarin security niet volstaat. In die gevallen is cyberweerbaarheid geboden en dat kun je ontwikkelen met opleiden, trainen en oefenen.



2

Dreigingen



Diensten

Dreigingsinformatie

Het jaarlijks dreigingsbeeld is hèt visitekaartje van Z-CERT.

Op basis van dreigingen en incidenten die in het vorige jaar speelden maken we een dreigingsanalyse met handelingsperspectieven voor het komende jaar.

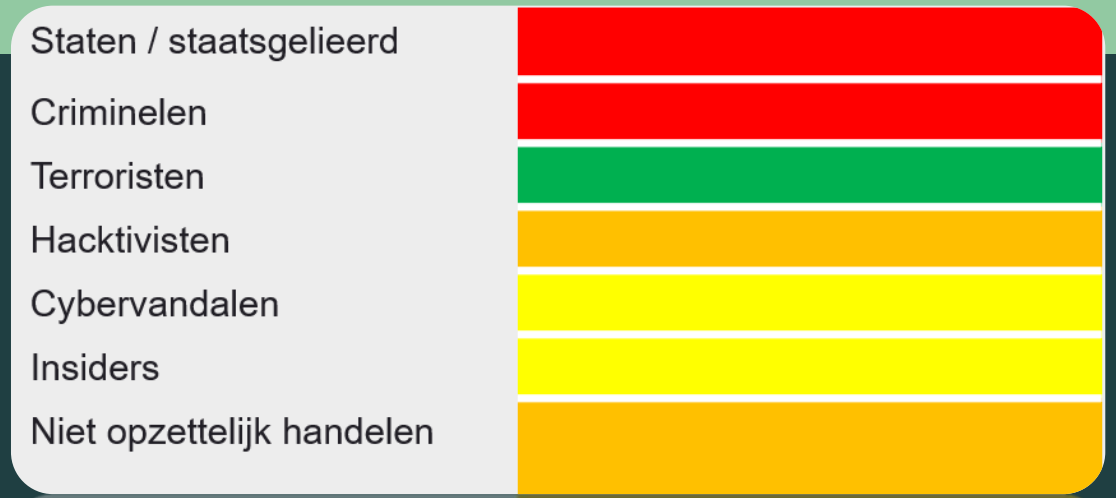
Jaarlijks

Kwartaal

Doorlopend

Dreigingsniveau Q1 2026

Bron van dreiging



Ransomware

- Chipsoft

Afpersing

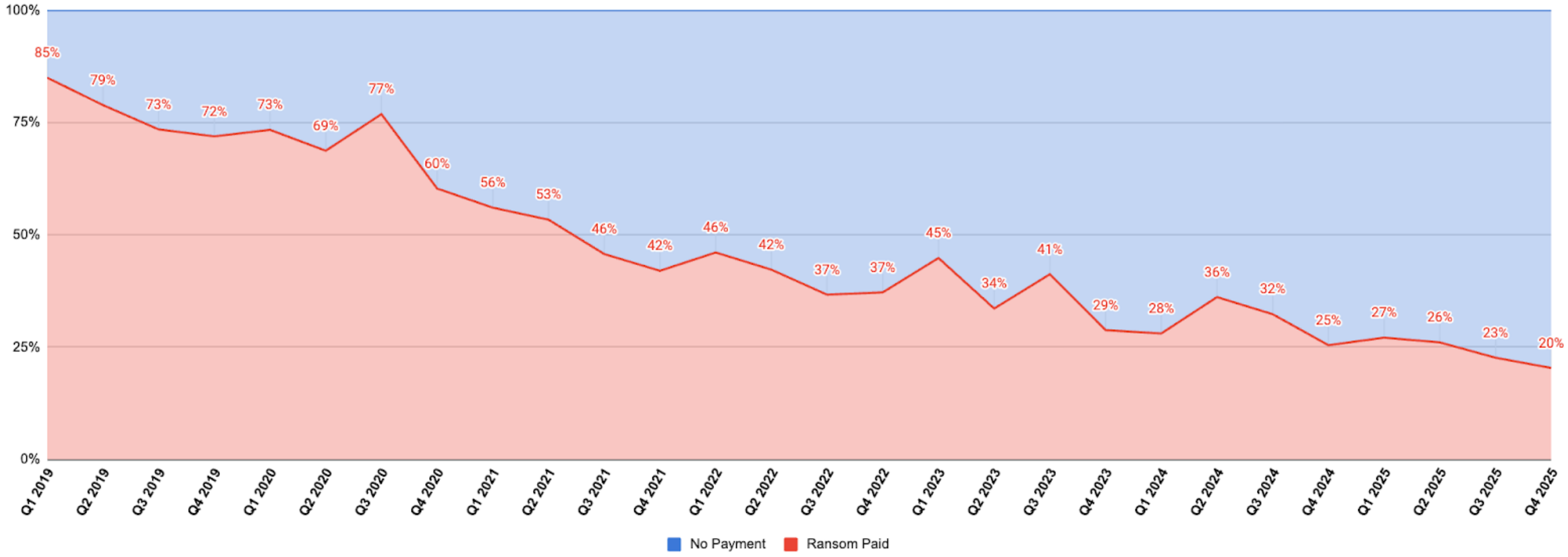
- Odido
- Incidenten via de software supply chain

Hacktivisme

- Medtech bedrijf Stryker geraakt door ontwrichtende, geopolitiek gemotiveerde aanval

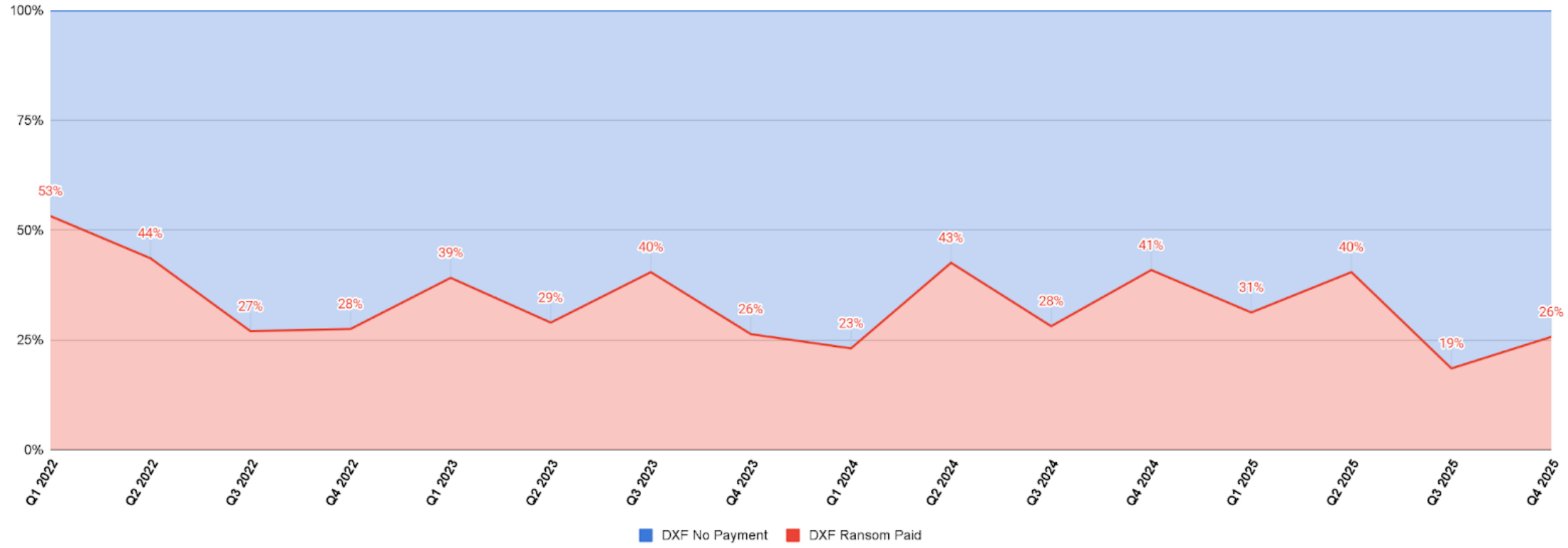
Datum	Land	Vendor / platform	Sector	Incident
2022	Nederland	Colosseum Dental Benelux	Tandartspraktijken	Ransomware met afpersing; tandartspraktijken raakten ontregeld.
2023-01	VS	NextGen Healthcare	Huisartspraktijken	BlackCat/ALPHV ransomware-/afpersingsclaim tegen een EPD-vendor.
2024	Roemenië	Hipocrate Information System	Ziekenhuizen	Ransomware trof het gedeelde ziekenhuisinformatiesysteem.
2025	VS	VirMedice	Huisartspraktijken	Pear-ransomware/afpersing met dreiging tot datalek.
2025	VS	drcloudemr.com	Huisartsenpraktijken / GGZ	SafePay-ransomware/afpersing met dreiging tot datalek.
2025	VS	PsychPlus	GGZ	Ransomware-/afpersingsclaim met dreiging tot datalek.
2025	Brazilië	MedicSolution	Ziekenhuis	Ransomware met afpersing en melding van gestolen zorgdata en medische beelden.
2026	Rusland	iGlobal Services, Medenet	Huisartspraktijken	Akira-ransomware met dreiging tot publicatie van gestolen data.
2026	Zwitserland	zHealthEHR	Chiropractie / wellnessklinieken	Kazu-ransomware met dreiging tot datalek.
2026	VS	CareCloud	Huisartspraktijken	Incident met patiëntgegevens die zijn gestolen.
2026	Nederland	ChipSoft	Huisartspraktijken, GGZ, ziekenhuizen	Ransomware/afpersing op EPD-vendor; later bevestigde diefstal van patiëntgegevens.

Trend: afname betalen voor Ransomware



De Nederlandse zorg digitaal veilig

Trend: redelijk stabiel – betalen n.a.v. dreigement lekken data



Datalek-afpersing Europa in de zorg - Q1 2026

Subsector	Aantal	Toelichting
Ziekenhuis / ziekenhuisgroep	**3**	Medical Park (**TR**), AZ Monica (**BE**), Pools ziekenhuis (**PL**)
Kliniek	2	Louise Medical Center (**BE**), Orthodontist.co.uk (**UK**)
Diagnostisch centrum	3	Oncologica (**UK**), Das Labor (**AT**), HT Médica (**ES**)
Gehandicaptenzorg	2	Franz Sales Haus (**DE**), Wohnverbund St. Gertrud (**DE**)
Geïntegreerde zorggroep	1	ISoSL (**BE**)
Totaal	**11**	

Nemen leveranciers dreigingsbeeld mee in risicoanalyse?

- Trends uit (jaarlijks) dreigingsbeeld:
  - Ransomware in de cloud → waar zitten de gaten in de beveiliging (gap-analyse)? Kan bestuurder dat aansturen?
  - Basis hygiëne – is hier op gelet?
    - Phishing resistent MFA / alleen toegestane (managed) devices
    - Applicatie allowlisting --> niet commercieel advies (voorkomt opstarten malware)
    - Time to patch → integreert leverancier “dreigingsinformatie” in prioritering kwetsbaarheden?
  - Voice phishing (actor: ShinyHunters)

Voorbeeld: ShinyHunters

https://www.checkpoint.com/security-report/?flz-category=items&flz-item=report-cyber-security-report-2026

Dreiging rondom AI

AI model mythos van Anthropic

- Effectief in vinden kwetsbaarheden en misbruiken ervan
  - Het model vindt 27 jaar oude kwetsbaarheid in besturingssysteem (OpenBSD)
  - Vind verschillende kwetsbaarheden in Linux (kernel) en kan ze “koppelen”

    (dagen (mens) versus minuten (AI))

Mythos

- Advies NCSC:
  - “Neem AI-ontwikkelingen expliciet op in de beveiligingsmaatregelen binnen de zorgorganisatie, met name patchmanagement. Gevonden kwetsbaarheden waar (nog) geen patch voor is (zero-days) kun je niet voorkomen, maar de “time-to-patch” moet omlaag; uitstel van dagen of weken past niet meer bij het huidige dreigingslandschap.”
- Scenario waarschijnlijker: een bepaalde dienst (onderdeel IT) preventief offline halen
- Oefenen en nadenken voor continuïteit zorgprocessen:
  - Preventief offline halen
  - Welke business processen raakt dit? En hoe ga je hiermee om?

Verwachting

- Ontwikkeling waarschijnlijk niet beperkt tot dit model
- Concurrenten zullen komen → grotere beschikbaarheid
- Bruikbaar voor zowel aanvallers als verdedigers
- Dilemma-sessie Z-CERT rondom o.a. AI

SaaS: digitaal medicatiebeheer – casus Nieuw Zeeland

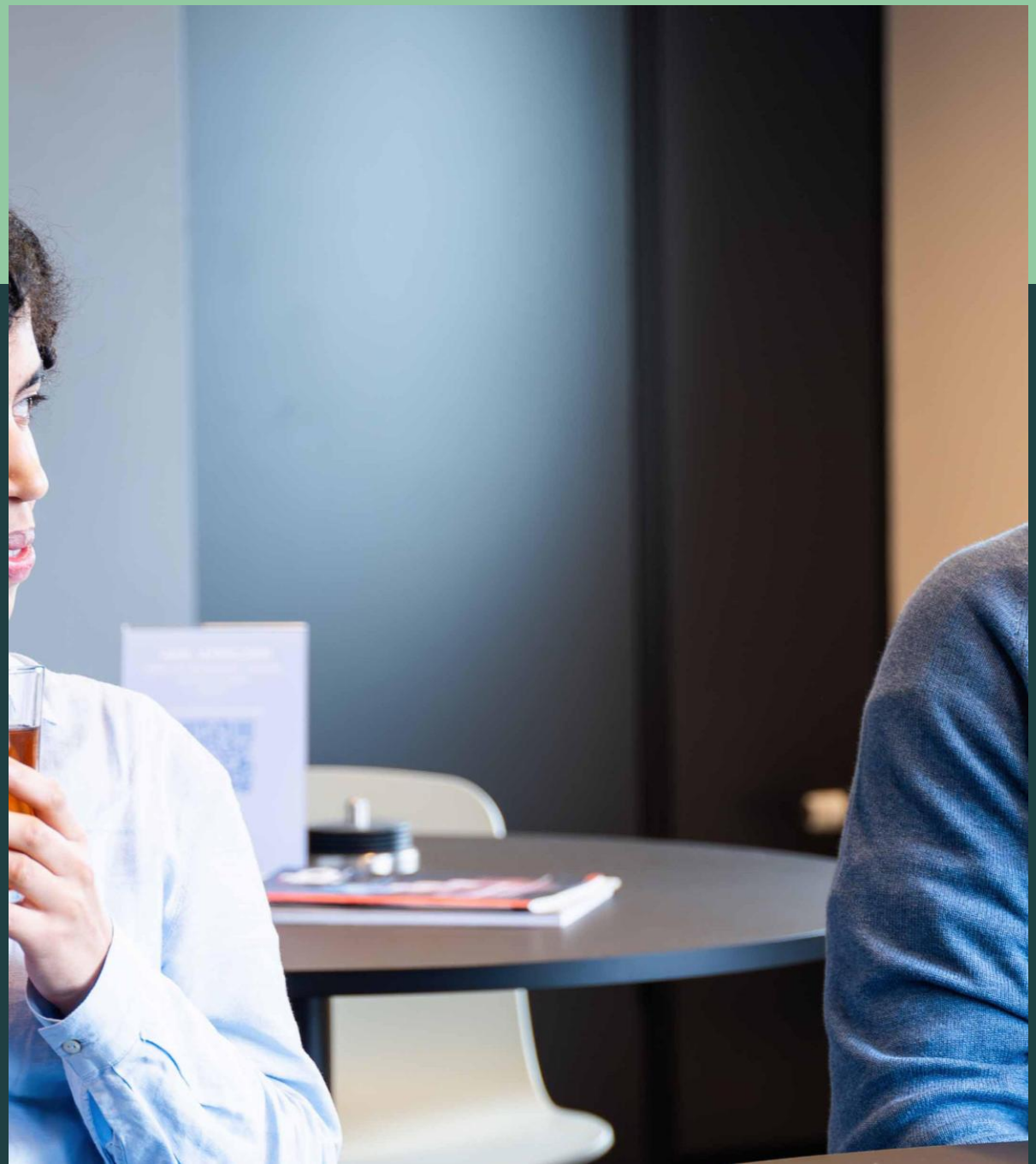
- Medimap: gebruikt in de ouderenzorg, gehandicaptenzorg, hospices etc
- Hacker krijgt toegang met geraden of gestolen credentials van 1 zorgverlener
- Wijzigingen:
  - Levende patiënten gelabeld als “overleden”
  - Namen veranderd in bekende politici
- SaaS-oplossing naar schatting 4 dagen offline uit voorzorg

https://www.healthcareitnews.com/news/anz/nz-meds-portal-medimap-goes-offline-after-hack

Poll

- *Openheid over fouten helpt ons veiliger te werken*

Bedankt voor de aandacht!



Voor vragen: onnotheuvenet@z-cert.nl

Z-CERT na inwerkingtreding Cyberbeveiligingswet (Cbw) – 2 labels:

csirt

Kosteloos voor entiteiten.

academy

€2500 ex btw per jaar

Z-CERT
CSIRT

De wettelijke taak

csirt

Waarschuwings-dienst

Kwetsbaarheden en, actieve dreigingen

Crisisnotificaties

Incident-coördinatie

24/7 Advies en coördinatie

Welke partij is wanneer nodig?

Groot netwerk achter de hand

Bewakingsdienst

Scannen IP-adressen en domeinnamen

Monitoring datalekken, darkweb, eigen analyse

Coördinatie Ethisch Hackers

Z-CERT ontzorgt en communiceert.

Centrale Hall of Fame sinds kort live!

Z-CERT
Academy

De wettelijke taak voorbij

academy

Digitale kennisbank

Whitepapers, handreikingen, factsheets, etc.

Toegang voor collega's tot dit platform

Self-service portal

Inzage & administratie

Contact-voorkeuren

Events

Om het jaar een groot fysiek evenement

Meerdere kleine bijeenkomsten

Webinars

Maandelijkse webinars

Eigen content en gastsprekers

Eigen aanspreek-punt

Business consultant helpt met vragen

'kennis-makelaar'

Grote community

Nu al 1000+ gebruikers

Spreek de hele zorg aan, niet alleen je eigen sector

Deelnemer worden

Vervolgstappen

csirt

academy

1a

Registreren
mijn.ncsc.nl

1b

Overeenkomst
ondertekenen

2

Informatie
aanleveren

3

Accounts
activeren

4

Borgen
processen

5

Optionele
betaalde opties

Informatieveilig gedrag op de werkvloer: concrete handvatten

Bettine Pluut
InformatieVeilig Gedrag in de Zorg (IVGZ)

16-06-2026

vereniging gehandicaptenzorg nederland

InformatieVeilig Gedrag in de Zorg (IVGZ)

Informeren, inspireren en activeren

De gedrags-component van veiligheid centraal

Gratis toegankelijke trainingen en hulpmiddelen

Agenda

- Rol van gedrag
- Toelichting direct toepasbare gedragsaanpak
- Rol en samenwerking van bestuurder en hun CISO
- Hulpmiddelen
- Aankondiging toolkit ‘grip op informatieveiligheid'

Incidenten komen vaak door gedrag…


Leidsch Dagblad · 18u

Vertrouwelijke jeugdzorgdocumenten in de privémailbox van een oud-bestuurder in Alphen; burgemeester doet aangifte

Vertrouwelijke documenten over de jeugdzorg in Alphen aan den Rijn zijn in de privémailbox van 'een oud-bestuurder' ...


CYBERVEILIGHEID

Datalek bij Limburgse voettherapie-keten: persoonlijke gegevens van duizenden cliënten mogelijk in verkeerde handen


Zorgorganisatie Pluryn meldt datalek door verloren USB-stick

De zorgorganisatie Pluryn meldt dat er een datalek heeft plaatsgevonden waarbij mogelijk gevoelige persoonsgegevens van medewerkers en cliënten betrokken zijn. Dit is het gevolg van het verlies van een USB-stick. Het bedrijf doet nog onderzoek naar het incident.

Volgens de organisatie is er in de week van 9 juni een onbeveiligde USB-stick verloren. Daarop stonden persoonsgegevens van cliënten en medewerkers, waaronder namen, adressen en burgerservicenummers. Mogelijk stonden er ook gegevens van voormalige cliënten en werknemers op de gegevensdrager. Vanwege de potentiële gevolgen van het incident heeft de organisatie een melding gedaan bij de Autoriteit Persoonsgegevens. Dit is verplicht wanneer de rechten en vrijheden van betrokkenen in het geding kunnen komen.

Het bedrijf doet nog onderzoek naar het incident en heeft daarvoor een externe partij ingeschakeld. Dit bedrijf kijkt of de verloren gegevens bijvoorbeeld ergens online te koop aangeboden worden. Getroffenen worden vanaf 17 juni geïnformeerd. De organisatie heeft een speciaal e-mailadres ingericht waar mensen vragen naar kunnen sturen, namelijk 'gegevensbescherming@pluryn.nl'. Ook is er een telefoonnummer beschikbaar: 088-779 3500.


AP waarschuwt voor gebruik van AI-chatbots na datalekmeldingen

De Autoriteit Persoonsgegevens waarschuwt voor de privacyrisico's die kleven aan het gebruik van AI-chatbots. De privacytoezichthouder zegt meldingen van datalekken door dergelijke tools te hebben ontvangen.

- Bron:
  Vertrouwelijke jeugdzorgdocumenten in de privémailbox van een oud-bestuurder in Alphen; burgemeester doet aangifte | Leidsch Dagblad
- Zorgorganisatie Pluryn meldt datalek door verloren USB-stick - IT Pro - Nieuws – Tweakers
- Datalek bij Limburgse voettherapie-keten: persoonlijke gegevens van duizenden cliënten mogelijk in verkeerde handen | De Limburger
- AP waarschuwt voor gebruik van AI-chatbots na datalekmeldingen - IT Pro - Nieuws - Tweakers

Conclusies uit publicaties en onderzoek

- 60% van alle datalekken ontstaat door ons eigen gedrag (Verizon 2025)
- Nieuwe ontwikkelingen (AI, NIS2/Cbw) maken cyberbeveiliging een strategische noodzaak
  - *“[Cyberveiligheid] vormt de basis voor operationele continuïteit, patiëntveiligheid en vertrouwen in gezondheidszorgsystemen. [Het is tijd om] over te stappen **van reactieve naar proactieve benaderingen**” (ICT& Health, 2026)*
- Samenwerking bestuur en experts kan en moet beter (IVGZ-onderzoek)

Stelling

“Meer dan 90% van de medewerkers in mijn organisatie zijn doordrongen van het belang van informatieveiligheid”

“Tijdens het begeleiden van een tr g in de
oefe aal werd ik e . Mijn
compute

Deze campagnes zijn gratis te gebruiken en op maat te maken

j
de praktijkeigenaar.”

De reputatie van jouw organisatie ligt op het spel

Laar zien dat gegevens bij jullie veilig zin

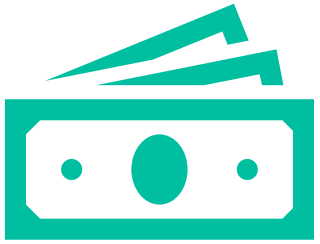
Gevolgen van hacks en incidenten

Identiteitsdiefstal

Geen zorg meer kunnen leveren

Inbreuk op de privacy

Geen vertrouwen meer in de organisatie



Financiële schade

Bedreiging

De alledaagse praktijk van medewerkers

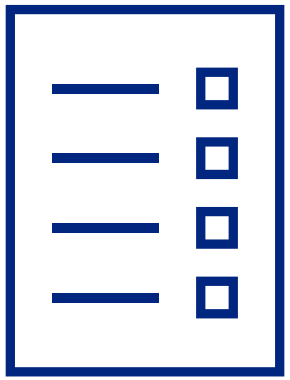
Voorbeeldsituatie:

Een medewerker gebruikt een externe AI-tool omdat die sneller werkt dan de door de organisatie goedgekeurde oplossing.

Mensen kiezen zelden bewust voor onveilig gedrag

Mensen doen wat op dat moment werkbaar, logisch of veilig voelt.

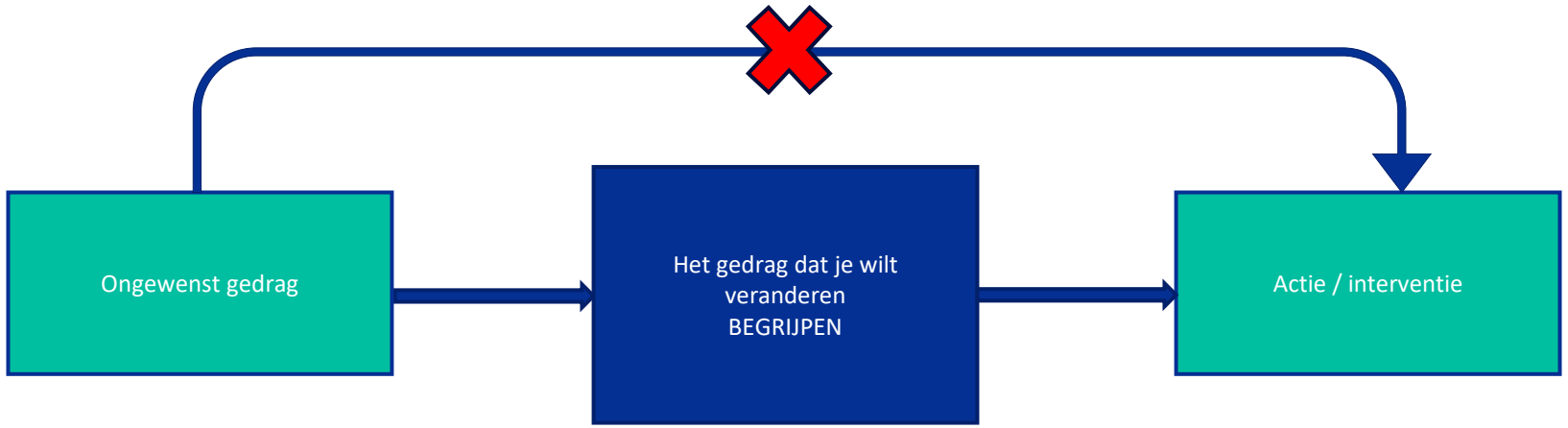
- gemak
- tijd
- goede patiëntenzorg
- sociale norm
- onzekerheid
- angst voor repercussies



Van probleem naar interventie

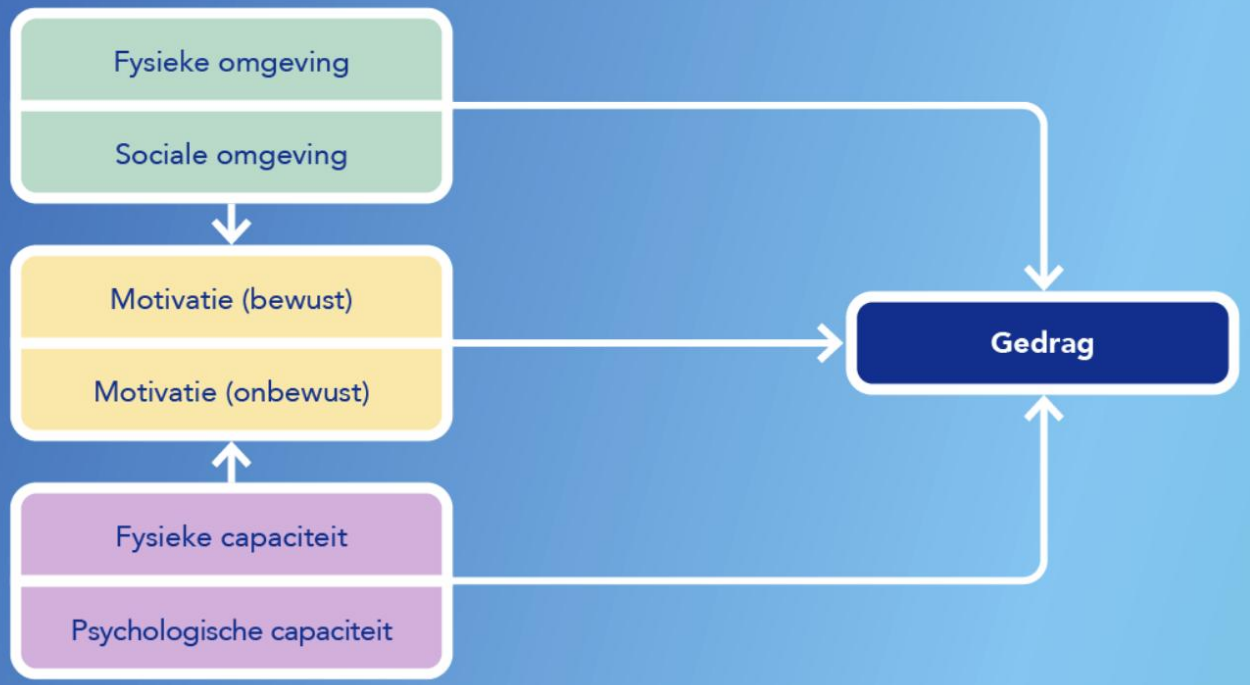
Een wegwijzer naar gedragsverandering

Waarom mislukken veel gedragsinterventies?



Een aanpak voor gedragsverandering

COM-B


Fysieke omgeving
Sociale omgeving
Motivatie (bewust)
Motivatie (onbewust)
Fysieke capaciteit
Psychologische capaciteit
Gedrag

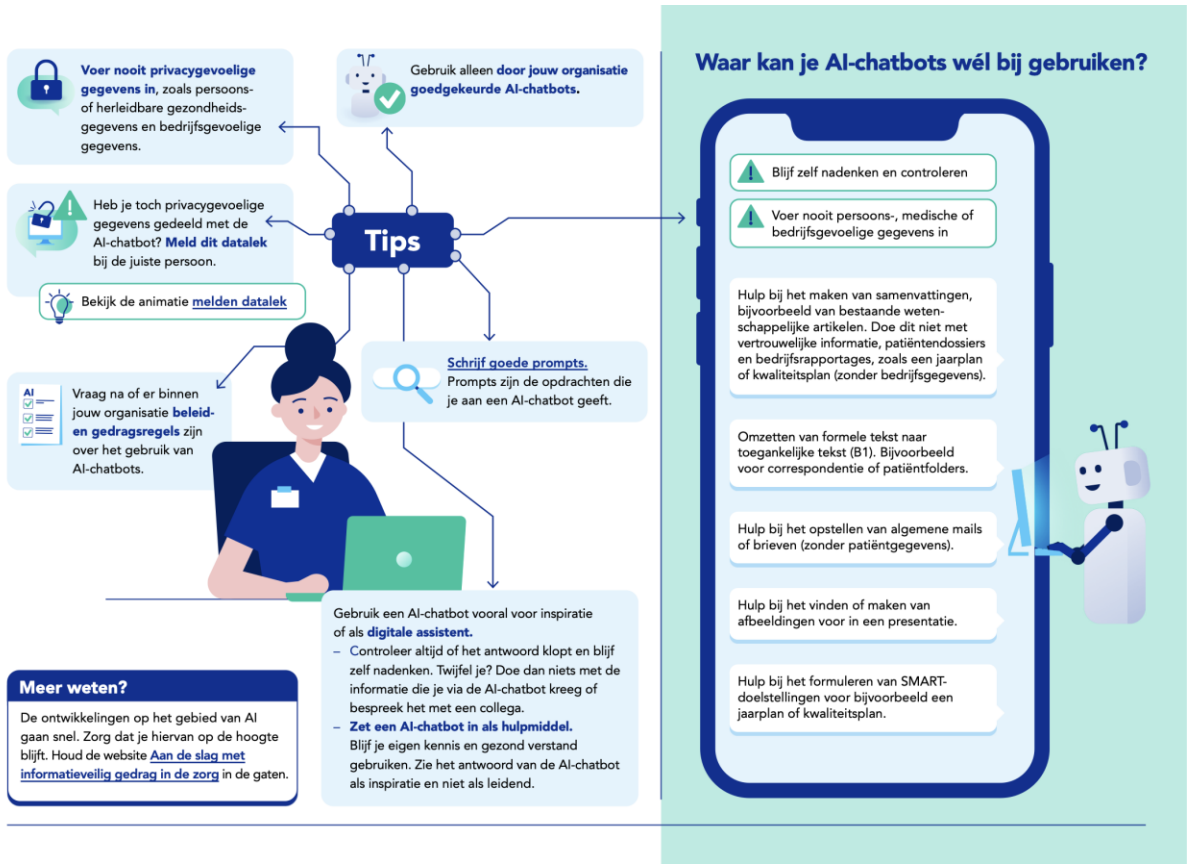
Sigra

Waarom gebruiken medewerkers toch onveilige tools?

Signaal uit de praktijk	COM-B
“De externe tool werkt sneller en beter”	Omgeving
“Ik weet niet precies welke tools wel/niet mogen”	Capaciteit
“Iedereen in mijn team gebruikt deze tool”	Omgeving
“Ik wil mijn werk sneller kunnen doen”	Motivatie
“De officiële tool werkt omslachtig”	Omgeving
“Wat kan er nou echt fout gaan?”	Motivatie
“Ik krijg vooral waardering voor het aantal uren dat ik draai”	Motivatie / omgeving

Onveilig gedrag ontstaat vaak uit een combinatie van afwegingen.

Een voorbeeld: hulpmiddel veilig gebruik van AI chatbots



Nog een voorbeeld: hulpmiddel datalek melden

Sigra

Wat betekent dit voor de rolverdeling in de organisatie?

De rol van jou en de expert informatieveiligheid

De bestuurder & NIS2

Naar verwachting treedt de Cyberbeveiligingswet 15 augustus 2026 in werking. Dit is de nationale NIS2-implementatiewet.

Wat betekent dit voor jullie als bestuurders?

- Eindverantwoordelijk en persoonlijk aansprakelijk
- Aantoonbare en actieve betrokkenheid vereist
- Snelle meldplicht bij incidenten (24 uur)

Concreet vraagt dit van bestuur:

- Integraal veiligheidsmanagement
- Opleidingsplicht (continu!)
- Regelmatige gesprekken met CISO / expert informatieveiligheid
- Structurele borging (“in control” zijn en blijven)

De rol van de expert

- Competentiekompas IVGZ:
  - Een profiel met
    - Taken en verantwoordelijkheden
    - Competenties
    - Kennis en ervaring
  - Advies over positionering in de organisatie: dichtbij met focus op verbinding van bestuur, management en praktijk
  - Reflectie- en ontwikkelingsvragen voor de expert

Competentie	Reflectie	Doel/actie
Adviesvaardigheid		
Strategisch inzicht		
Risicomanagement		
Sociale vaardigheden		
Projectmanagement		
Organisatiesensitiviteit		
Motiveren		

	Ontwikkeldoelen voor de komende periode
1	
2	
3	
4	
5	

Informatieveiligheid als gezamenlijk vraagstuk

- Bestuurders vinden het niet altijd eenvoudig om hun rol in informatieveiligheid te bepalen en het goede gesprek hierover te voeren.
- Daarom ontwikkelde IVGZ de toolkit Grip op informatieveiligheid. Deze ondersteunt bestuurders, informatieveiligheidsexperts en toezichthouders bij het voeren van betekenisvolle gesprekken over informatieveiligheid

VOOR KLEINE ORGANISATIES

Het goede bestuurlijke gesprek over informatieveiligheid:
Vijf succesfactoren

1: Maak het overleg integraal

Betrek diverse collega's bij het gesprek met jullie directeur/(praktijk)eigenaar, dus bijvoorbeeld ook mensen die met innovatie en kwaliteit bezig zijn. Door een diverse groep voorkom je een te eenzijdige focus op informatieveiligheid.

Koppel informatieveiligheid aan jullie bredere veiligheidscultuur. Link het dus bijvoorbeeld aan veiligheid van zorg of zelfs brandveiligheid. Dit voorkomt versnippering en vergroot de efficiëntie en effectiviteit van interventies.

2: Regelmaat en directe, korte lijnen

Organiseer elke 4 tot 8 weken een voortgangsoverleg voor continuïteit en opvolging. Wanneer er ook overleg is zonder de directeur/(praktijk)eigenaar, kan de frequentie met hem/haar naar eens per kwartaal.

Werk met een herkenbare voortgangsrapportage en vaste gespreksonderwerpen voor overzicht en focus.

Zoek elkaar tussendoor op bij incidenten of urgente dilemma's. Investeer dus in directe korte lijnen met de directeur/(praktijk)eigenaar.

3: Expliciet aandacht voor gedrag

Sta bewust stil bij gedrag om te voorkomen dat informatieveiligheid enkel een technische of papieren werkelijkheid is.

Sta stil bij wat gedrag verklaart. Het onderscheid tussen 'willen', 'kunnen' en 'gelegenheid' helpt hierbij. Pas als je een verklaring voor gedrag hebt, kun je passende interventies bedenken.

Maak in de voortgangsrapportage onderscheid tussen mens (gedrag), proces en techniek. Werk met verschillende vormen van sturingsinformatie.

Hulpmiddel: Bestuurlijke voortgangsrapportage

Hulpmiddel: Bestuurlijke dialoogkaarten

4: Agendeer kansen en dialoog

Maak bewust ruimte voor dialoog over visie, strategie en rolverdeling. Dit helpt om buiten de hectiek van alledag te werken aan een gezamenlijk kompas voor de besturing op informatieveiligheid

Kijk bewust ook naar kansen voor een win-win op veiligheid en vernieuwing. Eenzijdige sturing op het voorkomen van incidenten en minimaliseren van informatieveiligheidsrisico's remt innovatie.

5: Intelligent omgaan met risico's

Weeg informatieveiligheid als waarde in relatie tot andere waarden zoals efficiëntie, werkgeluk en kwaliteit van zorg.

Maak risico's concreet met scenario's en praktijk-voorbeelden. Dit maakt besluiten beter uitlegbaar en het gesprek wordt concreter en relevanter.

Prioriteer risico's samen en bespreek welke risico's acceptabel zijn. Leg bewuste risico's of uitzonderingen op beleid vast.

CONCEPT

Bestuurlijke voortgangsrapportage

Oplegger met highlights op mens, proces en techniek

Deze oplegger dient ter inspiratie en kan naar eigen inzicht worden overgenomen, aangescherpt of ingevuld

Periode: [...]

	Wat zien we? (bevindingen en trends)	Waarom relevant? (kansen en risico's)	Duiding (verklaring en dilemma's)	Bestuurlijke vraag (advies en te nemen besluiten)
Te beantwoorden vragen	• Welke KPI's, signalen en casussen vragen aandacht? • Wat zijn interessante ontwikkelingen? • Wat gaat anders dan verwacht?	• Welke doelen en stakeholders raakt dit? • Wat zijn de gevolgen van niets doen? • Wat kunnen we bereiken als we dit aanpakken?	• Wat betekent dit? • Hoe verklaren we dit? • Welke dilemma's volgen hieruit?	• Wat is het advies aan de bestuurder? • Waarop is extra sturing nodig? • Welke investeringen zijn nodig? • Welke risico's accepteren we, met welke onderbouwing en wie is eigenaar?
Fcator mens (willen, weten & kunnen, gelegenheid)				
Factor proces (beleid, afspraken, governance en samenwerking)				
Factor techniek (systemen, software, toegang, beveiliging, continuïteit)				

Voortgang op de factor mens

Onderlegger bij de bestuurlijke voortgangsrapportage

Deze onderlegger dient ter inspiratie en kan naar eigen inzicht worden overgenomen, aangescherpt of ingevuld

Periode: [...]

Thema	Soort sturingsinfo	Voorbeelden ter inspiratie	Norm	Huidige stand	Trend	Wat valt op/ vraagt aandacht?
Melden (willen)	KPI Signalen Casus	• Aantal datalekmeldingen (totaal of per team/afdeling) • % medewerkers dat incident meldde • % gemelde phishingmails versus phishing-clickrate • % medewerkers dat weet hoe te melden • Gesignaleerde verklaringen voor niet-melden • Voorbeelden van bijna-incidenten			↑=↓	
Aanspreekcultuur (willen)	KPI Signalen Casus	• % medewerkers en leidinggevenden dat afgelopen maand aangesproken is • % medewerkers dat afgelopen maand een collega heeft aangesproken • % medewerkers dat bewustzijn en/of aanspreken positief beoordeelt • Voorbeelden van corrigerend optreden			↑=↓	
Leiderschap en eigenaarschap (willen en kunnen)	KPI Signalen Casus	• Waardering van interne stakeholders over rolverdeling rond informatieveiligheid (cijfer 0-10) • Waardering van overleggen over informatieveiligheid (cijfer 0-10) • Geluiden over teams waar veel work-arounds bestaan die getolereerd worden • Voorbeelden van zichtbaar voorbeeldgedrag en leiderschap dat helpend was			↑=↓	
Onboarding en scholing (willen, weten en kunnen)	KPI Signalen Casus	• % medewerkers dat verplichte training binnen afgesproken termijn na indiensttreding heeft afgerond • % medewerkers dat opfriscursus / opfris-elearning heeft afgerond • Resultaten van toetsen / serious games • Veelgestelde vragen aan experts en/of helpdesk • Onderwerpen waarop fouten blijven optreden			↑=↓	
Werkbaarheid van maatregelen voor medewerkers (gelegenheid)	KPI Signalen Casus	• Aantal uitzonderingen op autorisatie-protocol • Aantal gesignaleerde work-arounds rond MFA • Wachttijd support/helpdesk • Waardering voor support/helpdesk (cijfer 0-10) • Doorlooptijd autorisatieverzoeken • Aantal datalekken waarbij werkdruk of ontevredenheid met software een rol speelde • Signalen over dat medewerkers werkbaarheid boven veiligheid plaatsen • Een voorbeeld van (gebrekkige) naleving van werkafspraken bij werkdruk			↑=↓	
Leren (willen, weten en kunnen)	KPI Signalen Casus	• Aantal afgeronde evaluaties van incidenten • Aantal ingezette verbeteracties en % afgeronde verbeteracties • Waardering medewerkers, cliënten/patiënten voor incident-afhandeling • Aantal gedeelde lessons learned • Signalen over angst onder medewerkers voor gevolgen van het melden van een fout • Verhaal van team dat professionaliseringsslag maakte na incident			↑=↓	

Inleiding ‘Bestuurlijke dialoogkaarten’

Waarover & hoe?

→ **Niveaus**

De kaarten zijn onderverdeeld in drie volwassenheidsniveaus:

- Starten: voor organisaties die bezig zijn de basis op orde te krijgen
- Groeien: voor organisaties die de basis willen doorontwikkelen
- Verdiepen: voor de gevorderde organisatie die meer diepgang wil

→ **Thema’s dialoogkaarten**

- Gedrag & cultuur
- Rollen & verwachtingen
- Leiderschap & voorbeeldgedrag
- Incidenten & leren
- Prioritering & schaarste
- Innovatie & informatieveiligheid
- Toezicht & verantwoording

Voorbeeld van een kaart

Starten: Leiderschap & voorbeeldgedrag

Stelling

"Medewerkers kijken vooral naar het gedrag van leidinggevenden om hun eigen gedrag te verdedigen"

Vragen

1. Welk voorbeeldgedrag willen we zien van leidinggevenden?
2. Wanneer geven leidinggevenden onbedoeld een verkeerd signaal af?
3. Hoe maken we informatieveiligheid zichtbaar in het dagelijks werk?

Dilemma

Een team gebruikt tijdelijk een AI-chatbot die volgens de werkafspraken eigenlijk niet gebruikt mag worden. Het team geeft aan hierdoor sneller te kunnen werken en een belangrijke deadline te halen. Wat doen we?

- Gedogen: In uitzonderlijke situaties moet dit soms kunnen
- Samen bespreken: We onderzoeken waarom teams afwijken van afspraken
- Norm stellen: Teams en leidinggevenden horen werkafspraken consequent te volgen

Link naar:

Onze materialen:

1. Wegwijzer ‘Aan de slag met informatieveiliggedrag’
2. Toolkit: Competentiekompas CISO
3. Toolkit: Veilig communiceren
4. Toolkit: Melden datalek
5. Toolkit: Veilig gebruik van AI-chatbots
6. Toolkit: Veilig omgaan met patiëntgegevens
7. Toolkit: Datalekken voorkomen

Onze socials:

1. Website: www.informatieveiliggedragindezorg.nl
2. LinkedIn: Aan de slag met informatieveilig gedrag
3. Spotify: Informatieveiligheid in de zorg begint bij de bestuurder
4. Youtube: Informatieveilig Gedrag in de Zorg

Binnenkort lanceren we onze nieuwe toolkit *Het bestuurlijke gesprek over informatieveiligheid*, met praktische handvatten voor bestuurders, toezichthouders en CISO’s

Afronding

Indien tijd: vragen?
Als we tijdens het webinar niet aan alle vragen zijn toegekomen, ontvangt u de antwoorden na afloop per e-mail

Afsluitende vraag: wat is uw belangrijkste inzicht?

De presentatie is opgenomen en u ontvangt deze, inclusief slides, na afloop.

Op 18 september organiseren we **webinar 3** over **gegevensuitwisseling en het gezondheidsinformatiestelsel**.
Meer informatie en aanmelden via deze link.
Als u zich al heeft aangemeld voor webinar 3, hoeft u dit niet opnieuw te doen.

vgn vereniging gehandicaptenzorg nederland