Cybersecurity-beeld Zorg 2025

De Nederlandse zorg digitaal veilig

Colofon

Stichting Z-CERT is hét expertisecentrum op het gebied van cybersecurity in de zorg. Het Cybersecuritybeeld Zorg beschrijft de belangrijkste digitale risico's voor de Nederlandse zorgsector van 2025. We gebruiken hiervoor de informatie uit meldingen van deelnemers, informatie van (inter-)nationale partners en kennisinstituten, eigen bevindingen, interviews met deskundigen, literatuuronderzoek, research van open bronnen en een enquête onder Nederlandse zorginstellingen.

Z-CERT is in 2017 opgericht op initiatief van de Nederlandse Vereniging van Ziekenhuizen (NVZ), de branchevereniging van de Nederlandse academische ziekenhuizen (UMCNL) en de Nederlandse GGZ. Z-CERT is een stichting en heeft geen winstoogmerk. We vormen een professioneel netwerk met de bij ons aangesloten zorginstellingen, het Nationaal Cyber Security Centrum (NCSC), Health-ISAC (Information Sharing and Analysis Center), brancheorganisaties, leveranciers en andere Computer Emergency Respons Teams (CERT's). Met elkaar pakken we cyberdreigingen aan, zoals ransomware, phishing, datalekken en hacken.

Disclaimer: De inhoud van dit Cybersecuritybeeld Zorg 2025 is met grote zorgvuldigheid samengesteld. Toch kan er onverhoopt een fout of onvolledigheid in zijn geslopen. Z-CERT en eventuele andere betrokken partijen kunnen daarvoor niet aansprakelijk worden gesteld. Voor tekstredactie en samenvatting is gebruikgemaakt van AI-ondersteunende hulpmiddelen. Er is geen nieuwe inhoud gegenereerd; alle inhoud is afkomstig van de auteurs en geverifieerd op basis van onderzoek en/of bronnen.

Inhoudsopgave

Colofon	2
Inhoudsopgave	3
Voorwoord	4
Samenvatting - Cybersecuritybeeld Zorg 2025	6
Dreigingsradar	7
Incidenten onder respondenten	9
Dreiging - Ransomware of afpersen met datalekken	10
Dreiging - Afpersing van leveranciers	17
Dreiging - Malware gericht op gebruikers	23
Dreiging - Phishing	28
Dreiging - DDoS op zorginstellingen	33
Dreiging - DDoS op leveranciers	38
Dreiging - Statelijke digitale operaties	42
Dreiging - Digitale financiële fraude in de zorg	47
Dreiging - Datalek door Insider Threat	52
Enablers van dreigingen	57
Aanbevelingen	61
Security beeld 2025	70
Extern aanvalsoppervlak	72
NEN 7510 certificering en tekortkomingen	74
Oefenen van dreigingsscenario's	77
Generatieve AI (GenAI)	80
Digitale autonomie	86
Uitleg bij dreigingsradar	90
Dankwoord	94

Voorwoord

"Zorg moet rekening houden met langdurige uitval van digitale systemen..."

In 2025 werd opnieuw zichtbaar hoe interessant de zorgsector is voor cybercriminelen. Z-CERT ontving dat jaar meldingen van ongeveer tien geslaagde digitale aanvallen op leveranciers van zorginstellingen. De ransomwareaanval op Clinical Diagnostics Nederland was daarvan een sprekend voorbeeld. Zulke incidenten laten zien hoe kwetsbaar de keten is: een verstoring bij één partij kan al snel gevolgen hebben voor processen, voor uitwisseling van gegevens en uiteindelijk voor de kwaliteit en veiligheid van de zorgverlening.

Digitale uitval raakt patiënten en zorgverleners

Wat we niet mogen vergeten: achter elke digitale storing zitten mensen die afhankelijk zijn van zorg én professionals die hun werk zo goed mogelijk willen blijven doen. Patiënten die wachten op een diagnose, een behandeling of een uitslag. Zorgverleners die hun werk zorgvuldig willen doen, maar afhankelijk zijn van systemen om dat veilig en op tijd te kunnen. Wanneer digitale hulpmiddelen wegvallen, is dat niet alleen een technisch probleem. Het zorgt voor onzekerheid, spanning en soms vertraging in de zorg die vaak direct gevoeld wordt.

Voorwoord, vervolg

Digitale dreiging als dagelijkse realiteit

De zorg leunt steeds meer op digitale systemen, cloudomgevingen en SaaS toepassingen. Gevoelige gegevens en belangrijke processen staan verspreid over verschillende platformen, vaak ook bij leveranciers. Dat maakt die keten aantrekkelijk voor aanvallers. Technieken om binnen te komen worden bovendien slimmer. Infostealers die inloggegevens buitmaken en phishingmails die bijna niet van echt te onderscheiden zijn, vormen dagelijks de eerste stap naar zwaardere aanvallen. Deze ontwikkeling laat opnieuw zien dat digitale dreiging geen abstract IT onderwerp is, maar een realiteit die iedereen in de zorg raakt.

Voorbereiden op langdurige uitval

Daarom is het belangrijk dat zorgorganisaties nadrukkelijk rekening houden met scenario's waarin systemen langere tijd uitvallen. Een ransomwareaanval, een grote IT storing of het verlies van toegang tot cruciale applicaties kan de zorgverlening direct ontregelen. In zo'n situatie hebben zorgprofessionals behoefte aan duidelijkheid: hoe gaan we verder, wie kunnen we bellen, wat is het alternatief? Een (op papier beschikbaar) digitaal noodpakket helpt daarbij. Het is te vergelijken met het fysieke noodpakket voor thuis: bedoeld om te blijven functioneren wanneer het gewone even niet werkt, zodat de zorgverlening veilig doorgaat. Ook als de digitale infrastructuur stilvalt.

"In een sector die steeds digitaler wordt, is een noodpakket geen luxe. Het is een basisvoorwaarde..."

Samenwerken en oefenen

Zo'n noodpakket werkt alleen wanneer het actueel is, bekend in de organisatie en regelmatig wordt geoefend. Dat vraagt om samenwerking, binnen de eigen organisatie maar vooral ook met leveranciers en ketenpartners. Want veilige zorg leveren bij langdurige IT uitval kan alleen als iedereen weet welke afspraken gelden, welke processen kunnen worden ingezet en hoe de onderlinge bereikbaarheid is geregeld. Het biedt niet alleen structuur in een technische crisis, maar geeft ook rust aan de mensen die op dat moment hun werk moeten doen.

In een sector die steeds digitaler wordt, is een noodpakket geen luxe. Het is een basisvoorwaarde om zorg betrouwbaar en toegankelijk te houden, juist wanneer systemen ons tijdelijk in de steek laten.

Wim Hafkamp - Directeur Z-CERT

Samenvatting Cybersecuritybeeld Zorg 2025

Zorginstellingen hebben te maken met een groeiende afhankelijkheid van leveranciers, cloudoplossingen en medische technologie. Tegelijkertijd worden aanvallers professioneler, sneller en creatiever in hun aanvalsmethoden.

Ransomware

Ransomware blijft de grootste bedreiging voor de zorgsector. Aanvallen leiden regelmatig tot versleuteling van systemen, diefstal van patiëntgegevens en verstoringen van zorgprocessen. Zowel kleine als grote zorginstellingen worden getroffen, en ook leveranciers blijven niet buiten schot. Incidenten bij laboratoria, IT-dienstverleners of medische softwareleveranciers hebben directe gevolgen gehad voor tientallen aangesloten zorgorganisaties en vooral voor mensen die gebruikmaken van die zorg.

Malware, phishing en digitale fraude

Daarnaast vormen malware, phishing en digitale fraude risico's. Een veel voorkomende aanval wordt uitgevoerd met infostealers. Hiermee proberen criminelen wachtwoorden buit te maken die vervolgens worden ingezet om toegang te krijgen tot bijvoorbeeld mailaccounts, cloudomgevingen of VPN-systemen. Phishing wordt steeds verder doorontwikkeld.

Generative AI

Dankzij AI-gegenereerde berichten en nieuwe technieken wordt digitale fraude, zoals CEO-fraude en gemanipuleerde facturen, steeds lastiger te ontdekken.

Statelijke actoren

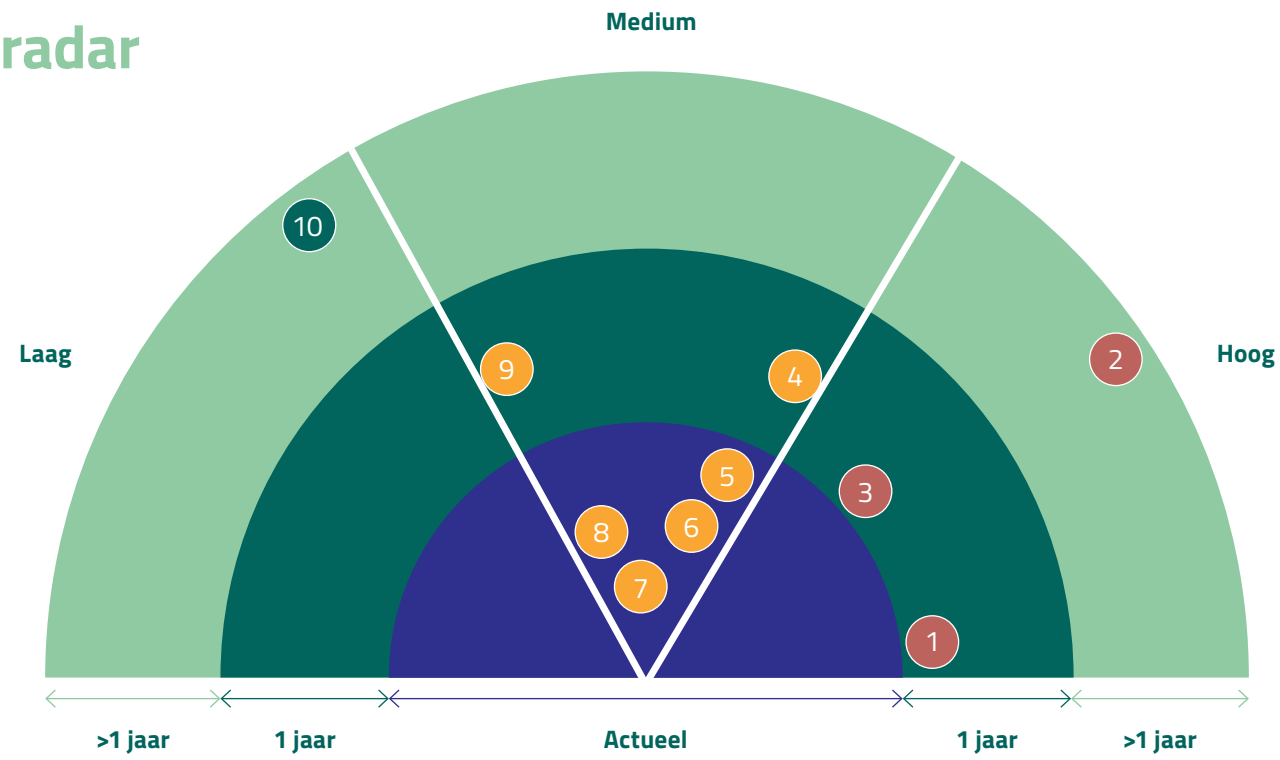
Een andere belangrijke dreiging komt van statelijke actoren die zich richten op spionage en datadiefstal. Dit is vooral een risico voor organisaties die beschikken over onderzoeksgegevens of grote medische datasets. Hoewel zulke incidenten moeilijk te detecteren zijn, laten analyses zien dat de zorgsector een doelwit is.

Insider Threats

Ook zagen we noemenswaardige incidenten in de categorie 'insider threats'. Ook al zijn dergelijke incidenten soms het gevolg van kleine foutjes, ze kunnen grote impact hebben. Tot slot laat het rapport zien dat 'enablers' zoals AI, geopolitieke spanningen, dataconcentratie, personeelstekorten en afhankelijkheid van grote technologiebedrijven de dreiging vergroten.

Om de digitale weerbaarheid van de zorg te versterken moet niet alleen de basisbeveiliging bij zorginstellingen op orde zijn. Er moet ook aandacht zijn voor leveranciersmanagement en crisisvoorbereiding met realistische oefenscenario's.

Dreigingsradar



1. Ransomware of afpersen met datalekken
2. Spionage (onderzoek)
3. Ransomware of afpersen met datalekken bij leverancier
4. DDoS bij leverancier
5. Malware
6. Credential phishing
7. Insider threats
8. Financiële fraude
9. DDoS
10. Spionage (reguliere zorginstellingen)

Lees ook de uitgebreide uitleg over de radar op pagina 90.

Toelichting

Beheersmaatregelen

In het Cybersecuritybeeld bieden we per dreiging zogenaamde handelingsperspectieven aan. Dit zijn adviezen waarbij wij verwijzen naar CIS Controls versie 8. De CIS Controls (Critical Security Controls) zijn een reeks beproefde methoden die organisaties vaak gebruiken om maatregelen uit de NEN 7510 of ISO 27001 praktisch in te richten. We verwijzen regelmatig naar deze CIS Controls zodat het eenvoudiger wordt om aandachtspunten te implementeren.

Meer lees je op https://www.cisecurity.org/controls

Actortypologie

Voor dit dreigingsbeeld sluiten we aan bij de actortypologie uit het Cybercrimebeeld Nederland 2024 van de politie en het Openbaar Ministerie. Een uitgebreide toelichting op deze indeling en de wijze waarop Z-CERT deze toepast, is opgenomen aan het einde van dit document.

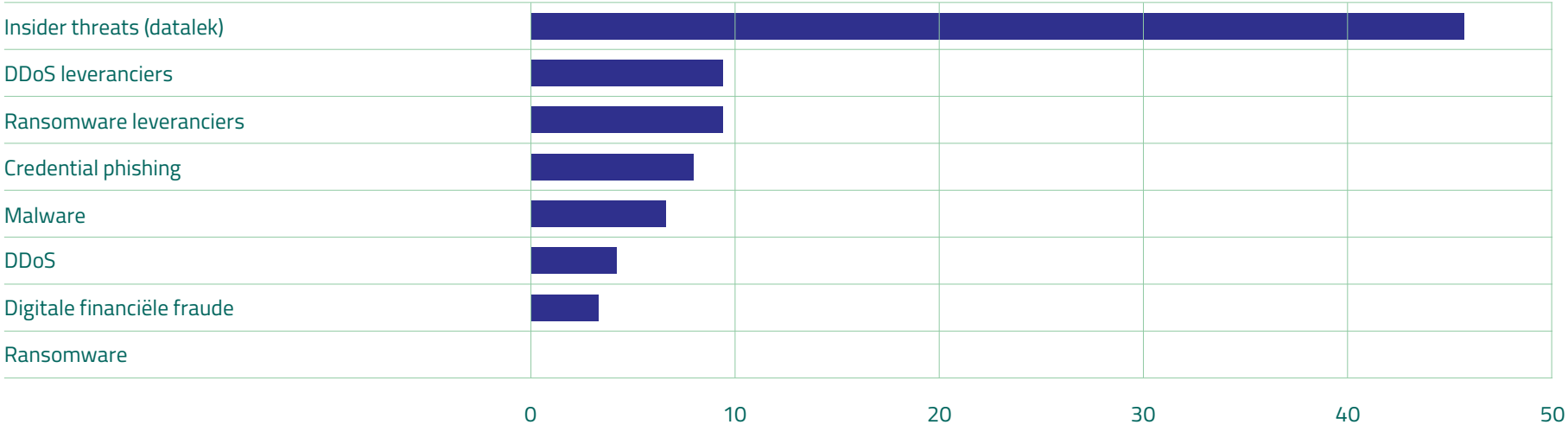
Incidenten onder respondenten

Voor het Cybersecuritybeeld heeft Z-CERT bij deelnemers geïnformeerd naar het type security-incidenten dat zij hebben meegemaakt. Bijna een vierde van de deelnemers heeft deze survey ingevuld. De resultaten worden hieronder weergegeven in een grafiek.

Deze informatie kan worden gebruikt om bewustwording te creëren binnen uw eigen organisatie en om maatregelen te prioriteren. De incidenten zullen verder besproken worden in de hoofdstukken over 'dreigingen' en zijn onder andere gebruikt om de dreigingsniveaus vast te stellen.

Het percentage geeft weer hoeveel procent van het totaal aantal respondenten één of meerdere incidenten hadden in deze categorie. Bij de categorie digitale financiële fraude in de grafiek gaat het om geslaagde financiële fraudepogingen die zijn gepleegd via digitale kanalen, zoals email en WhatsApp. Bij de categorie 'malware' in deze grafiek gaat het specifiek om malware die ontworpen is om gebruikers te verleiden deze malware op te starten. De categorie 'insider threats' is omvangrijk. Het gaat in dit Cybersecuritybeeld om datalekken die het gevolg zijn van onopzettelijkheid, nalatigheid, nieuwsgierigheid en kwaadwillend handelen door interne en externe betrokkenen, zoals medewerkers, leveranciers en ingehuurde krachten.

Figuur 1: Percentage respondenten dat geraakt werd per type incident



Dreiging
Ransomware of afpersen met datalekken

Dreiging - Ransomware of afpersen met datalekken

Inschatting dreiging: Hoog

Tijd: tot 1 jaar

In 2025 zijn er 3 incidenten bij Nederlandse zorginstellingen gemeld bij Z-CERT. Op Europees niveau zien we in de zorgsector een aantal keer per kwartaal afpersing middels ransomware of openbaarmaking van gestolen data.

Dreigingsniveau: Hoog

Z-CERT classificeert deze dreiging als hoog. Jaarlijks vinden er incidenten plaats in de Nederlandse zorgsector. De impact in Nederland bleef relatief beperkt, maar zorgprocessen kunnen in potentie verstoord raken en gevoelige patiëntgegevens openbaar worden gemaakt. In Europa kwamen ook dit jaar ziekenhuizen stil te liggen en verscheen gevoelige data online.

Actor: cybercriminelen met technische ervaring en georganiseerde cybercrime

Veel ransomware-groepen werken volgens een model waarbij één groep zich specialiseert in het verkrijgen van initiële toegang, de ransomware-operator ondersteunende diensten levert zoals tooling, infrastructuur en financiële afhandeling, en een partner uiteindelijk de infiltratie van het netwerk en de ransomware-uitrol uitvoert.

Capaciteit

Ransomware-groeperingen zijn doorgaans goed georganiseerd en beschikken over ruime financiële middelen om hun operaties te ondersteunen en te verbeteren. Een klein aantal groepen, zoals Cl0p, zet deze middelen in om onbekende kwetsbaarheden (zero-days) in software te misbruiken. In het geval van Cl0p gaat het onder meer om kwetsbaarheden in online bestandsopslagoplossingen [1] en een ERP-systeem [2].

Motivatie

Vooral financieel gewin.

Intentie

Veel ransomware-actoren benutten kansen zodra zich een mogelijkheid voordoet in de zorg. De sector staat wereldwijd op plek vier qua afpersen met gestolen data [2]. Z-CERT identificeerde 36 groepen die zorginstellingen als doelwit zien. Binnen de Ransomware-as-a-Service wereld zien we tweevoudige afpersing (versleuteling én dreigen met publicatie) en enkelvoudige afpersing, waarbij alleen wordt gedreigd met openbaarmaking van gestolen data. Die laatste methode wint terrein, waarschijnlijk omdat deze sneller uitvoerbaar is. Dit leidt tot een hoger rendement per aanval en bovendien is de kans om gedetecteerd te worden kleiner [2] [9].

Ook gebruiken ransomware-groepen andere drukmiddelen. De ransomware-groep Qilin zet juristen in om extra druk uit te oefenen, bijvoorbeeld door slachtoffers te

Dreiging - Ransomware of afpersen met datalekken, vervolg

wijzen op vermeende wetsovertredingen. Daarnaast geeft Qilin hackers de mogelijkheid DDoS-aanvallen uit te voeren [3].

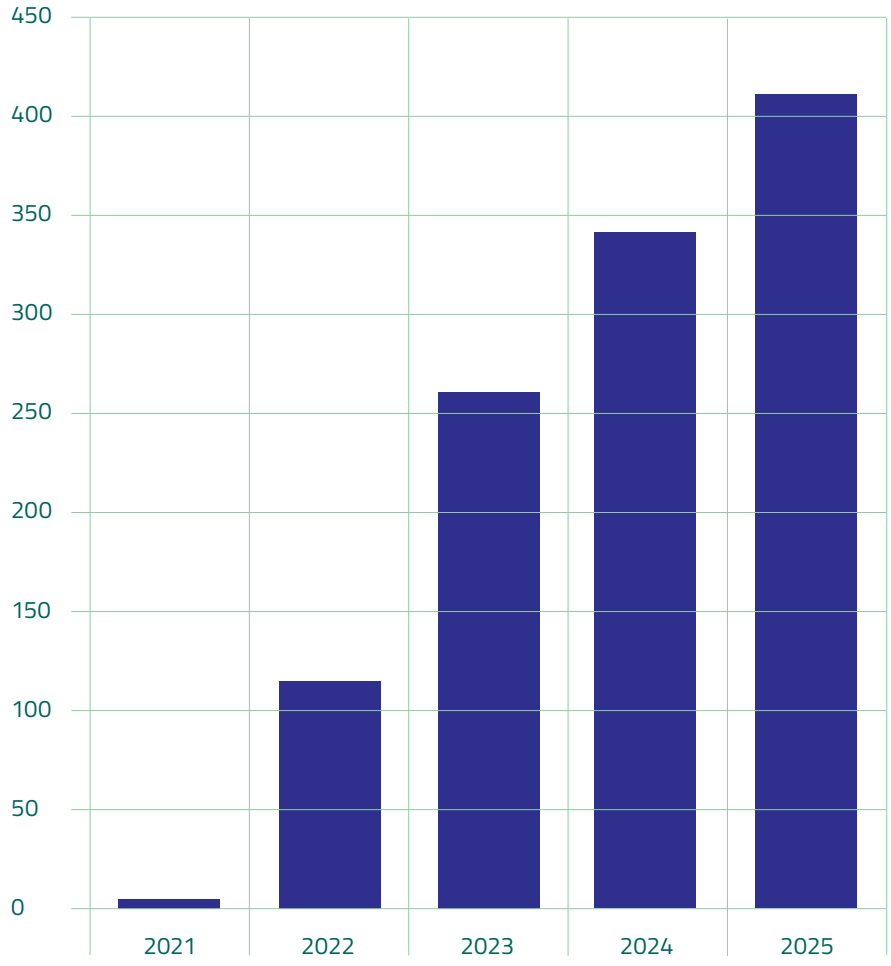
Hoe werd de dreiging zichtbaar?

Bij Z-CERT zijn drie ransomware-incidenten bij Nederlandse zorginstellingen bekend: een ziekenhuis, een fysiotherapeut en een commerciële kliniek. In twee gevallen waren netwerken met operationele technologie betrokken: een gebouwbeheer-systeem en systemen die betrokken waren bij energievoorziening.

Wereldwijd steeg in de zorgsector het aantal incidenten dat op datalekwebsites op het darkweb gepubliceerd wordt met 21%. Voor de zorgsector in Europa bleef het aantal gepubliceerde incidenten vrijwel gelijk ten opzichte van vorig jaar [8].

Ransomware-actoren zijn niet alleen uit op grote vermogende organisaties. Veel van de in Europa geclaimde incidenten betroffen juist kleine zorgverleners met minder dan 49 medewerkers, al zagen we in vrijwel alle grotere organisaties slachtoffers terugkomen. Klinieken en ziekenhuizen zijn het vaakst getroffen, gevolgd door huisartsenpraktijken en hospices; ook thuiszorgorganisaties, een ouderenzorginstelling en een ambulancedienst werden geraakt [8].

Figuur 1: Incidenten bij zorginstellingen wereldwijd, gepubliceerd op datalekwebsites van cybercriminelen.



Dreiging - Ransomware of afpersen met datalekken, vervolg

Impact

Van 77% van Europese zorgorganisaties die op datalekwebsites verschenen, werd daadwerkelijk data openbaar gemaakt [8]. Uit een onderzoek in de internationale zorgsector over een deel van 2025 bleek dat gemiddelde losgeldbedrag rond de 150.000 dollar lag, terwijl herstelkosten gemiddeld oplopen tot ongeveer 1 miljoen dollar, exclusief losgeld [4]. De hersteltijd varieert sterk. Ongeveer een derde van de zorginstellingen herstelt binnen een week, maar een aanzienlijk deel heeft meerdere weken tot maanden nodig. De impact kan groot zijn en zorgprocessen raken.
Bij een incident in een Frans ziekenhuis moest het personeel overschakelen op pen en papier omdat IT-systemen preventief waren uitgeschakeld [5].

Voorbeelden van incidenten in Nederland

- Bij een ziekenhuis werd een geïsoleerd OT-netwerk voor de energievoorziening getroffen door ransomware. De impact bleef beperkt. Aanvallers verkregen toegang omdat een externe toegangsoplossing (RDP) met een zwak wachtwoord vanaf het internet bereikbaar was. Deze externe toegang viel onder shadow-IT en was niet bekend bij de security en IT-afdelingen. Bovendien had het netwerk een aparte internetverbinding waardoor het onder de radar bleef.
- Een fysiotherapiepraktijk hostte een archief dat toegankelijk was via een externe toegangsoplossing (RDP). Een aanvaller kon hierop inloggen.
- Een gebouwbeheersysteem van een zorginstelling werd binnengedrongen doordat TeamViewer (een externe toegangsoplossing) ontsloten was aan het internet en een aanvaller daarop inlogde. De impact bleef beperkt.

Hoe gaan aanvallers te werk?

Om maatregelen goed te kunnen prioriteren, is het belangrijk te weten hoe aanvallers te werk gaan. We volgen daarbij op hoofdlijnen de drie fases van een aanval (In, Through en Out) zoals beschreven in de unified kill chain [6]. De unified kill chain is een model dat de verschillende stappen van een aanval gestructureerd beschrijft.

Fase 1: In

Uit een wereldwijd onderzoek [4] naar 291 ransomware-incidenten in de zorg blijkt dat de volgende vier technieken het meest werden gebruikt voor initiële toegang.

- Misbruik van kwetsbaarheden van aan het internet ontsloten systeem.
- Mail waarbij gebruiker wordt verleid malware op te starten
- Gebruik van te koop aangeboden inloggegevens
- Phishing

Fase 2: Through

Uit een onderzoek [7] naar bijna-ransomware-incidenten over een periode van tweeënhalf jaar bleek dat de volgende drie technieken het meest werden ingezet om het netwerk te infiltreren of om toegang te behouden:

Dreiging - Ransomware of afpersen met datalekken, vervolg

- Benutten van de onnodige grote bewegingsruimte in het netwerk.
- Het gebruik van legitieme externe-toegangssoftware zoals TeamViewer en AnyDesk om toegang te behouden tot de IT-infrastructuur.
- Aanvallers proberen extra accounts en toegangsrechten te bemachtigen door digitale sleutels en wachtwoordgegevens uit systemen te halen.

Fase 3: out

De volgende activiteiten werden veel waargenomen in deze fase, gericht op het behalen van de doelen van de aanvaller [4]:

- Data-diefstal
- Dataversleuteling door de aanvaller.
- Verstoring van processen

Verwachting volgend jaar

De door ransomware-as-a-servicegroepen gepubliceerde incidenten op datalekwebsites laten de afgelopen jaren wereldwijd een duidelijke stijging zien [2] [8]. Dit kan mogelijk worden verklaard door een groei in zowel het aantal actieve groepen als hun gezamenlijke capaciteit [2]. Daarnaast nemen de mogelijkheden voor aanvallers om binnen te komen niet af maar eerder toe, zoals toegelicht in de hoofdstukken over phishing en malware. Op basis hiervan acht Z-CERT het aannemelijk dat deze trend doorzet en verwacht Z-CERT in 2026 opnieuw enkele incidenten in de Nederlandse zorg.

Aandachtspunten voor komend jaar

- Aan het internet ontsloten systemen (VPN-oplossingen) blijven onverminderd doelwit.
- Nieuwe malware- en phishingtechnieken.
- Cloudomgevingen maken steeds vaker deel uit van aanvallen [3] [4], vooral omdat gevoelige data en back-ups daar staan.
- Vanuit het buitenland krijgen we steeds vaker signalen dat hackers IT-helpdesks bellen om wachtwoorden te resetten of MFA-methoden toe te voegen. Ook hebben criminelen geprobeerd om het slachtoffer malware te laten opstarten [9].
  In Nederland heeft Z-CERT hier nog geen voorbeelden van gezien, maar het kan in de toekomst een aandachtspunt worden.

Aanbevelingen

- Bescherm uw werkplekken en servers tegen malware
- Optimaliseer uw MFA tegen AiTM phishing
- Beveilig externe toegang met MFA.
- Prioriteer bij patchen aan het internet ontsloten systemen
- Identificeer aanvalspaden in uw netwerk en blokkeer deze.
- Gebruik accounts met hoge rechten uitsluitend op speciaal daarvoor ingerichte systemen, niet op gebruikerscomputers.

Voor aanvullende en meer gedetailleerde aanbevelingen, zie hoofdstuk '**Aanbevelingen**'.

Dreiging - Ransomware of afpersen met datalekken, vervolg

Enablers

- Data verspreiding en concentratie
- Tijdelijke medewerkers en hoog personeelsverloop
- Gebrek aan security awareness
- AI

Zie hoofdstuk 'Enablers' voor de uitwerking van de enablers.

Enablers

Bibliografie

[1] **NCSC**, "NCSC waarschuwt voor Cl0p-campagnes die zich richten op filetransfer-systemen," 6 Februari 2025. [Online]. Available: https://www.ncsc.nl/actueel/nieuws/2025/01/06/nationaal-cyber-security-centrum-ncsc-waarschuwt-voor-cl0p-campagnes-die-zich-richten-op-filetransfer-systemen

[2] **GuidePoint Security**, "2026 Ransomware and Cyber Threat Report," 2026. [Online]. Available: https://www.guidepointsecurity.com/resources/grit-2026-ransomware-cyber-threat-report-presentation-pd/

[3] **Cybereason**, "Ransomware Gangs Collapse as Qilin Seizes Control," 2025. [Online]. Available: https://www.cybereason.com/blog/threat-alert-qilin-seizes-control

[4] **Sophos**, "The State of ransomware in Healthcare 2025," October 2025. [Online]. Available: https://news.sophos.com/en-us/2025/10/08/the-state-of-ransomware-in-healthcare-2025/

[5] **L'Usine Digitale**, "Centre hospitalier intercommunal de Haute-Comté," 20 Oktober 2025. [Online]. Available: https://www.usine-digitale.fr/article/une-cyberattaque-touche-l-hopital-de-pontarlier-son-systeme-informatique-a-l-arret.N2239874

[6] **Paul Pols**, "The Unified Kill Chain," [Online]. Available: https://www.unifiedkillchain.com/

[7] **Talos**, "Stopping ransomware before it starts: Lessons from Cisco Talos Incident Response," [Online]. Available: https://blog.talosintelligence.com/stopping-ransomware-before-it-starts/

[8] **Z-CERT**, Intern onderzoek Z-CERT, 2025.

[9] **Microsoft**, "Microsoft Digital Defense Report 2025," p. 28, 2025.

Dreiging
Afpersing van leveranciers

Dreiging - Afpersing van leveranciers door middel van ransomware en datalekken

Inschatting dreiging: Hoog

Tijd: 0 tot 6 maanden

Bij Z-CERT zijn in 2025 een tiental gevallen gemeld van geslaagde digitale aanvallen gericht tegen leveranciers van zorginstellingen. De meest in het oog springende casus betrof de ransomware-aanval op Clinical Diagnostics Nederland, met vooral aanzienlijke impact voor de personen van wie persoons- en medische gegevens zijn gestolen [10]. Daarnaast zijn ook andere binnen- en buitenlandse leveranciers afgeperst met ransomware. En in sommige gevallen is reputatieschade ontstaan door de diefstal van gegevens bij deze leveranciers.

Dreigingsniveau: Hoog

Z-CERT schat het dreigingsniveau voor incidenten door ransomware en/of afpersen met openbaar maken van gegevens bij leveranciers van zorginstellingen in als 'hoog'. Dit kunnen IT-leveranciers zijn, maar net zo goed leveranciers buiten het IT-domein. Hoe groter de afhankelijkheid, hoe groter de mogelijke impact.

Actor: cybercriminelen met technische ervaring en georganiseerde cybercrime

Veel ransomwaregroepen werken volgens een model waarbij één groep zich specialiseert in het verkrijgen van initiële toegang, de ransomware-operator ondersteunende diensten levert zoals tooling, infrastructuur en financiële afhandeling, en een partner uiteindelijk de infiltratie van het netwerk en de ransomware-uitrol uitvoert.

Intentie

In toenemende mate worden persoons- en medische data opgeslagen bij toeleveranciers die ontsloten worden via SaaS-applicaties. Dit maakt deze toeleveranciers aantrekkelijke doelwitten voor aanvallers. Door slechts één doelwit aan te vallen krijgt de aanvaller potentieel toegang tot de infrastructuur of gevoelige informatie van enkele tientallen tot honderden klanten. Niet alleen kunnen deze gegevens als extra drukmiddel worden gebruikt, ook biedt het makkelijk nieuwe potentiële slachtoffers. Daarnaast is de leveranciersketen voor de zorg divers en bedient zij niet alleen zorginstellingen, maar bijvoorbeeld ook overheidsorganisaties of onderzoeksinstituten. Het verkrijgen van illegale toegang tot het IT-netwerk van zo'n leverancier opent deuren die ook interessant zijn voor bijvoorbeeld buitenlandse inlichtingendiensten. Volgens onder andere onderzoekers van EU-agentschap ENISA kunnen cybercrime groepen daarnaast hun toegang tot zo'n leveranciersnetwerk of

Dreiging - Afpersing van leveranciers door middel van ransomware en datalekken, vervolg

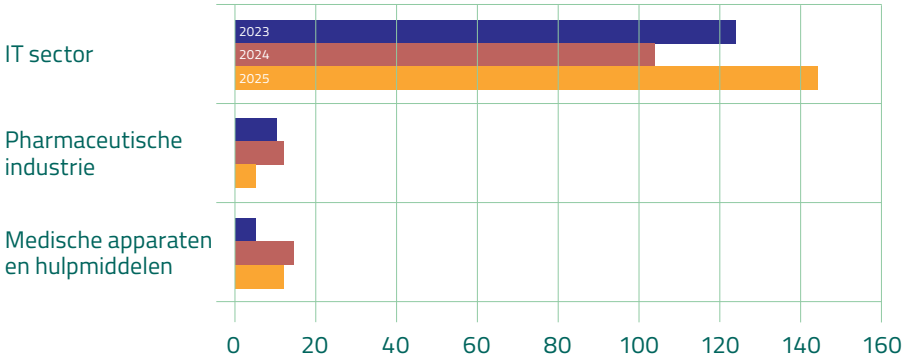
de gestolen data 'verkopen' aan de inlichtingendienst van het land van waaruit de cybercriminelen opereren [11] [12] [13].

Hoe werd de dreiging zichtbaar?

In onderstaande grafiek zijn de aantallen geclaimde aanvallen weergegeven gericht tegen leveranciers van de Europese zorgsector. Deze cijfers gaan uitsluitend over incidenten die op het dark web gepubliceerd zijn en die bij ons bekend zijn. Niet alle incidenten worden openbaar. Een onderzoek uit 2025 laat bijvoorbeeld zien dat bij 27% van de incidenten waarbij data versleuteld werd, data gestolen werd [4].

Opvallend is dat in 2025 de hoeveelheid geclaimde aanvallen op de farmaceutische industrie sterk is afgenomen zijn ten opzichte van voorgaande jaren. Het aantal aanvallen gericht tegen IT-sector blijft onverminderd hoog.

Figuur 2: Aantallen incidenten per jaar per type toeleverancier in Europa sinds 2023.



Algemene impact incident bij toeleverancier

Een hack bij een toeleverancier van een zorgorganisatie kan gevolgen hebben voor continuïteit en patiëntveiligheid. Bij ransomware kunnen systemen en diensten van de leverancier stilvallen, waardoor zorgprocessen vertragen of zelfs stilvallen. Dit raakt bijvoorbeeld medische technologie, domotica of IT-diensten. Een datalek vormt een groot risico voor privacy: gevoelige patiëntgegevens zoals medische dossiers kunnen op het dark web belanden, wat identiteitsfraude en afpersing mogelijk maakt.

Daarnaast leidt een incident tot reputatieschade, verlies van vertrouwen bij patiënten en partners, en kan het juridische en financiële consequenties hebben, zoals boetes wegens schending van de AVG. De afhankelijkheid van leveranciers in de zorgketen maakt dat één zwakke schakel grote impact op de keten kan veroorzaken. Kortom, een hack bij een leverancier bedreigt niet alleen data, maar ook de kwaliteit en veiligheid van zorg.

Voorbeelden van incidenten:

- De Engelse dienstverlener Synnovis, leverancier van pathologische diensten, werd in 2024 getroffen door een ransomware-incident. In juni 2025 werd bekend dat het overlijden van tenminste één patiënt gerelateerd is aan deze ransomware-aanval [15].
- Medisch laboratorium Clinical Diagnostics werd getroffen door een ransomwareaanval, waarbij gevoelige medische gegevens van 850.000 patiënten zijn buitgemaakt [16]. Voor alle organisaties die gebruik maakten van Clinical

Dreiging - Afpersing van leveranciers door middel van ransomware en datalekken, vervolg

Diagnostics-diensten, zorgde het incident voor extra operationele belasting en leidde het tot onrust en bezorgdheid bij veel patiënten van wie de gegevens via Bevolkingsonderzoek Nederland of andere zorgverleners bij het laboratorium waren verwerkt [16] [17].

- In Ierland is dit jaar Ocuco Limited, een softwarebedrijf voor oogzorg, het slachtoffer geworden van datadiefstal. Hierbij is ook medische patiëntinformatie gestolen [18].
- Het bedrijf Ascom, een leverancier van communicatie- en alarmsystemen voor de medische sector, is slachtoffer geworden van een ransomware-groep die het technische ticketsysteem kon hacken en claimde onder andere klantdata te hebben gestolen [19].

Hoe gaan aanvallers te werk?

Ransomware-actoren gebruiken bekende methoden zoals omschreven in het hoofdstuk over zorginstellingen en ransomware. Dit jaar werd bijvoorbeeld van meerdere leveranciers het ticketsysteem gecompromitteerd met een gestolen wachtwoord waardoor klantdata op straat kwam te liggen [20]. Er waren echter dit jaar ook voorbeelden van SaaS-leveranciers die werden aangevallen en die verder gaan dan de gebruikelijke methoden.

Cloud- en SaaS-partijen als sleutel tot klantdata

Deze doelwitten hebben een extra aanvalsoppervlak vanwege hun connectieve dienstverlening tussen leverancier en de vele afnemers. Aanvallers slagen er vaak in om met gestolen authenticatietokens toegang te krijgen tot deze strategische informatieknooppunten [21] [22]. Een voorbeeld in 2025 was de diefstal van authenticatietokens van een applicatie (Drift AI-chatagent) die integreert met de Salesforce SaaS-applicatie. Dit leidde tot datadiefstal uit Salesforce bij honderden klanten [23] [24].

Verwachting volgend jaar

Z-CERT verwacht dat ransomware-aanvallen bij leveranciers in 2026 opnieuw impact zullen hebben op de zorgsector. De aantallen die jaarlijks op datalekwebsites verschijnen laten al langere tijd een stijgende lijn zien, en er zijn geen signalen dat deze ontwikkeling afneemt. Doordat zorginstellingen sterk afhankelijk zijn van IT-dienstverleners, cloudleveranciers en SaaS-aanbieders, kan één ransomware-incident bij een leverancier meerdere organisaties tegelijk raken. Z-CERT acht het daarom waarschijnlijk dat ook in 2026 meerdere ransomware-incidenten bij leveranciers zullen plaatsvinden die gevolgen hebben voor de zorgsector.

Aanbevelingen

- Identificeer leveranciers of andere derde partijen die van belang zijn voor het uitoefenen van kerntaken.
- Ontwikkel continuïteitsprocedures om in geval van ransomware-incidenten bij deze partijen toch de kerntaken te kunnen blijven uitoefenen. Houd daarbij rekening

Dreiging - Afpersing van leveranciers door middel van ransomware en datalekken, vervolg

met de hersteltijd van ransomware-incidenten. Bijna tweederde van de leveranciers herstelt binnen een maand, bij de overige incidenten duurt het langer [25].

- Vraag aan leveranciers wat hun continuïteitsplannen en downtime procedures zijn.

Voor aanvullende en meer gedetailleerde aanbevelingen, zie hoofdstuk '**Aanbevelingen**'.

Enablers

- Data verspreiding en concentratie
- Tijdelijke medewerkers en hoog personeelsverloop
- Gebrek aan security awareness
- AI

Zie hoofdstuk 'Enablers' voor de uitwerking van de enablers.

Enablers >

Bibliografie

[4] **Sophos**, "The State of ransomware in Healthcare 2025," October 2025. [Online]. Available: https://news.sophos.com/en-us/2025/10/08/the-state-of-ransomware-in-healthcare-2025/

[10] **Z-CERT**, "Update datalek Clinical Diagnostics," 2025. [Online]. Available: https://z-cert.nl/actueel/nieuws/update-datalek-clinical-diagnostics

[11] **ENISA**, "ENISA Threat Landscape 2025," 2025. [Online]. Available: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025

[12] **Security**, **CIS**, "Initial Access Brokers How They're Changing," 2025. [Online]. Available: https://www.cisecurity.org/insights/blog/initial-access-brokers-how-theyre-changing-cybercrime

[13] **Trellix**, "Blurring the Lines: How Nation-States and Organized Cybercriminals Are Becoming Alike," 2025. [Online]. Available: https://www.trellix.com/blogs/research/blurring-the-lines-how-nation-states-and-cybercriminals-are-becoming-alike/

[14] **Sophos**, "THE STATE OFTHE STATE OF RANSOMWARE 2025," 24 Juni 2025. [Online]. Available: https://news.sophos.com/en-us/2025/06/24/the-state-of-ransomware-2025/

[15] **Health**, **Digital**, "Patient death linked to cyber attack on NHS pathology provider," 2025. [Online]. Available: https://www.digitalhealth.net/2025/06/patient-dies-as-a-result-of-cyber-attack-on-nhs-pathology-provider/

[16] **Clinical Diagnostics Nederland**, "Belangrijk bericht over gegevens van patiënten en zorgverleners," 2025. [Online]. Available: https://clinicaldiagnostics.nl/nl/belangrijk-bericht-over-gegevens-van-patienten-en-zorgverleners/

[17] **Bevolkingsonderzoek Nederland**, "Datalek veel groter dan eerder vermeld," 2025. [Online]. Available: https://www.bevolkingsonderzoeknederland.nl/nieuws/datalek-veel-groter-dan-eerder-vermeld/

[18] **Ocuco**, "Notice of Data Breach," 2025. [Online]. Available: https://www.ocuco.com/notice-of-data-breach/

[19] **Security.nl**, "HellCat-ransomwarebende slaat toe bij solution provider Ascom," 2025. [Online]. Available: https://www.security.nl/posting/880605/HellCat-ransomwarebende+slaat+toe+bij+solution+provider+Ascom

[20] **Ilascu**, **Ionut**, "HellCat hackers go on a worldwide Jira hacking spree," 20 Maart 2025. [Online]. Available: https://www.bleepingcomputer.com/news/security/hellcat-hackers-go-on-a-worldwide-jira-hacking-spree/

[21] **Security Brief**, "China-nexus hackers exploit cloud trust links in high-profile cyberespionage," 2025. [Online]. Available: https://securitybrief.asia/story/china-nexus-hackers-exploit-cloud-trust-links-in-high-profile-cyberespionage

[22] **The Hacker News**, "Commvault Confirms Hackers Exploited CVE-2025-3928 as Zero-Day in Azure Breach," 2025. [Online]. Available: https://thehackernews.com/2025/05/commvault-confirms-hackers-exploited.html

[23] **Dark Reading**, "Deja Vu: Salesforce Customers Hacked Again, Via Gainsight," 2025. [Online]. Available: https://www.darkreading.com/cyberattacks-data-breaches/salesforce-customers-hacked-gainsight

[24] **Mandiant**, **Google**, "Widespread Data Theft Targets Salesforce Instances via Salesloft Drift," 2025. [Online]. Available: https://cloud.google.com/blog/topics/threat-intelligence/data-theft-salesforce-instances-via-salesloft-drift

[25] **Sophos**, "The State of Ransomware 2025," 2025. [Online]. Available: https://www.sophos.com/en-us/whitepaper/state-of-ransomware

Dreiging
Malware gericht op gebruikers

Dreiging - Malware gericht op gebruikers

Inschatting dreiging: Medium

Tijd: Nu

Per kwartaal ontvangt Z-CERT enkele meldingen van malware-infecties. Dit jaar viel op dat bij meerdere organisaties tientallen werkstations besmet raakten met dezelfde malware, ondanks aanwezige antivirussoftware.

Dreigingsniveau: Medium

Hoewel de frequentie relatief hoog is, blijft het dreigingsniveau medium omdat de impact doorgaans beperkt is en de aanvaller niet vasthoudend opereert. In enkele gevallen kan een infectie echter dienen als opstap naar ernstigere incidenten, zoals ransomware-aanvallen of datalekken.

Actor: Cybercriminelen met technische ervaring

Malware wordt verspreid door diverse typen actoren, of door partijen die in hun opdracht handelen. Op basis van de bij Z-CERT gemelde malware-incidenten schat Z-CERT in dat deze voornamelijk het werk zijn van cybercriminelen.

Capaciteit

Deze actoren beschikken over capaciteiten voor het ontwikkelen en verspreiden van malware. Vaak wordt het aangeboden als dienst: 'malware-as-a-service'.

Motivatie

Financieel gewin.

Intentie

Op basis van de bij Z-CERT gemelde malware wordt deze als overwegend opportunistisch van aard ingeschat. Deze actoren infecteren systemen zodra zich een kans voordoet, ongeacht sector of organisatie. De verkregen toegang kan vervolgens worden doorverkocht aan andere cybercriminelen voor vervolgactiviteiten [9].

Hoe werd de dreiging zichtbaar?

Dit jaar zag Z-CERT vooral incidenten in de volgende categorieën: infostealers en malware die al aanwezig was op aangeschafte Android-apparaten.

Infostealers

Bij Z-CERT werden door 15 zorginstellingen infostealer-infecties gemeld. Daarnaast ontving Z-CERT van derden gegevens waaruit blijkt dat 70 zorginstellingen besmet zijn geweest, al is niet duidelijk wanneer deze infecties hebben plaatsgevonden. Een belangrijke bron van infectie was nepsoftware, vermomd als PDF-editors. Deze malware steelt wachtwoorden en andere credentials die vervolgens kunnen worden misbruikt voor verdere aanvallen.

Opvallend is dat het aantal geïnfecteerde systemen per organisatie aanzienlijk kan zijn. Bij één gehandicaptenorganisatie werden 70 computers geïnfecteerd, bij een andere 46 en bij een ziekenhuis 50 computers.

Dreiging - Malware gericht op gebruikers, vervolg

Waarom zo effectief?

De actor gebruikte een Google Ads-campagne om verkeer naar nepwebsites van PDF-editors te leiden. Deze sites waren overtuigend vormgegeven waardoor gebruikers de software zonder argwaan installeerden.

Hoewel er geen meldingen zijn geweest dat dit tot een ernstig incident heeft geleid, brengt het wel kosten met zich mee. Incident response met hulp van een externe partij is prijzig en ook voor interne IT-afdelingen kost het veel tijd om alle systemen te herstellen.

Plaats in het Cybersecuritybeeld

Infostealers vormen een belangrijke dreiging omdat gestolen credentials vaak een startpunt zijn voor vervolgaanvallen, zoals ransomware of datadiefstal [9]. In een onderzoek naar ransomware-incidenten bij zorginstellingen blijkt dat 'gestolen credentials' op de derde plek staat als oorzaak van een ransomware-aanval [4]. Ook worden credentials door cybercriminelen veel gedeeld op platforms als Telegram. Als slachtoffers wachtwoorden hergebruiken kunnen aanvallers de wachtwoorden die zij hier vinden, gebruiken om in te loggen op bijvoorbeeld VPN-oplossingen of clouddiensten.

BadBox 2.0 malware

Bij Z-CERT kwamen 28 meldingen binnen van Android-malware, bekend als BadBox 2.0. Deze malware kwam voor op schermen van fitnessapparatuur, digitale fotolijstjes of geïnfecteerde telefoons die soms op gastnetwerken in zorg-instellingen worden aangesloten.

De apparaten draaien een niet-gecertificeerde versie van Android en worden meestal geproduceerd door kleinere fabrikanten in Azië. Ze komen vaak al besmet uit de fabriek of raken geïnfecteerd via malafide apps tijdens installatie. Hoewel deze apparaten meestal niet in gevoelige netwerksegmenten staan, is er risico dat de toegang misbruikt wordt. Open bronnen melden dat geïnfecteerde apparaten kunnen dienen als opstapje voor criminele activiteiten, zoals advertentiefraude, het aanmaken van nepaccounts en het exfiltreren van gevoelige data [26].

Hoe gaan aanvallers te werk

Infostealers worden op verschillende manieren verspreid: via Google-advertentie-campagnes (malvertising), nepwebsites, e-mail en gecompromitteerde websites. Opvallend is de opkomst van de zogenaamde 'clickfix'-aanval, die Z-CERT in februari voor het eerst in de zorgsector heeft waargenomen. Het slachtoffer ziet een nep-foutmelding of verificatiebericht (fake captcha) en krijgt tips om het 'probleem op te lossen'. Het slachtoffer wordt verleid om een kwaadaardig script te kopiëren en uit te voeren.

Verwachting volgend jaar

Z-CERT verwacht dat de stroom malware-infecties in de zorgsector blijft aanhouden en mogelijk zal toenemen, vooral door distributiemethoden zoals malvertising via legitieme

Dreiging - Malware gericht op gebruikers, vervolg

advertentieplatformen en misleidende websites. Infostealers blijven een risico omdat gestolen credentials kunnen leiden tot vervolgincidenten zoals ransomware. Het ontbreken van applicatie-allowlisting is een risico omdat actoren toch met enige regelmaat de antivirus kunnen omzeilen. Daarnaast zal de stroom van geïnfecteerde Android-apparaten aanhouden. Deze apparaten kunnen een opstapje zijn voor allerlei criminele activiteiten.

Aanbevelingen

- Verbeter uw malware verdediging en vertrouw niet alleen op de anti-virussoftware.
- Gebruik alleen Android-apparaten waarvan de leverancier aantoonbaar heeft gecontroleerd dat er geen malafide code aanwezig is.

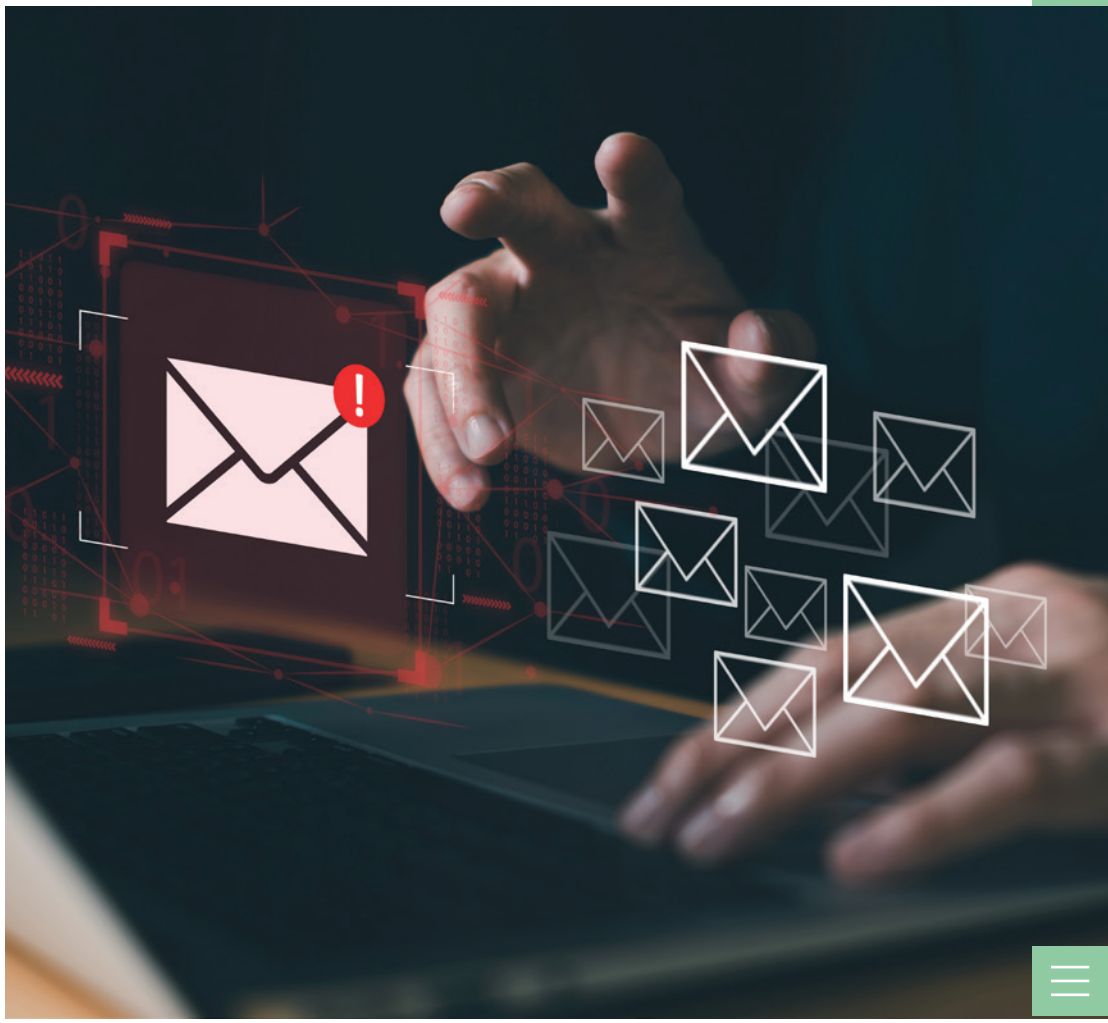
Voor aanvullende en meer gedetailleerde aanbevelingen, zie hoofdstuk '**Aanbevelingen**'.

Enablers

- Data verspreiding en concentratie
- Tijdelijke medewerkers en hoog personeelsverloop
- Gebrek aan security awareness
- AI

Zie hoofdstuk 'Enablers' voor de uitwerking van de enablers.

Enablers



Bibliografie

[4] **Sophos**, "The State of ransomware in Healthcare 2025," October 2025. [Online]. Available: https://news.sophos.com/en-us/2025/10/08/the-state-of-ransomware-in-healthcare-2025/

[9] **Microsoft**, "Microsoft Digital Defense Report 2025," p. 28, 2025.

[26] **S. T. I. a. R. Team**, "Satori Threat Intelligence Disruption: BADBOX 2.0 Targets Consumer Devices with Multiple Fraud Schemes," 5 Maart 2025. [Online]. Available: https://www.humansecurity.com/learn/blog/satori-threat-intelligence-disruption-badbox-2-0/

Dreiging
Phishing

Dreiging - Phishing

Inschatting dreiging: Medium

Tijd: Nu

Z-CERT ziet elk kwartaal enkele gevallen waarbij kwaadwillenden erin slagen om toegang te krijgen tot accounts.

Dreigingsniveau: Medium

Elke dag worden er veel phishingmails verstuurd. Het komt geregeld voor dat hierdoor accounts worden gecompromitteerd. De impact varieert. Vaak wordt vanuit de gekraakte mailbox weer phishing gestuurd naar interne en externe ontvangers. Het kan leiden tot datalekken en reputatieschade, maar het kan ook de bron zijn voor een ransomware-aanval.

Actor: cybercrimineel met of zonder technische ervaring

Phishingmail wordt verspreid door diverse typen actoren, of door partijen die in hun opdracht handelen. Op basis van de bij Z-CERT gemelde phishing-incidenten schat Z-CERT in dat deze voornamelijk het werk zijn van cybercriminelen met of zonder technische ervaring.

Capaciteit

De capaciteit van actoren wisselt. Duidelijk is wel dat aanvallers makkelijker geavanceerde aanvallen kunnen uitvoeren dankzij Phishing as a Service (PhaaS) platformen [27] [28]. Deze platformen worden ook wel phishing-kits genoemd, 'gereedschapskisten' om phishingmails te sturen zonder dat je er veel verstand van hebt. Om het de gebruiker makkelijk te maken is veel geautomatiseerd. Zo kan een kwaadwillende vanaf $100 per maand, mede dankzij AI, erg overtuigende phishingcampagnes uitvoeren [27].

Motivatie

Financieel gewin. Het merendeel van de aanvallen wordt gepleegd met het doel om op een of andere manier geld te verdienen. Maar ook spionage kan een doel zijn [29].

Intentie

Op basis van de bij Z-CERT gemelde phishingincidenten wordt deze phishing als overwegend opportunistisch ingeschat. Bij dit type phishing is het vaak de bedoeling om toegang tot accounts of inloggegevens te verkrijgen, waarna gehackte accounts opnieuw kunnen worden misbruikt, bijvoorbeeld om verdere phishingcampagnes te versturen. In enkele door Z-CERT onderzochte gevallen is de verkregen toegang daadwerkelijk gebruikt voor digitale financiële fraude. Toegang kan daarnaast worden ingezet voor andere vervolgactiviteiten, zoals datadiefstal of het faciliteren van ransomware-aanvallen [30].

Hoe werd de dreiging zichtbaar?

Z-CERT ziet maandelijks dat een account van een zorginstelling of leverancier misbruikt wordt om phishing mee te versturen. Rustigere maanden wisselen elkaar af met

Dreiging - Phishing, vervolg

piekmomenten. Dan zien wij als het ware een olievlek ontstaan, als de gehackte mailbox van de ene organisatie wordt gebruikt om in te breken op mailboxen bij andere organisaties. Z-CERT telde 29 gevallen waarbij phishing werd verzonden vanuit een gekraakte mailbox van een organisatie in de zorgketen.

De impact voor organisaties verschilt. Bij de ene wordt misbruik van accounts direct gedetecteerd en gemitigeerd. Andere organisaties moeten door derden gewezen worden op een incident om het te kunnen bestrijden.

Voor bij Z-CERT aangesloten organisaties hadden geslaagde phishingaanvallen vooral de volgende nadelige gevolgen: malafide mailregels, datalekken, reputatieschade (helemaal als een datalek wordt opgepikt door de media), kosten voor forensisch onderzoek en het versturen van phishing vanuit de gekraakte mailbox (intern en/of naar externe partners). Respondenten van de survey gaven verder aan dat phishingmails door gebruik van AI beter en effectiever worden.

Voorbeelden van incidenten in Nederland

- Een arts kreeg een mail met QR-code van het gehackt account van diens accountant. De link achter de QR-code leidde naar een phishingpagina waarop de arts met multifactorauthenticatie (MFA) inlogde. Het IP-adres waarmee kwaadwillenden daarna het account benaderden, werd door de leverancier herkend als malafide. De aanval werd tegengehouden.
- Van een derde partij werd een mail ontvangen die de voortzetting leek te zijn van een lopende conversatie. Er zat echter een phishinglink in. De derde partij waarschuwde ontvangers dezelfde dag. Maar men realiseerde zich pas dat er een account was gehackt toen er grote hoeveelheden mail (phishing) mee werden verstuurd. De kwaadwillende had ondertussen ook een nieuwe MFA-methode toe kunnen voegen.
- Vanuit een account van een zorginstelling waarmee wordt samengewerkt, wordt een OneNote bestand gedeeld op SharePoint, met een standaard uitnodiging van Microsoft (voor zover dus volledig legitiem). Toen de ontvanger klikte om het bestand te openen, werd die doorgestuurd naar een website die erg leek op een standaard login-pagina van Microsoft. Kort nadat de gebruiker 'inlogde', probeerde een kwaadwillende vanaf een IP-adres uit de VS in te loggen op het account. Dit werd voorkomen doordat geofencing was ingesteld als onderdeel van het beleid voor voorwaardelijke toegang.

Hoe gaan aanvallers te werk?

Bij de meeste phishing die bij Z-CERT wordt gemeld is er sprake van Adversary in the Middle (AiTM) phishing. Hierbij lift de kwaadwillende mee op het gehele authenticatieproces, inclusief MFA en verkrijgt hij credentials en toegang. Standaard MFA biedt dus geen bescherming meer tegen de meeste phishingaanvallen. Dat betekent niet dat het nutteloos is geworden. Het beschermt wel heel goed tegen aanvallen waarbij kwaadwillenden een wachtwoord proberen te raden of een gestolen wachtwoord gebruiken [31]. Om bestand te zijn tegen AiTM aanvallen implementeren steeds meer

Dreiging - Phishing, vervolg

organisaties bijvoorbeeld phishingresistente MFA in combinatie met aanvullende toegangseisen. Verder ziet Z-CERT dat kwaadwillenden hun technieken constant wijzigen om detectie te voorkomen. Phishinglinks worden vaak aangeboden via een legitieme of legitiem ogende oplossing om bestanden te delen (zoals SharePoint, DocuSign, etc.). Verder valt op dat kwaadwillenden verschillende technische trucs en social engineering combineren om hun aanval te laten slagen en dus detectie te voorkomen [32]. Zo worden phishinglinks bijvoorbeeld verstopt in QR-codes [33], plaatjes of een webpagina als bijlage [34, p. 8].

Verwachting volgend jaar

Z-CERT verwacht dat de inzet van AI zal toenemen. Ook zal AiTM veel gebruikt blijven worden terwijl de route naar AiTM-phishingpagina's zal verschillen. Veel organisaties zijn nog onvoldoende beschermd tegen dit type phishing. Z-CERT verwacht daarom dat het aantal malafide mails dat verstuurd wordt vanuit vertrouwde partijen vergelijkbaar zal zijn of mogelijk zal toenemen.

Aandachtspunten voor komend jaar

- Een trend uit 2024 die zal doorzetten is dat kwaadwillenden het social engineering aspect van hun aanval proberen uit te voeren buiten het zicht van security-monitoring [35] [36]. Dan valt te denken aan telefonische phishing (vishing) of phishing via berichten op mobiele apparaten of social media. Soms start zo'n aanval wel vanuit een gemonitorde mailbox, maar verplaatst de aanvaller de conversatie naar een ander medium. Een aantal respondenten gaf in de survey al aan dat zij phishing via een telefoongesprek (vishing) en phishing via SMS (smishing) hadden waargenomen.
- Microsoft ziet een toename van een nieuwe techniek genaamd 'device code phishing' [31]. Device code authenticatie biedt bijvoorbeeld de mogelijkheid om in te loggen op een apparaat zonder input mogelijkheden (toetsenbord of muis). Aanvallen richten zich vaak op Microsoft Azure omgevingen [37] [38] [39].

Aanbevelingen

- Breng de basisbeveiliging tegen phishing op orde.
- Zorg voor effectieve maatregelen tegen AiTM-phishing.
- Geef in uw risicoanalyse analyse aandacht aan nieuwe phishingtechnieken zoals "device code phishing".

Voor aanvullende en meer gedetailleerde aanbevelingen, zie hoofdstuk '**Aanbevelingen**'.

Enablers

- Data verspreiding en concentratie
- Tijdelijke medewerkers en hoog personeelsverloop
- Gebrek aan security awareness
- AI
- Geopolitieke situatie

Zie hoofdstuk 'Enablers' voor de uitwerking van de enablers.

Enablers >

> < <

Bibliografie

[27] **Sekoia**, "Global analysis of Adversary-in-the-Middle phishing threats," 11 June 2025. [Online]. Available: https://blog.sekoia.io/global-analysis-of-adversary-in-the-middle-phishing-threats/

[28] **ENISA**, "ENISA THREAT LANDSCAPE 2025," 2025. [Online]. Available: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025

[29] **NCTV**, "Cybersecuritybeeld Nederland 2025," 2025. [Online]. Available: https://www.nctv.nl/site/binaries/site-content/collections/documents/2025/11/26/cybersecuritybeeld-nederland-2025/cybersecuritybeeld-nederland-2025.pdf

[30] **Kela**, "Unveiling Black Basta's Use of PhaaS Platforms," 2025. [Online]. Available: https://www.kelacyber.com/resources/research/unveiling-black-bastas-use-of-phaas-platforms-report/

[31] **Microsoft**, "Microsoft Digital Defense Report 2025," 2025. [Online]. Available: https://www.microsoft.com/en-us/corporate-responsibility/cybersecurity/microsoft-digital-defense-report-2025/

[32] **Push Security**, "Phishing detection is broken: Why most attacks feel like a zero day," 25 April 2025. [Online]. Available: https://www.bleepingcomputer.com/news/security/phishing-detection-is-broken-why-most-attacks-feel-like-a-zero-day/

[33] **Barracuda**, "Threat Spotlight: Split and nested QR codes fuel new generation of 'quishing' attacks," 20 August 2025. [Online]. Available: https://blog.barracuda.com/2025/08/20/threat-spotlight-split-nested-qr-codes-quishing-attacks

[34] **KnowBe4**, "Phishing Threat Trends Report," 2025. [Online]. Available: https://www.knowbe4.com/hubfs/Phishing-Threat-Trends-2025_Report.pdf

[35] **CrowdStrike**, "The CrowdStrike 2025 Global Threat Report," 2025. [Online]. Available: https://www.crowdstrike.com/en-us/global-threat-report/

[36] **Unit 42**, "2025 Unit 42 Global Incident Response Report: Social Engineering Edition," 30 juli 2025. [Online]. Available: https://unit42.paloaltonetworks.com/2025-unit-42-global-incident-response-report-social-engineering-edition/

[37] **Huntress**, "Oh, Auth 2.0! Device Code Phishing in Google Cloud and Azure," 6 Februari 2025. [Online]. Available: https://www.huntress.com/blog/oh-auth-2-0-device-code-phishing-in-google-cloud-and-azure

[38] **Microsoft**, "Storm-2372 conducts device code phishing campaign," 13 Februari 2025. [Online]. Available: https://www.microsoft.com/en-us/security/blog/2025/02/13/storm-2372-conducts-device-code-phishing-campaign/

[39] **Obsidian**, "Securing OAuth for Microsoft Environments," 5 November 2025. [Online]. Available: https://www.obsidiansecurity.com/blog/securing-oauth-for-microsoft-environments

Dreiging
DDoS op zorginstellingen

Dreiging - DDoS op zorginstellingen

Inschatting dreiging: Medium

Tijd: 0-6 maanden

Dreigingsniveau: Medium

Het dreigingsniveau van DDoS-aanvallen op zorginstellingen wordt als medium ingeschat. In Nederland deden zich weinig DDoS-incidenten voor en de verstoringen die plaatsvonden waren van korte duur. Vergeleken met 2024 behoort de zorgsector niet langer tot de tien meest aangevallen sectoren [40] [41] [42]. Wereldwijd ziet Cloudflare wel een toename van het aantal DDoS-aanvallen (40%) en een stijging in het volume van grote aanvallen [40] [41] [42]. Volgens ENISA kwamen Europese zorginstellingen in 2025 wel DDoS-aanvallen tegen, maar zonder grote verstoringen [43]. In de rapportages van Microsoft krijgt de DDoS-dreiging een minder prominente rol dan in 2024, al blijven verstoringsaanvallen op infrastructuren een continu cyberrisico [9].

Actor: Hacktivist

Op dit moment komt de DDoS-dreiging vooral uit de hacktivistische hoek.

Capaciteit

Net als vorig jaar ziet Z-CERT op Telegram-kanalen dat online groepen steeds meer samenwerken bij het uitvoeren van DDoS-aanvallen. Groepen roepen elkaar op om gezamenlijk doelwitten aan te vallen. Er worden screenshots gedeeld met bewijs dat een doelwit niet meer bereikbaar is. Doelwit is veelal de website van een organisatie. Door samen te werken lukt het groepen om websites vaak voor enkele uren tot dagen onbereikbaar te maken. Tooling voor het meedoen aan DDoS-aanvallen wordt steeds vaker beschikbaar gesteld aan een breder publiek [44].

Motivatie

Ideologisch gedreven.

Intentie

Z-CERT constateert uit monitoring van Telegram-kanalen dat DDoS-aanvallen sterk gekoppeld zijn aan geopolitieke conflicten. Een DDoS-aanval is vaak een reactie op het handelen van een land tijdens het conflict of een publieke steun-betuiging. De websites van ziekenhuizen en gezondheidsautoriteiten waren veelal het doelwit.

Dreiging - DDoS op zorginstellingen, vervolg

Tabel 1: Geopolitiek gedreven DDoS-aanvallen op de zorg (2025).

Geopolitieke intentie	Landen waarin zorginstellingen zijn aangevallen	Groepen
Pro-Russisch	Oekraïne en NAVO-landen als België, Frankrijk, Duitsland	Keymous+ NoName057(16)
Pro-Palestijns Pro-Koerdisch Pro-Islamitisch	Israël en landen die Israël steunen	Dark Storm Team, Hezi Rash, Cyber Islamic resistance

Hoe werd de dreiging zichtbaar?

Onderstaande statistieken laten zien hoeveel DDoS-aanvallen op de zorgsector aan Z-CERT zijn gemeld of op doelwitlijsten stonden op Telegram:

Tabel 2a + 2b: Aantal zorginstellingen in 2025 waarvoor DDoS-aanvallen zijn gemeld.

Q1		Q2	
Totaal Nederland	6	Totaal Nederland	5
Totaal Europa (Niet NL)	18	Totaal Europa (Niet NL)	22
Totaal buiten Europa	9	Totaal buiten Europa	60
Totaal	33	Totaal	87

Tabel 2b:

Q3		Q4	
Totaal Nederland	0	Totaal Nederland	0
Totaal Europa (Niet NL)	25	Totaal Europa (Niet NL)	7
Totaal buiten Europa	24	Totaal buiten Europa	12
Totaal	49	Totaal	19

Casussen uit de zorg

Van de 110 respondenten gaven 4 zorginstellingen aan dat er DDoS-incidenten waren op de eigen infrastructuur. Hieronder is enkel beschreven wat aan Z-CERT is gemeld:

- Bij een regionale ambulancevoorziening waren er 5 DDoS-incidenten. De groep NoName057(16) overspoelde de instelling elke keer gedurende enkele uren met HTTP (applicatielaag) en SYN-pakketten (netwerklaag). De ambulancevoorziening gaf aan dat dit erg stressvol was en resulteerde in een directe migratie naar een leverancier voor DDoS-bescherming.
- Bij een gehandicaptenzorginstelling waren er 3 DDoS-incidenten van elk korter dan een uur. Dit resulteerde in het doorvoeren van mitigerende maatregelen.
- Een academisch ziekenhuis heeft eenmalig 3 dagen last gehad van een DDoS-aanval, waarbij de DDoS-filter van de internetserviceprovider de aanval grotendeels heeft afgevangen.

Dreiging - DDoS op zorginstellingen, vervolg

- Een jeugdzorginstelling gaf aan dat er 2 DDoS-incidenten waren die een halve dag tot een dag hebben geduurd. Er is een vermoeden uitgesproken dat deze aanvallen door een oud-medewerker zijn uitgevoerd. De zorginstelling heeft besloten een back-uplijn in te schakelen voor het internetverkeer.

Hoe gaan aanvallers te werk?

De anatomie van de meeste DDoS-aanvallen bestaat nog steeds uit het overspoelen van een doelwit met pakketten op de netwerklaag (SYN Flood) en pakketten op de applicatielaag (HTTP Flood) [40] [41] [42].

Geavanceerdere technieken worden beschreven in het hoofdstuk over DDoS op leveranciers. De bekendste tooling voor het uitvoeren van DDoS-aanvallen is DDoSia. Ontwikkeld door de pro-Russische hacktivistengroep NoName057(16). DDoSia functioneert als een DDoS-for-hire botnet, waarbij vrijwilligers via sociale mediakanalen zoals Telegram worden gerekruteerd om de tool op hun eigen computer te installeren en zo mee te doen met DDoS-aanvallen [45].

Verwachting komend jaar

Verstoring door DDoS-aanvallen is een dreiging die continu speelt. Ondanks geopolitieke ontwikkelingen is de verwachting dat de Nederlandse zorg in 2026 niet meer of minder het doelwit wordt van DDoS-aanvallen.

Aanbevelingen

- Breng in kaart welke online diensten/systemen binnen eigen beheer vallen. Neem vervolgens technische en organisatorische maatregelen tegen verschillende vormen van (D)DoS-aanvallen.
- Zet een response- en communicatiestrategie op.

Voor aanvullende en meer gedetailleerde aanbevelingen, zie hoofdstuk '**Aanbevelingen**'.

Enablers:

- Geopolitieke situatie

Zie hoofdstuk 'Enablers' voor de uitwerking van de enablers.

Enablers >

< >

Bibliografie

[9] **Microsoft**, "Microsoft Digital Defense Report 2025," p. 28, 2025

[40] **Radar**, [Online]. Available: https://radar.cloudflare.com/reports/ddos-2025-q1

[41] **Radar**, [Online]. Available: https://radar.cloudflare.com/reports/ddos-2025-q2

[42] **Radar**, [Online]. Available: https://radar.cloudflare.com/reports/ddos-2025-q3

[43] **Enisa**, [Online]. Available: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025

[44] **Sekoia**, [Online]. Available: https://www.sekoia.io/en/glossary/ddosia-project/

[45] **Recorded Future**, "Anatomy of DDoSia: NoName057(16)'s DDoS Infrastructure and Targeting," 2025. [Online]. Available: https://therecord.media/china-linked-hackers-target-european-health-orgs

Dreiging DDoS op leveranciers

Dreiging - DDoS op leveranciers

Inschatting dreiging: Medium

Tijd: 0-6 maanden

Dreigingsniveau: Medium

De dreiging van DDoS-aanvallen op leveranciers is 'medium'. Verstoring door DDoS-aanvallen is een dreiging die continu speelt. In 2025 hebben DDoS-aanvallen op enkele leveranciers voor verstoring gezorgd bij meerdere Nederlandse zorginstellingen.

Zoals in het hoofdstuk over DDoS op zorginstellingen is gemeld, ziet Cloudflare wereldwijd een toename in de hoeveelheid DDoS-aanvallen. Zowel wereldwijd als in Europa staan IT-dienstverlening en internetserviceproviders beide in de top-5 van meest aangevallen sectoren [40] [41] [42] [43]. Doordat de Nederlandse zorg steeds afhankelijker wordt van clouddiensten en SaaS-applicaties, neemt hiermee het risico op verstoring door een DDoS-incident bij een leverancier toe.

Actor: Hacktivist

Op dit moment komt de de DDoS-dreiging vooral uit de hacktivistische hoek.

Hoe werd de dreiging zichtbaar?

Van de 110 respondenten gaven 11 zorginstellingen aan dat er verstoringen waren door DDoS-incidenten bij leveranciers. Hieronder zijn enkele casussen beschreven van wat aan Z-CERT is gemeld.

Voorbeelden van incidenten

- De digitale identiteitsdienst DigiD van de Nederlandse overheid heeft in 2025 last gehad van meerdere DDoS-aanvallen [46]. Dit heeft impact op zorginstellingen omdat DigiD veel wordt gebruikt, onder andere voor het inloggen van patiënten op hun zorgportaal [47].
- Een internetserviceprovider die diensten levert aan een ziekenhuis werd aangevallen. Hierdoor had een ziekenhuis gedurende twee dagen geen toegang tot hun afsprakenterminals en moest men overschakelen op handmatig werken. Ook konden Jeugdgezondheidszorg medewerkers die op schoollocaties hun werk doen, niet meer digitaal werken door de DDoS-aanval.
- Een aantal zorginstellingen meldde onderbrekingen van websites van leveranciers. Zo was een leverancier die levert aan een gehandicaptenzorginstelling meerdere keren niet bereikbaar. En kon een ziekenhuis een aantal keer niet bij hun SaaS-oplossing. Het is niet altijd duidelijk of het om een DDoS-aanval ging.

Dreiging - DDoS op leveranciers, vervolg

Hoe gaan aanvallers te werk?

Veel gebruikte technieken staan beschreven in het vorige hoofdstuk. In aanvulling hierop blijkt uit consultatie van een aantal ISP's die leveren aan de zorg dat er twee technieken in opkomst zijn:

- DDoS carpet bombing richt zich op een heel blok systemen tegelijk. Per systeem valt de belasting mee, maar dit overbelast de achterliggende netwerkapparatuur, zodat diensten slecht bereikbaar zijn. De grootste gemeten DDoS-aanval tot nu toe (29,7 Tbps) was een voorbeeld van zo'n carpet bombing aanval [42].
- DNS Water Torture richt zich op DNS servers die verantwoordelijk zijn voor een domeinnaam van een organisatie. Door deze servers via heel veel verschillende routes te overbelasten met aanvragen kunnen zij hun normale functie niet meer goed uitvoeren, waardoor websites voor gebruikers slecht of helemaal niet bereikbaar zijn.

Aandachtspunten voor komend jaar

Z-CERT verwacht dat aanvallers zich blijven ontwikkelen. Wanneer eenvoudige DDoS-aanvallen die bestaan uit het versturen naar heel veel SYN- en HTTP-pakketten niet meer het gewenste resultaat bereiken, verwacht Z-CERT dat aanvallers meer overgaan op nieuwere technieken zoals DDoS carpet bombing en DNS Water Torture-aanvallen.

Aanbevelingen

- Breng in kaart voor welke online diensten leveranciers verantwoordelijk zijn en maak afspraken met deze leveranciers over bescherming tegen DDoS-aanvallen, inclusief nieuwe aanvalstypen zoals beschreven in dit Cybersecuritybeeld.

Voor aanvullende en meer gedetailleerde aanbevelingen, zie hoofdstuk '**Aanbevelingen**'.

Enablers

- Dataverspreiding en concentratie
- Geopolitieke situatie

Zie hoofdstuk 'Enablers' voor de uitwerking van de enablers.

Enablers >

< >

Bibliografie

[40] **Radar**, [Online]. Available: https://radar.cloudflare.com/reports/ddos-2025-q1

[41] **Radar**, [Online]. Available: https://radar.cloudflare.com/reports/ddos-2025-q2

[42] **Radar**, [Online]. Available: https://radar.cloudflare.com/reports/ddos-2025-q3

[43] **Enisa**, [Online]. Available: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025

[46] **NOS**, [Online]. Available: https://nos.nl/artikel/2560424-digid-opnieuw-tijdelijk-onbereikbaar-geweest-door-ddos-aanval

[47] **Nictiz**, [Online]. Available: https://nictiz.nl/nieuws/digid-inlogs-patient-digitale-toegang-zorg

Dreiging
Statelijke digitale operaties

Dreiging - Statelijke digitale operaties

Inschatting dreiging: Situatie-afhankelijk

Tijd: >1 jaar
Bij Z-CERT zijn geen incidenten bekend van digitale operaties door statelijke actoren tegen de Nederlandse zorgsector.

Dreigingsniveau: situatie-afhankelijk
Z-CERT schat het dreigingsniveau voor cyberspionage door statelijke actoren voor de verschillende typen zorgorganisaties anders in. Voor statelijke cyberactoren is de Nederlandse zorgsector vooral relevant vanwege het stelen van wetenschappelijke onderzoek, intellectuele eigendommen en grote datasets aan medische- en persoonsgegevens. Voor zorgorganisaties die beschikken over dergelijke gegevens, schat Z-CERT de dreiging van cyberspionage door statelijke actoren in als 'hoog'. Voor andere type zorg-organisaties schat Z-CERT de dreiging van cyberspionage door statelijke actoren in als 'laag'. Z-CERT verwacht dat cyberspionage in 2026 actueel zal blijven.

Actor: statelijke actor

Capaciteit
De hoge dreiging wordt ook veroorzaakt doordat statelijke aanvallers goed georganiseerd zijn en over veel technische vaardigheden beschikken om hun opdrachten heimelijk uit te voeren.

Motivatie
Statelijke actoren ontvangen van hun nationale overheid een mandaat en de benodigde capaciteiten om diverse type digitale operaties uit te voeren, zoals spionage, sabotage en beïnvloeding. De motivatie is divers, maar over het algemeen wordt deze gedreven door politieke, economische en/of militaire belangen van een land.

Intentie
Statelijke actoren hebben in de basis de intentie om voor langere tijd ergens onopvallend mee te kijken met de informatiestromen van hun doelwit. Daarna stelen ze belangrijke informatie en maken ze hiervan een rapport. Dat gebruiken ze voor nieuwe spionageacties of om hun politieke opdrachtgevers te informeren. De zorgsector wordt daarbij niet overgeslagen als het past bij de motivatie van de statelijke actor.

Hoe werd de dreiging zichtbaar?
De dreiging van statelijke actoren laat zich moeilijk vangen in cijfers. Het Europese instituut ENISA doet een goede poging. Uit hun onderzoek blijkt dat Russische, Chinese en Noord-Koreaanse actoren het het meest voorzien hebben op Europese landen. Van alle NIS2-sectoren staat de zorgsector op een 5e plaats [48].

Zo zijn door 'IT'ers' uit Noord-Korea vacatures opgevuld in de IT-dienstverlening van gezondheidsorganisaties met als doel geld te verdienen voor het regime [50].

Dreiging - Statelijke digitale operaties, vervolg

Daarnaast bestaat het risico dat deze Noord-Koreaanse 'IT'ers' ook medische- en persoonsgegevens stelen of aan de haal gaan met intellectuele eigendommen [49] [50] [51].

Hoe gaan aanvallers te werk?

De initiële toegang kan zowel opportunistisch als doelgericht zijn en dient vooral om binnen te komen in een netwerk. Vervolgens ligt de nadruk op het uitbreiden van die toegang en het verkennen van systemen zonder op te vallen. Hierbij maken zij vaak gebruik van legitieme beheertools en verzamelen zij informatie gedoseerd, waardoor hun activiteiten moeilijk te detecteren zijn [48].

Hoewel bij Z-CERT geen spionage-incidenten door statelijke actoren in de Nederlandse zorgsector zijn gemeld, zijn er internationaal in open bronnen wel voorbeelden bekend van dergelijke activiteiten gericht op de zorgsector. De volgende casussen illustreren hoe statelijke actoren in de praktijk te werk kunnen gaan.

Casus 1: Rusissche spionage actor

In mei 2025 publiceerde Microsoft, in samenwerking met de Nederlandse inlichtingendiensten, een rapport over een nieuwe Russische spionage actor. Volgens Microsoft zou deze actor, Void Blizzard genaamd, ook gezondheidsorganisaties hebben bespioneerd. De werkwijze van deze actor was minder geraffineerd dan die van andere bekende Russische groepen, desondanks waren ze wel succesvol [52].
Op grote schaal voerden ze 'password spray-aanvallen' uit of maakten ze gebruik van op het dark web gekochte credentials om bij een doelwit binnen te komen. Op deze manieren konden ze toegang krijgen tot Exchange en SharePoint Online omgevingen van hun slachtoffers. Ook maakten ze gebruik van AitM-spearphishingtechnieken en namaakdomeinnamen die sterk lijken op de echte om aan credentials te komen. Eenmaal binnen konden ze onder andere meeliften op cloud-API's van Microsoft-platformen om meer informatie te verkrijgen over de digitale omgeving van het slachtoffer. Via gecompromitteerde accounts wisten de aanvallers met scripts grote hoeveelheden data, met name e-mails en bestanden, te stelen [52].

Casus twee: Silver Fox

Silver Fox, een vermoedelijk door China gesteunde APT-groep, heeft zich in 2025 onder andere gericht op gezondheidsorganisaties en publieke instellingen. Ze verspreiden gemanipuleerde medische software waarin malware is verstopt, zoals een aangepaste Philips DICOM-viewer. Slachtoffers worden verleid deze te openen via phishing en via SEO-poisoning, waarbij zij via zoekresultaten op kwaadaardige downloadsites terechtkomen. Bij deze aanpak maken criminelen gebruik van een combinatie van social engineering, legitiem ogende software en cloudinfrastructuur om langdurige controle en data-diefstal mogelijk te maken [53] [54] [55].

Dreiging - Statelijke digitale operaties, vervolg

Verwachting volgend jaar

Z-CERT verwacht niet dat er in 2026 een incident wordt gemeld dat het directe gevolg is van een digitale aanval door een statelijke actor gericht tegen de Nederlandse zorgsector. Het is namelijk heel lastig om vast te stellen dat een land achter een aanval zit. En áls dat al lukt, wordt die informatie meestal niet openbaar gemaakt.

Aandachtspunten voor volgend jaar:

- Geopolitieke ontwikkelingen kunnen het dreigingsniveau verhogen wanneer bijvoorbeeld Nederland direct betrokken zou raken in een militair conflict. Het is dan mogelijk dat digitale operaties minder voorzichtig en omzichtig gaan worden, en dat de operaties meer gericht zullen zijn op digitale sabotage en beïnvloeding. Diverse landen en initiatieven bereiden zich voor op zo'n scenario waarbij ook de zorgsector een doelwit gaat zijn [56] [57] [58]. In Nederland worden ook voorbereidingen getroffen op een mogelijk oorlogsscenario [59] [60] [61].
- Tot slot dient de Nederlandse gezondheidssector ook rekening te houden met statelijke digitale operaties tegen andere vitale sectoren, waarbij een keteneffect kan ontstaan richting de fysieke en/of digitale processen in de zorg [62].

Aanbevelingen

- Volg de aanbevelingen tegen ransomware-groepen en andere cyberdreigingen zoals gedefinieerd in dit Cybersecuritybeeld. Deze maatregelen kunnen ook effectief zijn tegen digitale spionage.
- Gebruik maken van goede detectie en/of SOC-partijen met veel kennis over statelijke actoren.
- Maak gebruik van cyber threat intelligence en threat hunting om proactief kennis te nemen van actuele digitale dreigingen en deze op te sporen.

Voor aanvullende en meer gedetailleerde aanbevelingen, zie hoofdstuk '**Aanbevelingen**'.

Enablers

- Data verspreiding en concentratie
- Tijdelijke medewerkers en hoog personeelsverloop
- Gebrek aan security awareness
- Geopolitieke situatie
- AI

Zie hoofdstuk 'Enablers' voor de uitwerking van de enablers.

Enablers

Bibliografie

[48] **ENISA**, "ENISA Threat Landschape 2025," 2025. [Online]. Available: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025

[49] **Duitse Binnenlandse Inlichtingendienst**, "Private Sector Security Advisory | 02/2024 | 1 October 2024 | Subject: North Korean IT Workers," 2025. [Online]. Available: https://www.verfassungsschutz.de/SharedDocs/kurzmeldungen/EN/2024/2024-10-01-private-sector-security-advisory.html

[50] **OKTA**, "North Korea's IT Workers expand beyond US big tech," 2025. [Online]. Available: https://www.okta.com/newsroom/articles/north-korea-s-it-workers-expand-beyond-us-big-tech/

[51] **AnyRun**, "Smile, You're on Camera: A Live Stream from Inside Lazarus Group's IT Workers Scheme," 2025. [Online]. Available: https://any.run/cybersecurity-blog/lazarus-group-it-workers-investigation/

[52] **Microsoft**, "New Russia-affiliated actor Void Blizzard targets critical sectors for espionage," 2025. [Online]. Available: https://www.microsoft.com/en-us/security/blog/2025/05/27/new-russia-affiliated-actor-void-blizzard-targets-critical-sectors-for-espionage/

[53] **Forescout**, "Healthcare Malware Hunt, Part 1: Silver Fox APT Targets Philips DICOM Viewers," 2025. [Online]. Available: https://www.forescout.com/blog/healthcare-malware-hunt-part-1-silver-fox-apt-targets-philips-dicom-viewers/

[54] **Picus Security**, "Silver Fox APT Targets Public Sector via Trojanized Medical Software," 2025. [Online]. Available: https://www.picussecurity.com/resource/blog/silver-fox-apt-targets-public-sector-via-trojanized-medical-software

[55] **Trustwave**, "Inside Silver Fox's Den: Trustwave SpiderLabs Unmasks a Global Threat Actor," 2025. [Online]. Available: https://www.trustwave.com/en-us/resources/blogs/trustwave-blog/inside-silver-foxs-den-trustwave-spiderlabs-unmasks-a-global-threat-actor/

[56] **Harvard**, "Enhancing the Resilience of Europe's Civilian Health Systems as Conflict with Russia Escalates," 2025. [Online]. Available: https://globalhealth.harvard.edu/news-enhance-resilience-of-health-systems-in-europe/

[57] **RUSI**, "European Medical Provision in Times of War," 2025. [Online]. Available: https://www.rusi.org/explore-our-research/publications/commentary/european-medical-provision-times-war

[58] **BNR Nieuws**, "Na Frankrijk verhoogt ook Duitsland medische capaciteit voor mogelijke oorlog Rusland," 2025. [Online]. Available: https://www.bnr.nl/nieuws/internationaal/10583412/na-frankrijk-verhoogt-ook-duitsland-medische-capaciteit-voor-mogelijke-oorlog-rusland

[59] **Acute Zorg Regio**, "Gewapend conflict - zorgketen paraat?," 2025. [Online]. Available: https://www.acutezorgeuregio.nl/nieuws/gewapend-conflict-zorgketen-paraat/

[60] **Defensie**, "Generaal Eichelsheim: "Opvang Nederlandse oorlogsgewonden moet fors omhoog"," 2025. [Online]. Available: https://www.defensie.nl/actueel/nieuws/2024/11/15/generaal-eichelsheim-opvang-nederlandse-oorlogsgewonden-moet-fors-omhoog

[61] **BNR Nieuws**, "Nederlandse krijgsmacht en ziekenhuizen bereiden zich voor op oorlogs-scenario," 2025. [Online]. Available: https://www.bnr.nl/nieuws/internationaal/10586143/nederlandse-krijgsmacht-en-ziekenhuizen-bereiden-zich-voor-op-oorlogsscenario

[62] **AHA Verenigde Staten**, "Advisory warns of activity by Chinese state-sponsored cyber actors," 2025. [Online]. Available: https://www.aha.org/news/headline/2025-09-03-advisory-warns-activity-chinese-state-sponsored-cyber-actors

Dreiging
Digitale financiële fraude in de zorg

Dreiging - Digitale financiële fraude in de zorg

Inschatting dreiging: Medium

Tijd: Nu

Bij Z-CERT zijn in 2025 tientallen incidenten van digitale financiële fraude gemeld. De meeste van deze incidenten zijn gestrand als pogingen zonder financiële gevolgen of reputatieschade.

Dreigingsniveau: Medium

Het dreigingsniveau van digitale fraude in de zorg is 'medium'. De frequentie van pogingen is hoog en komt voor bij diverse type en grootte van zorg-organisaties. De impact is overwegend laag, want veel zorgorganisaties die Z-CERT gesproken heeft, hebben vooral procesmatig goede voorzorgsmaatregelen genomen.

Actor: cybercriminelen met beperkte technische ervaring

De bij Z-CERT gemelde aanvallen kunnen zonder veel technische kennis worden uitgevoerd, omdat digitale financiële fraude vooral op social engineering berust. Wanneer vooraf een mailbox wordt gecompromitteerd, gebeurt dat mogelijk in samenwerking met cybercriminelen die wél technisch vaardig zijn.

Capaciteit

Voor de bij Z-CERT waargenomen gevallen van digitale financiële fraude zijn slechts beperkte technische capaciteiten nodig. De meeste aanvallen worden uitgevoerd met eenvoudig toegankelijke middelen, zoals WhatsApp, Gmail of andere publieke communicatieplatformen. Wanneer phishing wordt ingezet, kunnen aanvallers gebruikmaken van kant-en-klare phishingkits of 'phishing-as-a-service'-diensten, die de technische drempel verder verlagen.

Motivatie

Financieel gewin.

Intentie

De plegers van digitale fraude zijn overwegend opportunistisch omdat ze snel willen toeslaan. De meer ervaren fraudeurs weten dat veel organisaties al maatregelen hebben genomen, voornamelijk procesmatig, tegen digitale fraude. Daarom bedenken ze steeds nieuwe manieren om toch hun doelwit succesvol te verleiden. Daarbij worden zij geholpen door steeds betere generatieve AI-technologie om social engineering succesvol te laten zijn.

Hoe werd de dreiging zichtbaar?

Z-CERT heeft in het afgelopen jaar een dertigtal meldingen ontvangen van (pogingen tot) digitale fraude bij zorgorganisaties. Dit komt overeen met de resultaten van de jaarlijkse enquête, waar 29 van de 110 inzendingen aangaven dit jaar één of meerdere incidenten te hebben gehad met digitale fraude. Bij zeven deelnemers heeft dit geleid tot geen of beperkte financiële schade. Bij twee van de zeven deel-nemers heeft het optreden van de betrokken bank voorkomen dat er schade zou optreden. Daarnaast gaven maar liefst 48 respondenten aan dat ze dit jaar één of

Dreiging - Digitale financiële fraude in de zorg, vervolg

meerdere incidenten met categorie CxO-fraude (bijv. via e-mail, WhatsApp, etc.) hebben waargenomen. Bij drie deelnemers heeft dit geleid tot beperkte financiële schade.

Hoe gaan aanvallers te werk?

De meeste digitale fraudeurs benaderen hun doelwit direct via e-mail, social media-platforms of chatapps. Z-CERT ziet echter dat fraudeurs in toenemende mate gebruik maken van gekaapte accounts van een legitiem persoon of bedrijf. Dit zijn veelal accounts van andere zorginstellingen of (IT-)leveranciers. Z-CERT zag dit jaar een diverse reeks aan thema's en technieken terugkomen die aanvallers gebruikten om hun doelwitten in gerichte of opportunistische campagnes te misleiden, een greep hieruit:

Terugkerende thema's:

- Veel CEO-fraude pogingen
- Waarschuwingen om bijvoorbeeld snel de zorgtoeslag te betalen
- Verzoek tot het betalen van facturen voor medische of IT-gerelateerde diensten
- Het plaatsen van bestellingen bij een leverancier uit naam van de zorgorganisatie

Terugkerende technieken:

- Het achterlaten van QR-codes op fysieke locaties om mensen te verleiden een donatie te doen voor een 'goed' medisch doel.
- QR-codes worden aan e-mails en bestanden toegevoegd om vertrouwen uit te stralen en mensen het gemakkelijker te maken om een betaling te doen.
- Vanuit veel gebruikte e-maildiensten en social mediaplatformen wordt eerst contact gelegd met het doelwit, zonder direct gebruik te maken van besmette bestanden en/of links naar websites.
- Het hacken van mailboxen om vervolgens handig in spelen op lopende e-mail-conversaties.

Voorbeelden van digitale fraude in de zorg

- In de zomer van 2025 is bij een partnerorganisatie van een zorginstelling het account gekaapt op een reserveringsplatform. Via dat account zijn pogingen ondernomen om financiële fraude te plegen. Hoewel er door de hackers geen geld afhandig is gemaakt bij de zorgorganisatie, zijn cliënten en hun familieleden via het reserveringsplatform wel blootgesteld aan ongewenste informatie en mogelijke misleiding. Dit heeft geleid tot reputatieschade en misgelopen reserveringen, geschat in de enkele tienduizenden euro's.
- Dit jaar zijn bij Z-CERT meerdere gevallen gemeld waarbij een hacker een lopende e-mailconversatie heeft gebruikt om fraude te plegen. In één geval was de lopende mailconversatie dusdanig goed gemanipuleerd dat de zorgorganisatie werd misleid om een overboeking te doen van enkele tonnen. Hierbij ging het om een betaling van een legitieme openstaande factuur waarbij alleen het ontvangende rekeningnummer was gewijzigd. De bank van de zorgorganisatie greep gelukkig in en voorkwam de daadwerkelijke storting.

Dreiging - Digitale financiële fraude in de zorg, vervolg

- Eind november 2025 bracht het onderzoeksprogramma Pointer een variant van financiële fraude aan het licht waarbij deepfake-video's ingezet zijn om producten te verkopen op basis van misleidende gezondheidsclaims. De fraudeurs hebben met generatieve AI bekende Nederlandse artsen en onderzoekers nagemaakt om de misleidende gezondheidsclaims te verspreiden [63]. Artsenfederatie KNMG heeft eerder in 2025 advies uitgebracht over wat te doen als zorgmedewerkers te maken krijgen met deepfakes [64].

Verwachting volgend jaar

Z-CERT verwacht dat digitale financiële fraude in het komende jaar verder zal toenemen. De drempel voor dit type aanvallen blijft laag doordat aanvallers gebruikmaken van eenvoudig toegankelijke communicatieplatformen. AI verlaagt deze drempel verder doordat iedereen hiermee overtuigend ogende en professioneel geformuleerde berichten kan genereren, ook aanvallers zonder communicatieve vaardigheden. Omdat AI-hulpmiddelen steeds meer mainstream worden en breder beschikbaar zijn, wordt het voor een grotere groep aanvallers eenvoudiger om de stap naar digitale fraude te zetten. Daarnaast maakt AI het mogelijk om in korte tijd meer fraudepogingen uit te voeren.

Aandachtspunten voor komend jaar

- De combinatie met phishing en het versturen van legitieme facturen waar de aanvaller het rekeningnummer heeft aangepast in zijn eigen rekeningnummer.
- Nepinformatie door gebruik te maken van deepfake video's.
- Continue stroom van nepfacturen, CEO-fraudepogingen en wijzigingsverzoeken van rekeningen.
- Professionaliteit van fraudepogingen neemt toe door gebruik van GenAI.

Aanbevelingen

Neem maatregelen tegen financiële fraude bij:

- Personeelsadministratie
- Crediteurenadministratie
- Heb een proces voor de uitgifte van cadeaubonnen
- Neem technische antispoof-maatregelen

Voor aanvullende en meer gedetailleerde aanbevelingen, zie hoofdstuk '**Aanbevelingen**'.

Enablers

- Tijdelijke medewerkers en hoog personeelsverloop
- Gebrek aan security awareness
- AI

Zie hoofdstuk 'Enablers' voor de uitwerking van de enablers.

Enablers

Bibliografie

[63] **Pointer KRO NCRV**, "Ruim 40 BN'ers en artsen slachtoffer van deepfakes voor supplementen: 'Schadelijk en misleidend'," 2025. [Online]. Available: https://pointer.kro-ncrv.nl/bners-en-artsen-slachtoffer-van-deepfake-videos

[64] **KNMG**, "Medische deepfakes: bedreiging voor vertrouwen en volksgezondheid," 2025. [Online]. Available: https://www.knmg.nl/actueel/nieuws/nieuwsbericht/medische-deepfakes-bedreiging-voor-vertrouwen-en-volksgezondheid

Dreiging Datalek door Insider Threat

Dreiging - Datalek door Insider Threat

Inschatting dreiging: Medium

Tijd: Nu

Onopzettelijk en nalatig handelen werd dagelijks tot maandelijks waargenomen door respondenten. Nieuwsgierig/opzettelijk handelen werd jaarlijks waargenomen.

Dreigingsniveau: Medium

Het is voor medewerkers vrij makkelijk om data te lekken en daarom wordt deze dreiging zeer frequent waargenomen. De impact van een datalek door deze dreiging verschilt per incident.

Actor: Insider Threat

Capaciteit

De insider heeft vaak toegang tot veel (gevoelige) informatie. Of het handelen van een insider threat grote impact heeft, hangt af van de kennis en vaardigheden van de persoon met het omgaan met data.

Motivatie

Onopzettelijk, nalatig, nieuwsgierig (opzettelijk).

Intentie

Nalatig en onopzettelijk handelen is vaak een onbewust proces. Dit is anders bij de nieuwsgierige insiders die bijvoorbeeld data willen inzien van mensen in de persoonlijke sfeer, zoals zorgdata van familie of BN'ers of de buren.

Het opzettelijk veroorzaken van een datalek komt bijvoorbeeld voort uit onvrede, wraak, gewoonweg schade willen aanrichten, persoonlijk of financieel gewin [65]. Bij Z-CERT is één casus bekend waarbij een persoon de dossiers van personen binnen de familiesfeer heeft ingezien voor persoonlijk gewin.

Hoe werd de dreiging zichtbaar?

Nog steeds is het ongeoorloofd gebruik van cloudgebaseerde AI-chatbots (zoals ChatGPT) actueel. Het gebruik van deze chatbots kan tot incidenten leiden. Na het blokkeren van deze chatbots binnen het netwerk van zorginstellingen gingen medewerkers over op het gebruik op de persoonlijke mobieltjes. Uit de survey bleek dit nog steeds dagelijks tot wekelijks voorkomt. Het is lastig om maatregelen te treffen tegen persoonlijk gebruik van chatbots op eigen apparaten. Daarnaast bleek uit de enquête dat onbeheerde schermen op de werkvloer een veel voorkomend probleem blijven. Uit ons onderzoek blijkt dat er in 2025 door medewerkers ongeoorloofd gegevens zijn ingezien van EPD/ECD-data of andere uitslagenbronnen. Data inzien uit nieuwsgierigheid komt daarbij vaker voor dan het inzien van data uit kwade opzet. Deze laatste vorm werd een enkele keer gezien.

In de tabel op de volgende pagina is te zien dat er datalekken waren als gevolg van insider threats, maar dat de impact beperkt is gebleven. Wel hebben datalekken gevolgen gehad voor de betrokkenen en bijgedragen aan het risico op het mijden van zorg.

Dreiging - Datalek door Insider Threat, vervolg

Tabel 3: Datalekken als gevolg van Insider Threats.

Insider Threat	Nooit (%)	Dagelijks (%)	Wekelijks (%)	Maandelijks (%)	Jaarlijks (%)
Datalekken door onopzettelijk en nalatig handelen					
Verkeerd bezorgd (mail)	6	0	13	42	37
Patiënt- of cliëntverwisseling bij het invoeren van gegevens in het EPD/ECD	13	0	31	33	23
Publicatiefout (bestanden op verkeerde plekken: website, intranet, SharePoint)	42	0	2	17	37
Misconfiguratie (bijv. in webapplicatie)	54	0	0	8	37
Onjuiste rechten (onterecht behoud van rechten bij functiewisselingen, rechten groepen verkeerd ingesteld)	33	2	0	17	46
Ongeoorloofd gebruik van cloudgebaseerde opslag- en samenwerkingsapplicaties (zoals Dropbox)	52	2	2	13	27
Ongeoorloofd gebruik van cloudgebaseerde AI chatbots (zoals chatGPT)	40	8	12	15	21
Onbeheerde openstaande schermen	15	13	27	29	12
Verlies of diefstal van apparaten (smartphone, laptop, etc.)	35	0	2	13	46
Datalekken door nieuwsgierig en opzettelijk handelen					
Ongeoorloofde inzage EPD/ECD of andere uitslagenbronnen (motief: nieuwsgierigheid)	62	0	0	8	31
Ongeoorloofde inzage EPD/ECD of andere uitslagenbronnen (motief: kwaadwillend)	88	0	0	0	10
Datalek door toedoen ontevreden medewerker	92	0	0	0	4
Datalek door toedoen ontevreden ex-medewerker	92	0	0	0	4
Datalek door toedoen van een ontevreden medewerker van leverancier of partner	94	0	0	0	2

Dreiging - Datalek door Insider Threat, vervolg

Voorbeelden van incidenten in 2025

- Van een medewerker van een ziekenhuis werd een laptop gestolen waarbij de harde schijf niet was versleuteld. De patiëntgegevens (waaronder foto's) op de laptop waren alleen binnen de applicatie in te zien. Voor de toegang tot die applicatie werd echter een zwak wachtwoord gebruikt.
- Op GitHub werden klantgegevens van meerdere zorgverzekeraars gelekt, waaronder gegevens van zorgverleners. Deze data is na ontdekking verwijderd. Een zelfstandige gebruikte zonder medeweten van de zorgverleners deze data om een AI-model te trainen.
- Eén respondent gaf aan dat een ingeschakelde developer ongeautoriseerd toegang had tot een productiedatabase.
- Binnen een applicatie die wordt gebruikt door apothekers is een kwetsbaarheid gevonden. Hierdoor kon de gebruiker de cloud back-ups van andere gebruikers ophalen en de data daarvan inzien. In deze back-ups waren wachtwoorden onversleuteld opgeslagen. De kwetsbaarheden zijn waarschijnlijk bij het ontwerp van de applicatie ontstaan.
- Uit nieuwsgierigheid hebben medewerkers van een zorgorganisatie ongeoorloofd dossiers ingezien van onder andere buren. Bij het uitvoeren van controles kwamen deze ongeoorloofde inzages aan het licht [66].
- Bij een zorgorganisatie was een USB-stick met cliëntdata zoekgeraakt door een menselijke fout.

Verwachting komend jaar

De dreiging door insider threats zal komend jaar actueel blijven. Een belangrijke factor voor de uiteindelijke impact is of het incident plaatsvindt binnen de eigen zorgorganisatie of bij een externe partij, zoals een leverancier.

Aanbevelingen

- Voer een integrale insider threat-aanpak gericht op preventie, detectie, response en herstel.
- Controleer ook bij externe/ingehuurde partijen hoe zij omgaan met het onderwerp insider threat.

Voor aanvullende en meer gedetailleerde aanbevelingen, zie hoofdstuk '**Aanbevelingen**'.

Enablers

- Data verspreiding en concentratie
- Tijdelijke medewerkers en hoog personeelsverloop
- Gebrek aan security awareness

Zie hoofdstuk 'Enablers' voor de uitwerking van de enablers.

Enablers

Bibliografie

[65] **CISA**, "CISA.GOV," [Online]. Available: https://www.cisa.gov/topics/physical-security/insider-threat-mitigation/defining-insider-threats

[66] **NOS.nl**, "NOS.nl," 9 10 2025. [Online]. Available: https://nos.nl/artikel/2585793-ziekenhuis-dordrecht-ontslaat-medewerkers-die-1100-dossiers-bekeken-uit-nieuwsgierigheid

Enablers van dreigingen

Enablers van dreigingen

Enablers van dreigingen zijn politieke, economische, sociale, technologische, juridische en ecologische ontwikkelingen die niet op zichzelf als cyberdreiging gelden, maar wel omstandigheden creëren die cyberdreigingen in de zorg-sector kunnen versterken of nieuwe aanvalsvectoren mogelijk maken. Dit Cybersecuritybeeld richt zich op hun dreigingsversterkende rol, hoewel sommige ontwikkelingen ook positieve effecten op de weerbaarheid kunnen hebben.

Er bestaan veel enablers die relevant zijn voor de zorg, maar in dit Cybersecuritybeeld hebben we een top 5 geselecteerd die op dit moment als meest actueel en impactvol wordt beschouwd. Deze selectie is mede tot stand gekomen door een vragenlijst die we hebben verspreid onder zorginstellingen.

Data verspreiding en concentratie

Binnen de zorgsector worden grote hoeveelheden patiënt- en cliëntdata opgeslagen. Deze data bevindt zich op veel plekken: bij zorginstellingen zelf, bij leveranciers en ketenpartners, en in informele omgevingen zoals mailboxen en SharePoint. Soms slaan zorginstellingen data die normaal in een SaaS-oplossing staan ook lokaal op, bijvoorbeeld ten behoeve van business intelligence. Voor business intelligence wordt vaak één grote dataverzameling samengesteld uit verschillende bronnen. Er is binnen een organisatie dus zowel sprake van verspreiding van data als van concentratie van data. Het gaat daarbij vaak om niet gepseudonimiseerde data, wat de gevoeligheid en het risico bij toegang vergroot. De spreiding en concentratie creëren veel potentiële toegangspunten. Zodra een actor toegang krijgt, kan hij de data gebruiken voor zijn eigen doeleinden.

De volwassenheid van informatiebeveiliging verschilt sterk binnen de keten. Eén kwetsbare partij kan al voldoende zijn om toegang tot veel gevoelige data te verkrijgen.

Tijdelijke medewerkers en hoog personeelsverloop

Veel zorgorganisaties werken met tijdelijke krachten en kennen een hoog verloop onder personeel. Dit leidt ertoe dat medewerkers minder vertrouwd raken met geldende beveiligingsmaatregelen en procedures. Dit vergroot de kans op menselijke fouten.

Daarnaast stimuleert deze situatie het gebruik van ‘Bring Your Own Device’ (BYOD), waarbij medewerkers hun eigen apparaten gebruiken voor werkdoeleinden. Dit maakt het voor organisaties lastiger om uniforme beveiligingsmaatregelen af te dwingen en vergroot de kwetsbaarheid voor malware en phishing.

Enablers van dreigingen, vervolg

Gebrek aan security awareness

Alert en digitaal vaardig personeel verkleint de kans op beveiligingsincidenten. De mate van awareness bepaalt in belangrijke mate hoe 'vatbaar' een organisatie is voor cyberdreigingen. Veel zorgorganisaties zien dat digitale vaardigheden en security awareness bij medewerkers verbeterd kunnen worden. Dit vraagt niet alleen om kennis, maar ook om aandacht voor cultuur en prioriteit. Interne uitdagingen spelen hierbij een rol, zoals het creëren van een open meldcultuur, het vrijmaken van tijd voor privacy- en security-awareness trainingen en het omgaan met verschillen tussen kantoor- en zorgmedewerkers. Als deze punten onvoldoende worden opgepakt, neemt de kans toe dat aanvallen zoals phishing succesvol zijn en incidenten langer onopgemerkt blijven, waardoor de organisatie kwetsbaarder wordt.

AI

Generatieve AI (GenAI) vergroot het digitale dreigingslandschap op meerdere manieren. Allereerst zetten aanvallers AI in om aanvallen sneller en geautomatiseerd uit te voeren. Omdat ze gebruik maken van dezelfde infrastructuur als legitieme partijen, kunnen ze zich beter verhullen. Daarnaast maakt GenAI ontwikkelaars gemakzuchtiger, wat mogelijk leidt tot extra kwetsbaarheden in software. Bovendien vergroot het gebruik van AI die niet door de organisatie is goedgekeurd, het risico op datalekken. Zo kunnen gevoelige gegevens inclusief wachtwoorden mogelijk uitlekken naar leveranciers, aanvallers en online platforms. Innovatie krijgt vaak voorrang boven veilige en betrouwbare implementatie, terwijl AI uit zichzelf niet bestand is tegen digitale aanvallen. Het is noodzakelijk om beveiliging om AI heen te bouwen. Security professionals vertrouwen AI vaak niet vanwege hallucinaties en het gebrek aan controleerbaarheid, waardoor processen niet zonder meer op AI mogen steunen.
Zie het hoofdstuk over GenAI voor meer informatie.

Enablers van dreigingen, vervolg

Geopolitieke situatie

Geopolitieke ontwikkelingen hebben invloed op verschillende digitale dreigingen die in dit Cybersecuritybeeld worden beschreven.

Nederlandse steun aan Oekraïne heeft geleid tot digitale aanvallen van pro-Russische hacktivisten, vooral wanneer nieuwe steun of sancties worden aangekondigd. In het verleden resulteerde dit in DDoS aanvallen op Nederlandse ziekenhuizen.

Ook bredere geopolitieke spanningen, zoals die tussen Europa, China en de Verenigde Staten, kunnen digitale risico's voor de zorg vergroten. De zorgsector is daarbij kwetsbaar door afhankelijkheden: Europa is sterk afhankelijk van China voor hardware die veel wordt gebruikt in de zorg, en van Amerikaanse leveranciers voor digitale werkplekken, cloudomgevingen en AI technologie. Een situatie waarin de gevolgen van deze afhankelijkheid zichtbaar werden, deed zich voor in 2025. Door Amerikaanse sancties tegen de hoofd-aanklager van het Internationaal Strafhof verloor hij tijdelijk de toegang tot zijn Microsoft e-mailaccount. Deze gebeurtenis was voor het ICC aanleiding om de digitale werkplekomgeving onder te brengen bij een Europees alternatief.

Daarnaast maken cybercriminelen vaak misbruik van geopolitieke gebeurtenissen, bijvoorbeeld door thematische phishing die aansluit bij actuele conflicten of nieuwsberichten.

Aanbevelingen

Aanbevelingen

De maatregelen in dit hoofdstuk vormen geen volledige set beheersmaatregelen, maar een geprioriteerde selectie die helpt risico's te verkleinen die voortkomen uit de beschreven dreigingen. De lijst kan organisaties ondersteunen bij het selecteren en prioriteren van maatregelen. In de kolom 'Doel' wordt gebruikgemaakt van de cybersecurity-concepten uit NEN 7510 2-2024. Daar waar een relatie te leggen is met de NEN 7510 of CIS Controls versie 8, is dat in de tabel aangegeven.

Dreiging: Malware gericht op gebruikers

In het kader van het huidige dreigingslandschap zijn er een paar aanbevelingen extra actueel, zie onderstaande tabellen (1a en 1b).

Tabel 1a: Specifieke aanbevelingen voor 'Malware gericht op gebruikers' 2025.

Maatregelen	CIS control	NEN-7510	Doel
Neem ClickFix-aanvallen op in de awareness-training.	14	6.3	Beschermen
Blokkeer en detecteer 'support op afstand' tools die niet gebruikt worden binnen de organisatie.	2	8.7 8.1	Beschermen Detecteren
Zorg dat leverancierscontracten expliciet eisen bevatten voor security-assessments van Android-apparaten, inclusief controles op software supply chain risico's zoals BadBox2-malware.	15	5.20 5.21	Identificeren

Tabel 1b: Algemene aanbevelingen voor 'Malware gericht op gebruikers' 2025.

Maatregelen	CIS control	NEN-7510	Doel
Installeer en onderhoud anti-malware software.	10	8.7 8.1	Beschermen Detecteren
Zorg dat malafide activiteiten, die niet het gevolg van malware zijn, gedetecteerd en gestopt worden.	8 16	8.15 8.16 5.26	Detecteren Reageren Herstellen
Neem anti-malware maatregelen op e-mail en browser niveau.	9	5.14 8.23	Beschermen
Zorg dat alleen software opgestart kan worden die goedgekeurd is	2	8.7 8.1	Beschermen Detecteren
Organiseer periodiek security awareness trainingen.	14	6.3	Beschermen
Zorg voor een incidentresponsplan voor malware incidenten, inclusief afspraken over voorbereiding, afhandeling en evaluatie.	17	5.24 5.25 5.26 5.27	Identificeren Beschermen Detecteren Reageren Herstellen
Beperk waar mogelijk BYOD-apparaten vanwege de verhoogde kans op malware infecties. Maak waar dat niet mogelijk is gebruik van MDM of MAM (Mobile Application Management).	1 4	8.1 5.10 5.15	Beschermen

Aanbevelingen, vervolg

Dreiging: Credential phishing

In het kader van het huidige dreigingslandschap zijn er een paar aanbevelingen extra actueel, zie onderstaande tabellen (2a t/m 2e).

Tabel 2a: Maatregelen specifiek tegen AiTM phishing.

Maatregelen	CIS control	NEN-7510	Doel
Gebruik waar mogelijk phishing resistente MFA. Prioriteer accounts met verhoogde rechten.	6 5	8.5 8.2	Beschermen
Implementeer regels waarbij toegang alleen wordt verleend op basis van vooraf gedefinieerde voorwaarden. Een belangrijke voorwaarde is dat inloggen uitsluitend mogelijk is vanaf apparaten die compliant zijn en door de organisatie worden beheerd.	6 4	8.35 8.3 8.1	Beschermen

Tabel 2b: Maatregelen tegen het creëren van achterdeuren in cloudomgevingen.

Maatregelen	CIS control	NEN-7510	Doel
Vereis opnieuw authenticatie bij het wijzigen van beveiligingsinstellingen (zoals wachtwoorden).	6	8.5	Beschermen
Sta niet toe dat gebruikers in cloudomgevingen zelfstandig OAuth-apps installeren. Implementeer een beleid waarbij alleen vooraf goedgekeurde of door een beheerder geautoriseerde applicaties toegang krijgen.	5 6	5.18 5.19 5.23	Identificeren Beschermen

Tabel 2c: Maatregelen tegen phishing die niet binnenkomt via e-mail.

Maatregelen	CIS control	NEN-7510	Doel
Beperk de mogelijkheid tot phishing in MS Teams, bijvoorbeeld door enkel berichten van vertrouwde externe domeinen toe te staan.	6	5.23	Beschermen
Phishing kan via verse niet-gemonitorde kanalen (LinkedIn, WhatsApp, etc.). Een gebruiker moet op de link klikken om de phishingsite te openen. Zorg daarom dat al het web- en DNS-verkeer effectief wordt gefilterd om malafide domeinen en URL's te blokkeren.	13	8.20 8.23	Beschermen Detecteren

Tabel 2d: Maatregelen tegen device code phishing.

Maatregelen	CIS control	NEN-7510	Doel
Blokkeer Device Code Flow voor accounts waarvoor het niet nodig is. Maak alleen uitzonderingen voor specifieke, vertrouwde applicaties.	6	8.2 8.3	Beschermen

Aanbevelingen, vervolg

Dreiging: Credential phishing, vervolg

Tabel 2e: Algemene aanbevelingen voor 'Credential phishing' 2025.

Maatregelen	CIS control	NEN-7510	Doel
Implementeer de CIS beveiligingsmaatregelen rondom e-mail en webbrowsers.	9	8.7 8.20 8.23 5.14	Beschermen Detecteren
Implementeer periodieke awareness training zodat medewerkers phishing kunnen herkennen en tijdig melden.	14	6.3	Beschermen
Richt toegangscontrole en accountmanagement in volgens best practices.	5 6	5.15 5.18 8.3 8.5	Beschermen
Faciliteer in de mailclient de mogelijkheid om phishing te melden.	9 14	6.3 6.8	Beschermen Detecteren
Gebruik een veilige mailoplossing voor gevoelige data.	3 9	5.14	Beschermen
Implementeer DLP-oplossingen en bestands-classificatie.	3	8.12 5.12 5.13	Beschermen Detecteren
Pas het 'least privilege' principe toe om de impact van gecompromitteerde accounts door phishing te beperken.	6	5.15 5.18 8.3	Beschermen

Aanbevelingen, vervolg

Dreiging: Ransomware of afpersen met datalekken

In het kader van het huidige dreigingslandschap zijn er een paar aanbevelingen extra actueel, zie onderstaande tabellen (3a en 3b).

Voor aanvullende praktische richtlijnen en incident responsemaatregelen bij ransomware aanvallen kan de NCSC publicatie over ransomware worden geraadpleegd [1].

Tabel 3a: Specifieke aanbevelingen voor 'Ransomware of afpersen met datalekken' 2025.

Maatregelen	CIS control	NEN-7510	Doel
Sta op met internet verbonden systemen alleen toegang op afstand toe via een veilige gateway met MFA en blokkeer RDP en ad hoc externe toegangstools zonder MFA.	12 6 4	5.15 8.5 8.20 8.35	Beschermen Detecteren
Zorg dat edge apparaten zoals firewalls, VPN gateways prioriteit krijgen bij patch-management.	7	8.20	Beschermen

Tabel 3b: Algemene aanbevelingen voor 'Ransomware of afpersen met datalekken' 2025.

Maatregelen	CIS control	NEN-7510	Doel
Om initiële toegang te voorkomen, besteed aandacht aan de maatregelen die zijn gedefinieerd bij phishing en malware.	-	-	-
Beperk de bewegingsruimte van aanvallers door netwerksegmentatie op basis van vertrouwens-niveaus en het blokkeren van bekende aanvalspaden. Maak gebruik van beschikbare (kosteloze) software om aanvalspaden en veelvoorkomende misconfigu-raties op te sporen.	4 13	8.20 8.22 8.35	Beschermen
Pas sterke authenticatie ook toe op interne systemen en accounts met verhoogde rechten.	6	8.5 8.2	Beschermen
Laat beheerders nooit werken vanaf gewone werkstations; zij moeten beheertaken uitvoeren vanaf speciaal beveiligde systemen. Dit verkleint de kans dat aanvallers via een gecompromitteerd gewone account kunnen opklimmen naar beheer-dersrechten.	5 6 12	8.1 8.2 8.35	Beschermen

Aanbevelingen, vervolg

Dreiging: Ransomware leveranciers

Maatregelen tegen ransomware zijn opgenomen in het kopje "Dreiging: ransomware" en zijn grotendeels ook toepasbaar op leveranciers.

Tabel 4: Algemene aanbevelingen voor 'Ransomware leveranciers' 2025.

Maatregelen	CIS control	NEN-7510	Doel
Identificeer, classificeer en prioriteer leveranciers en andere derde partijen die ondersteunend zijn voor het uitvoeren van kerntaken. Dit geldt ook voor niet-IT-leveranciers.	15	5.19	Identificeren
Ontwikkel continuïteitsprocedures om bij ransomware-incidenten bij leveranciers kritieke functies te kunnen blijven uitvoeren.	15 17	5.24 5.25 5.26 5.27	Herstellen
Zorg voor een incident response plan voor leveranciersincidenten, inclusief beslissingen over externe toegang en afsluiten lokale systemen.	15 17	5.19 5.24 5.25 5.26 5.27	Identificeren Beschermen Reageren Herstellen
Voorzie waar mogelijk in alternatieve leveranciers of inkoop-goederenstromen voor noodsituaties.	15	5.19	Identificeren
Test en actualiseer continuïteitsplannen en downtimeprocedures regelmatig.	17	5.24 5.27	Identificeren Beschermen Reageren Herstellen

Dreiging: DDoS bij leveranciers en zorgorganisaties

In het kader van het huidige dreigingslandschap zijn er een paar aanbevelingen extra actueel, zie onderstaande tabellen (5a en 5b).

Tabel 5a: Specifieke aanbevelingen voor 'Ransomware of afpersen met datalekken' 2025.

Maatregelen	CIS control	NEN-7510	Doel
Besteed bij het in kaart brengen van de online diensten waarvoor leveranciers verantwoordelijk zijn ook aandacht aan DNS providers.	15	5.19 5.23	Identificeren Beschermen
Controleer of leveranciers bestand zijn tegen nieuwere DDoS-technieken zoals carpet bombing en DNS Water Torture-aanvallen.	15	5.19 5.23	Identificeren Beschermen

Tabel 5b: Algemene aanbevelingen voor 'Ransomware of afpersen met datalekken' 2025.

Maatregelen	CIS control	NEN-7510	Doel
Factsheet Continuïteit van online diensten [2].	13 15	5.19 5.23 8.21	Identificeren Beschermen
Factsheet Technische maatregelen voor continuïteit voor onlinediensten [3].	13 15	8.20 8.21 5.19	Identificeren Beschermen Detecteren

Aanbevelingen, vervolg

Dreiging: Insider threat

In het kader van het huidige dreigingslandschap zijn er een paar aanbevelingen extra actueel, zie onderstaande tabellen (6a en 6b).

Raadpleeg de publicatie van het NCSC genaamd 'Omgaan met insider threats' over het managen van de insiders threats [4].

Tabel 6a: Specifieke aanbevelingen voor 'Insider threat' 2025.

Maatregelen	CIS control	NEN-7510	Doel
Sla data uitsluitend op op locaties die daarvoor geautoriseerd zijn.	3	5.10 7.10	Beschermen
Pas dataminimalisatie toe: wissel alleen de minimaal noodzakelijke gegevens uit voor het beoogde doel.	3	5.12 5.13	Identificeren Beschermen
Controleer of leveranciers beleid hebben voor awareness én veilig accountbeheer (in-, uitdiensttreding en toegangscontrole).	14 15	5.19 (5.20)	Beschermen
Versleutel draagbare media.	3	7.10	Beschermen
Leveranciers moeten applicaties zo ontwerpen dat gebruikers uitsluitend toegang hebben tot hun eigen data, met data-isolatie en toegangs-controle vanaf het begin ingebouwd.	15 16	5.19 5.23	Beschermen

Tabel 6b: Aanvullende maatregelen voor ongeoorloofde dossierinzage (EPD/ECD).

Maatregelen	CIS control	NEN-7510	Doel
Betrek medewerkers, OR, bestuur en relevante stakeholders bij het inrichten van loggingcontroles op dossiereinzage.	-	-	-
Informeer medewerkers dat inzage in patiënt- of cliëntgegevens uitsluitend functiegerelateerd is en dat logging verplicht en opvraagbaar is.	14	6.3 5.15	Beschermen
Beperk autorisaties en sta noodinzage alleen toe via een 'break-glass'-mechanisme met automatische signalering voor beoordeling achteraf.	6 8	5.15 5.18 8.15	Beschermen
Ontwerp een autorisatiematrix gebaseerd op zorgprocessen, als basis voor automatische loggingcontroles.	6	5.15 5.18 8.15	Beschermen
Detecteer afwijkend inzagegedrag via regels voor opvallende patronen, zoals uitzonderlijk veel verschillende dossier inzagen.	8 16	8.16 8.15	Detecteren Reageren
Beoordeel en bespreek potentiële onterechte inzagen met betrokken medewerkers volgens een vastgelegde procedure.	17	6.4 5.25	Beschermen Reageren

Aanbevelingen, vervolg

Dreiging: Digitale financiële fraude

Voor deze dreiging heeft Z-CERT een separaat kennisproduct geproduceerd [5].

Bibliografie

[1] **NCSC**, "Incidentresponsplan Ransomware," [Online]. Available: https://www.ncsc.nl/incidenten-en-herstellen/incidentresponsplan-ransomware

[2] **NCSC**, "Continuïteit van online diensten," [Online]. Available: https://www.ncsc.nl/ddos/continuiteit-van-online-diensten

[3] **NCSC**, "Technische maatregelen voor de continuïteit van online diensten," [Online]. Available: https://www.ncsc.nl/ddos/technische-maatregelen-voor-de-continuiteit-van-online-diensten

[4] **NCSC**, "Omgaan met insider threats," 29 februari 2024. [Online]. Available: https://www.ncsc.nl/documenten/publicaties/2024/februari/29/omgaan-met-insider-threats

[5] **Z-CERT**, "Financiële fraude (factsheet)," [Online]. Available: https://z-cert.nl/kennisbank/phishing-fraude/factsheet-financiele-fraude

Securitybeeld 2025

Securitybeeld 2025

Cybersecurity omvat meer dan het in kaart brengen van dreigingen. Het gaat om een totaalbeeld van digitale weerbaarheid: van naleving van normen tot het testen van crisisprocessen, van het beheersen van externe aanvalsvlakken (EASM) tot het verantwoord inzetten van nieuwe technologieën. In deze sectie schetsen we een breder beeld van de staat van cybersecurity binnen de Nederlandse zorgsector: waar staan we, welke uitdagingen spelen er, en welke ontwikkelingen vragen om aandacht?

Extern aanvalsoppervlak

Extern aanvalsoppervlak

Z-CERT monitort ruim 165.000 actieve IP-adressen, IP-ranges, domeinnamen, certificaten en webapplicaties in de Nederlandse zorgsector. Het scannen van dergelijke systemen helpt Z-CERT om een overzicht te krijgen van de cybersecurity-status van de Nederlandse zorg. Daarnaast helpt het individuele instellingen bij het identificeren en mitigeren van risico's. In dit securitybeeld gaan we in op Web Application Firewalls (WAFs), op de issues die het vaakst voorkomen en op de belangrijkste issues.

Web application firewalls

Van de webapps gebruikt 25,2% een web application firewall (WAF). Een WAF beschermt webapplicaties en webportalen van shared hosters tegen aanvallen. In de helft van die gevallen wordt er gebruik gemaakt van Cloudflare. Dat betekent dat bij een eventuele Cloudflare-storing zoals in november 2025, minimaal ruim 2.000 webapplicaties in de Nederlandse zorg niet (goed) bereikbaar zijn.

Driekwart van alle webapps gebruikt geen WAF. Bij het scannen daarvan blijken drie risico's het meest voor te komen. Bovenaan staat 'Plaintext Authentication' wat betekent dat data onversleuteld met een formulier kan worden verzonden. Op de tweede plaats staan kwetsbaarheden in veelgebruikte software (Handlebars) die wordt gebruikt voor het maken van een webpagina. Op plek drie staat cross-site scripting (XSS), een kwetsbaarheid waarbij aanvallers schadelijke code kunnen injecteren in webpagina's die dan door bezoekers van de pagina onbewust kan worden uitgevoerd.

Belangrijke en veel voorkomende issues

De meest kritieke issues die Z-CERT bij het scannen van alle assets aantreft, hebben te maken met kwetsbare software. Vaak gaat het hier om eerder genoemde scripts (Handlebars), een webserver oplossing (Apache HTTP), software om op afstand in te loggen (OpenSSH van OpenBSD) en databasesoftware MariaDB. In de praktijk hoeft het door gebruik van backports niet altijd om daadwerkelijk kwetsbare software te gaan.

Wat Z-CERT het vaakst aantreft zijn issues die niet direct een groot gevaar vormen, maar een indicatie zijn van digitale slordigheden. Voorbeelden zijn incorrecte headers, gebruik van HTTP-linkjes in plaats van HTTPS-linkjes en direct aan het internet hangen van applicaties die beter met een VPN beschermd kunnen worden.

Aanbevelingen

Het met technische scans vanaf internet analyseren van zorginfrastructuur levert veel op. Zorginstellingen kunnen veel issues oplossen door degelijk updatebeleid en door niet 'zomaar' applicaties via het internet te ontsluiten. Gebruik waar mogelijk IP-allowlisting en/of een VPN oplossing.

Lang niet alle webapplicaties in de zorg gebruiken op dit moment een WAF. Z-CERT raadt aan dit wel te doen. Tegelijkertijd kan het een risico voor de sector als geheel opleveren als veel organisaties daarvoor van dezelfde cloudoplossing gebruikmaken. Maak een weloverwogen keuze, wellicht afgestemd binnen je regio en/of zorgketen.

NEN 7510 certificering en tekortkomingen

NEN 7510 certificering en tekortkomingen

In Nederland zijn ongeveer 1.000 organisaties NEN 7510 gecertificeerd. Daarvan zijn 200 zorgaanbieder en 800 leveranciers. Aanvullend hierop werken er organisaties volgens de norm zonder gecertificeerd te zijn.

Z-CERT heeft van drie grote certificerende instanties gegevens gekregen over tekortkomingen die bij NEN 7510 audits geconstateerd zijn.

De gegevens van de drie certificerende instanties (hierna: CI's) zijn niet samen te voegen omdat de dwarsdoorsnedes net anders zijn. We benoemen ze eerst per dataset en beschouwen daarna de relatie met de dreigingen uit de andere hoofdstukken. We hebben ervoor gekozen de nummering van de NEN 7510-2017 aan te houden omdat de audits op dit moment vooral nog deze versie van de NEN betreffen.

CI-1

De top drie van tekortkomingen is als volgt:

- A9.4 toegangsbeveiliging van systeem en toepassing
- A18.2 Informatiebeveiligingsbeoordelingen
- A12.4 Verslaglegging en monitoring

Rondom elk van deze beheersdoelstellingen heeft deze CI bij ruim 20% van de organisaties in de sector Zorg en Welzijn één of meer tekortkomingen geconstateerd in de periode 2020-2025.

CI-2

De auditors troffen meer tekortkomingen aan in het managementsysteem dan in de maatregelen per beheersdoelstelling:

- Afwijkingen en corrigerende maatregelen 10.1
- Rollen verantwoordelijkheden en bevoegd heden 5.3
- Risicobehandeling 6.1.3

Dit is op basis van tekortkomingen vanuit de NEN 7510 audits in het kalenderjaar 2024. In de maatregelen komen de meeste tekortkomingen voor bij de doelstellingen "beveiliging in ontwikkelings- en ondersteunende processen (A14.2)", "beheer van dienstverlening van leveranciers (A15.2)" en "informatiebeveiliging in leveranciersrelaties (A15.1)"

CI-3

De derde CI leverde gegevens aan op basis van de NEN7510 tekortkomingen in het jaar 2025 tot eind september. Voor het managementsysteem zijn dit de meest voorkomende onderwerpen:

- leiderschap (hoofdstuk 5) ,
- doelstellingen (6.2) en
- ondersteuning (7).

Qua maatregelen steken er bovenuit:

- incident management (A16.1)
- interne organisatie (A6.1) en
- veilig personeel tijdens het dienstverband (A7.2)

NEN 7510 certificering en tekortkomingen, vervolg

Relatie tussen tekortkomingen en dreigingen

Het is vanzelfsprekend dat een goed functionerend managementsysteem voor informatiebeveiliging een organisatie weerbaarder maakt ten opzichte van dreigingen. In een continue ontwikkelend dreigingslandschap is continue verbetering noodzakelijk en dat gaat nu eenmaal beter met een goed functionerend managementsysteem.

Als onderstaande maatregelen effectief zijn...	... helpt dat tegen deze dreigingen
Snelle detectie (CI-1, A12.4)	Ransomware
Goede beveiliging in leveranciersrelaties (CI-2, A15.1 en A15.2)	Ransomware bij leveranciers DDOS bij leveranciers
Veilig personeel (CI3-A7.2)	Phishing Financiële fraude

Specifieker geldt dat een snelle detectie (CI-1, A12.4) en goed incident management (CI3 – A16.1) de impact van eventuele incidenten kunnen beperken. En een goede beveiliging in leveranciersrelaties (CI-2, A15.1 en A15.2) helpt bij dreigingen vanuit de supply chain.

Tenslotte is naast de techniek ook veilig personeel (CI3-A7.2) van belang in het herkennen van dreigingen zoals phishingmails, CEO-fraude enzovoort.

Aanbeveling

Analyseer de relatief vaak voorkomende tekortkomingen in relatie tot de actuele cyberdreigingen voor de eigen organisatie. Neem de belangrijkste op in de scope van een interne audit (CI-1, A18.2).

Oefenen van dreigingsscenario's

Oefenen van dreigingsscenario's

In dit securitybeeld geven we per dreiging aanbevelingen om te voorkomen dat een dreiging een incident wordt. Aanvullend is het nuttig om uw organisatie voor te bereiden op situaties waarin de beveiliging heeft gefaald en het aankomt op weerbaarheid als menselijke factor. Dat is zeker het geval voor de scenario's die specifiek in het securitybeeld zijn genoemd. Ga die scenario's oefenen want daarvan is de dreiging het grootst.

Om te inventariseren of dit oefenen al gebeurt, heeft Z-CERT een survey uitgevoerd onder de deelnemers van Z-CERT. 65 Personen reageerden daarop.

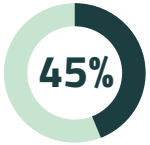
Dit zijn de uitkomsten van de survey:

65 deelnemers hebben de vragenlijst over hun voorbereiding op cyberweerbaarheid ingevuld.

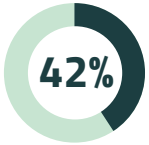
86% heeft rollen en competenties toegewezen aan sleutel-functionarissen.

1 uit de 10 Heeft een programma om rollen en competenties te ontwikkelen tot het doelniveau.

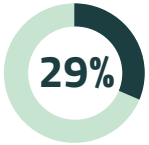
Heeft structurele middelen voor opleiden, trainen en oefenen (zelf of via ROAZ).



Heeft in de afgelopen 12 maanden een cyberoefening gedaan.



Heeft een beleid vastgesteld voor opleiden, trainen en oefenen.



Heeft een doelniveau vastgesteld voor cyberweerbaarheid.

Knelpunten

Jaarlijkse crisistraining ▪ best practice ▪ oefenen ▪ hulpmiddelen ▪ planmatige aanpak ▪ BOB ▪ betaalbare awareness ▪ opleidingen ▪ faciliteiten ▪ advies ▪ ondersteuning oefenen ▪ BCM opleiding ▪ portfolio ▪ ondersteuning IT-beheer ▪ beleidsontwikkeling ▪ kennis delen ▪ crisisrol Z-CERT ▪ grootschalig oefenen

Behoeften

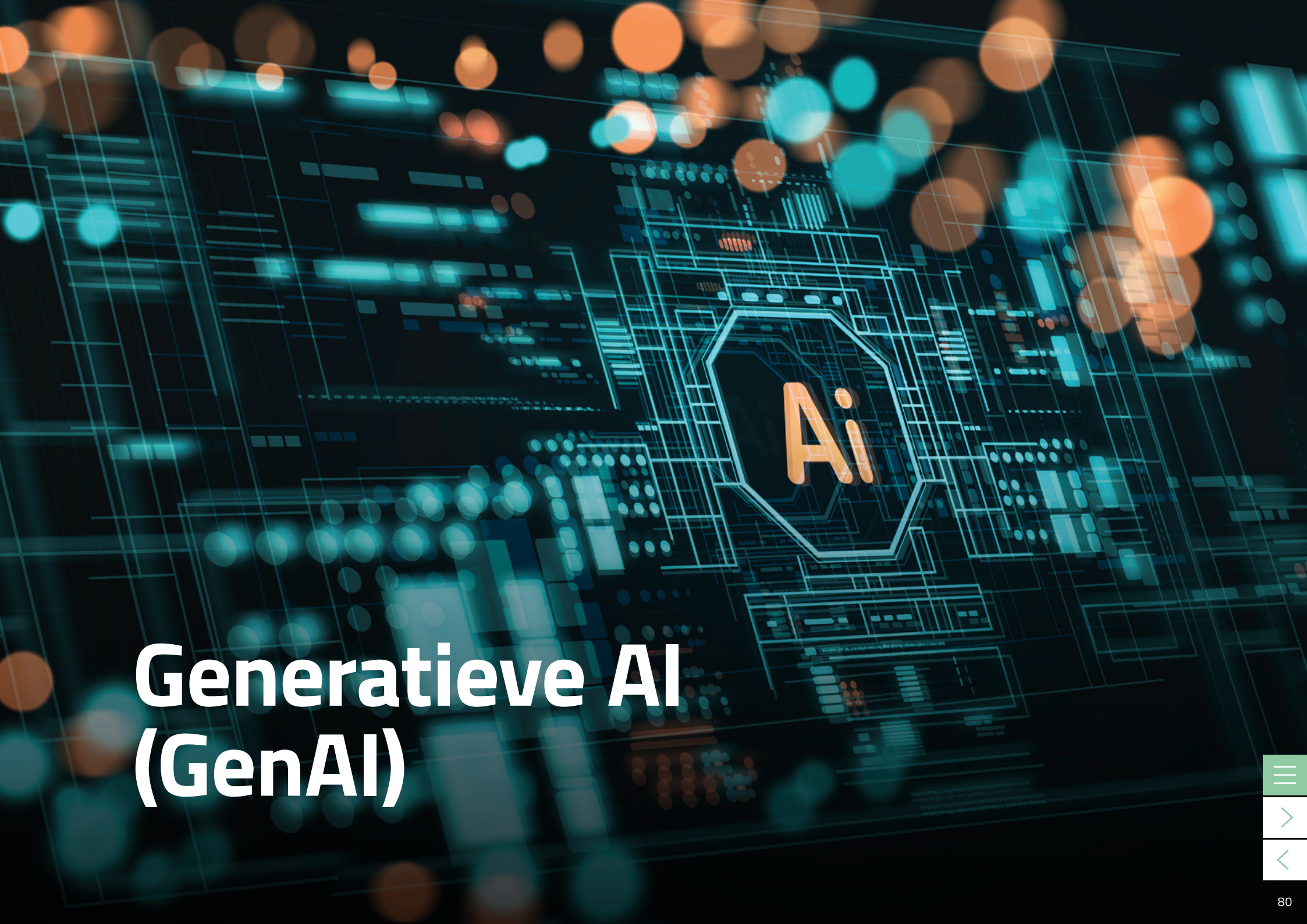
Kennis ▪ urgentie ▪ visie ▪ aandacht ▪ resources ▪ plan ▪ volwassenheid ▪ zzp-ers

Oefenen van dreigingsscenario's, vervolg

De belangrijkste uitkomsten zijn:

1. Nagenoeg alle respondenten (86%) hebben crisisrollen toegewezen aan functionarissen in hun organisatie;
2. Bijna geen enkele respondent (10%) heeft een plan om te zorgen dat die functionarissen zich in hun crisisrol kunnen ontwikkelen.

Voor de weerbaarheid van de zorg is het van belang dat de 10% dichter in de buurt komt bij de 86%. Op de website van Z-CERT (www.z-cert.nl/cyberweerbaar) staan diverse hulpmiddelen waarmee je vandaag kunt starten: Bepaal met het bierviltje de IST en SOLL situatie. Gebruik daarna voor de eerste stappen de roadmap voor het maken van een oefenplan!



Generatieve AI (GenAI)

Generatieve AI (GenAI)

In de zorgsector liggen vele kansen voor GenAI. Bijvoorbeeld om de administratieve lasten te reduceren [67]. Security specialisten, ook van Z-CERT, zien ook de keerzijde: 'early adopters' van AI en beslissers zien gebrek aan vertrouwen als een hindernis [68].

In 2024 gaf Z-CERT het advies: 'Wees waakzaam met de inzet van AI in de zorg.' [69] Het jaar 2025 liet een grote stijging zien in de toepassing van GenAI door kwaadwillenden. GenAI is niet vanzelf beveiligd tegen digitale aanvallen. Dit moet je zelf configureren of er omheen bouwen. Z-CERT ontving in 2025 vanuit de Nederlandse zorg geen cyberincidenten die gerelateerd waren aan misbruik van AI-gekoppelde systemen. In 2026 verwacht Z-CERT hier wel meldingen over te ontvangen. Om deze te helpen voorkomen, schetsen we in deze sectie een aantal risico's en sluiten we af met aanbevelingen om deze in te perken.

Snellere en betere aanvallen

GenAI biedt kwaadwillenden de mogelijkheid om steeds efficiënter aanvallen uit te voeren. In 2025 bleek dat met behulp van GenAI meerdere onderdelen van aanvalsscenario's zijn te automatiseren [70]. GenAI kan zeer overtuigende en misleidende informatie genereren [71]. Daarnaast hoeven kwaadwillenden niet meer te beschikken over hoge technische kennis. Ze kunnen GenAI-diensten vragen om te functioneren als onderdeel van een digitale aanval [72]. Hoewel taalmodellen de toekomst lijken voor geautomatiseerde aanvallen, blijken aanvallers nu nog last te hebben van de onbetrouwbaarheid in door AI-gegenereerde code [73] en kunnen AI-agents afgeleid raken tijdens aanvallen, 'going down rabbit holes' [74].

Kwetsbaarheid AI-systemen zelf

AI-agents worden ontwikkeld om ons zoveel mogelijk digitaal te ontlasten. Deze welwillendheid van GenAI zorgt er ook voor dat ze eenvoudig misleid kunnen worden. Zo blijken moderne AI-browsers namens de gebruiker te kunnen klikken op phishinglinkjes en zo zichzelf te laten infecteren [75]. Onderzoek heeft aangetoond dat ook de AI-agents van aanvallers eenvoudig zijn te misleiden door deze welwillendheid [76]. De kwetsbaarheid van GenAI systemen voor digitale aanvallen is in 2025 goed zichtbaar geworden.

Hieronder enkele voorbeelden:

- De kwetsbaarheid EchoLeak, CVE-2025-32711, gaf aanvallers de mogelijkheid om zonder gebruikersinteractie, via Microsoft 365 Copilot, data te lekken uit iemands e-mail door enkel aan het slachtoffer een mailtje te sturen [77]. Volgens een bericht op LinkedIn is hiervan misbruik waargenomen [78].
- Door een kwetsbaarheid in Azure Machine Learning (AML) kon een aanvaller, met enkel toegang tot een Storage Account, uiteindelijk beheerdersrechten verkrijgen [79].
- Onderzoekers hebben aangetoond een smarthome te kunnen overnemen door malafide instructies voor Google Gemini te verstoppen in een kalenderuitnodiging [80].
- Door teksten te laten samenvatten door GenAI kunnen malafide instructies worden gegeven aan de GenAI, die voor het menselijk oog niet zichtbaar waren [81].

Beveiligingsmaatregelen omzeilen

Meerdere malen is aangetoond dat maatregelen tegen misbruik van de taalmodellen in GenAI systemen, eenvoudig zijn te omzeilen. Dit bevestigt het beeld dat de beveiliging

Generatieve AI (GenAI)

van GenAI systemen niet moet afhangen van het lerend vermogen van AI. Hoe je een taalmodel ook traint, er zullen altijd uitzonderingen zijn die aanvallers kunnen inzetten om de AI te misleiden [82].

Hieronder enkele voorbeelden:

- Detectie voor het herkennen van deepfake audiofragmenten bleek te omzeilen door de nepfragmenten af te spelen en nogmaals op te nemen met echte achtergrondgeluiden [83].
- Malafide code werd gezien als veilige code doordat het verstopt zat tussen wettelijke disclaimers of gebruikersvoorwaarden [84].
- Zeer geavanceerde AI-modellen zoals GPT-5 blijken nog steeds vatbaar voor het produceren van ongewenst gedrag, als dit in verhaalvorm en stapje voor stapje aan hen wordt gevraagd [85].
- Aan AI-security tooling is te verzoeken om 'niet te kijken' [86].
- Maatregelen als 'Human-in-the-Loop', waarbij de AI eerst aan de gebruiker toestemming vraagt om iets te doen, zijn op creatieve manier omzeild [87].

Kwetsbare code

Meerdere bronnen wijzen op kwetsbaarheden in systemen die ontstaan zijn door het gebruik van AI-gegenereerde code en het ontsluiten van AI-systemen aan het internet:

- De herhaling van kwetsbare codepatronen in open-source software vormt een ernstig probleem, vooral omdat AI-systemen deze onveilige patronen onbedoeld reproduceren en verspreiden [88].
- Bij het controleren van door AI-gegenereerde code, bleek uit een onderzoek dat 45% van de code niet voldoet aan security-vereisten en introduceerde AI bekende kwetsbaarheden [89].
- Bij het scannen van het internet, bleken meerdere AI-servers publiekelijk toegankelijk te zijn, waarvan 20% onbeveiligd [90].

Nog meer creativiteit

GenAI maakt bestaande aanvallen effectiever en kwaadwillenden investeren in de ontwikkeling van taalmodellen zonder ethische restricties, zoals GhostGPT, WormGPT, DarkGPT en FraudGPT [91]. GenAI wordt ingezet om overtuigende phishingpagina's te maken [92], om malware aan te passen, zodat het virusscanners omzeilt [93]. GenAI wordt ook al ingezet om bij het laden van een phishingpagina te achterhalen of het praat met een potentieel slachtoffer of met security onderzoekers, om vervolgens andere content te laten zien, cloaking-as-a-service [94]. Volgens ENISA vertegenwoordigen AI-ondersteunde phishingcampagnes meer dan 80 procent van de waargenomen social engineering-activiteiten wereldwijd [95]. Microsoft stelt dat het gebruik van AI de kans dat een slachtoffer op een phishing-link klikt aanzienlijk vergroot, namelijk 54% versus de 12% bij een door mensen opgestelde phishingmail [96]. Tot slot zijn kwaadwillenden begonnen met het dreigen om gestolen data aan AI-modellen te voeden als trainingsmateriaal, als slachtoffers niet bereid zijn te betalen [97].

Generatieve AI (GenAI)

Aanbevelingen

- Zoek bij investeringen in GenAI meer balans tussen innovatie en het op een veilige en betrouwbare manier inrichten van IT [98].
- Vervang niet volledige IT-processen door GenAI, maar enkel de onderdelen die aantoonbaar en controleerbaar een toegevoegde waarde hebben in de zorg.
- Pas de principes toe van zero-trust bij het koppelen van systemen aan GenAI. De technologie achter GenAI is niet veilig tegen digitale aanvallen. Die beveiliging moet je er zelf omheen bouwen.
- Promoot het gebruik van goedgekeurde GenAI toepassingen om shadow-AI te voorkomen.

Bibliografie

[67] **NOS**, [Online]. Available: https://nos.nl/nieuwsuur/artikel/2569723-800-miljoen-voor-ai-in-de-zorg-wat-kan-agema-daarmee-doen

[68] **Veiligheid en veerkracht**, [Online]. Available: https://www.veiligheidenveerkracht.nl/projecten/cybersecurity-van-genai-in-de-veiligheidszorg/

[69] **Z-Cert**, [Online]. Available: https://z-cert.nl/actueel/nieuws/ai-in-de-zorg

[70] **Straiker**, [Online]. Available: https://www.straiker.ai/blog/cyberspike-villager-cobalt-strike-ai-native-successor

[71] **Barracuda**, [Online]. Available: https://blog.barracuda.com/2025/09/11/poisongpt-weaponizing-ai-disinformation

[72] **Eset**, [Online]. Available: https://www.eset.com/us/about/newsroom/research/eset-discovers-promptlock-the-first-ai-powered-ransomware/

[73] **Netskope**, [Online]. Available: https://www.netskope.com/blog/the-future-of-malware-is-llm-powered

[74] **J. C. Andreas Happe**, "Can LLMs Hack Enterprise Networks? Autonomous Assumed Breach Penetration-Testing Active Directory Networks," ACM, 2025. [Online]. Available: https://arxiv.org/abs/2502.04227v3

[75] **Guard**, [Online]. Available: https://guard.io/labs/scamlexity-we-put-agentic-ai-browsers-to-the-test-they-clicked-they-paid-they-failed

[76] **Y. M. Daniel Ayzenshteyn**, "Cloak, honey, trap: proactive defenses against LLM agents," 2025. [Online]. Available: https://dl.acm.org/doi/10.5555/3766078.3766493

[77] **Aim**, [Online]. Available: https://www.aim.security/lp/aim-labs-echoleak-blogpost

[78] **LinkedIn**, [Online]. Available: https://www.linkedin.com/posts/pradeeps_cve-2025-32711-is-a-turning-point-last-activity-7342387287927767040-BLEr/

[79] **Orca**, [Online]. Available: https://orca.security/resources/blog/azure-machine-learning-privilege-escalation/

[80] **Dark Reading**, [Online]. Available: https://www.darkreading.com/cyberattacks-data-breaches/google-gemini-ai-bot-hijacks-smart-homes

[81] **Cloudsek**, [Online]. Available: https://www.cloudsek.com/blog/trusted-my-summarizer-now-my-fridge-is-encrypted----how-threat-actors-could-weaponize-ai-summarizers-with-css-based-clickfix-attacks

[82] **NCSC**, [Online]. Available: https://www.ncsc.gov.uk/blog-post/prompt-injection-is-not-sql-injection

[83] **N. M. a. P. Sperl**, "Replay Attacks Against Audio Deepfake Detection," arXiv, 2025. [Online]. Available: https://arxiv.org/abs/2505.14862

[84] **Hackread**, [Online]. Available: https://hackread.com/legalpwn-attack-genai-tools-misclassify-malware-safe-code/com/2025/08/researchers-uncover-gpt-5-jailbreak-and.html

Bibliografie, vervolg

[85] **The Hacker News**, [Online]. Available: https://thehackernews.com/2025/08/researchers-uncover-gpt-5-jailbreak-and.html

[86] **The Hacker News**, [Online]. Available: https://thehackernews.com/2025/12/malicious-npm-package-uses-hidden.html

[87] **Checkmarx**, [Online]. Available: https://checkmarx.com/zero-post/bypassing-ai-agent-defenses-with-lies-in-the-loop/

[88] **O. G. Jafar Akhoundali**, "Eradicating the Unseen: Detecting, Exploiting, and Remediating a Path Traversal Vulnerability across GitHub," arXiv, 2025. [Online]. Available: https://arxiv.org/abs/2505.20186

[89] **Veracode**, "2025 GenAI Code Security Report," Veracode, 2025. [Online]. Available: https://www.veracode.com/blog/genai-code-security-report

[90] **Cisco**, [Online]. Available: https://blogs.cisco.com/security/detecting-exposed-llm-servers-shodan-case-study-on-ollama

[91] **Cisco**, [Online]. Available: https://blog.talosintelligence.com/cybercriminal-abuse-of-large-language-models

[92] **Okta**, [Online]. Available: https://www.okta.com/newsroom/articles/okta-observes-v0-ai-tool-used-to-build-phishing-sites

[93] **Dark Reading**, [Online]. Available: https://www.darkreading.com/endpoint-security/ai-malware-poc-evades-microsoft-defender

[94] **Infosecurity-magazine**, [Online]. Available: https://www.infosecurity-magazine.com/news/ai-cloaking-tools-enable-complex

[95] **Enisa**, "ENISA Threat Landscape 2025," ENISA, 2025. [Online]. Available: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025

[96] **Microsoft**, "Microsoft Digital Defense Report 2025," Microsoft , 2025. [Online]. Available: https://www.microsoft.com/en-us/corporate-responsibility/cybersecurity/microsoft-digital-defense-report-2025

[97] **Security Affairs**, [Online]. Available: https://securityaffairs.com/182014/malware/lunalock-ransomware-threatens-victims-by-feeding-stolen-data-to-ai-models.html

[98] **Cert-EU**, [Online]. Available: https://cert.europa.eu/publications/security-guidance/generative-ai-in-cybersecurity-balancing-innovation-and-risk

[99] **Month of AI Bugs**, [Online]. Available: https://monthofaibugs.com

Digitale autonomie

Digitale autonomie: Regie over je digitale afhankelijkheid

Diverse instanties, zoals het Rathenau Instituut [100], de Algemene Rekenkamer [101] en de AIVD [102], waarschuwden al eerder voor de toenemende afhankelijkheid van grote technologiebedrijven (dit betreft dan vaak de Amerikaanse Big Tech), die cruciale digitale diensten en infrastructuur leveren. Deze afhankelijkheid beperkt de controle over kernprocessen en zou de continuïteit in gevaar kunnen brengen. Ook binnen de zorg lopen veel kritieke IT-diensten via een of enkele grote Europese en niet-Europese aanbieders.

Bij de inkoop van producten uit China is er bezorgdheid over de potentiële invloed van de Chinese staat op bedrijven. In de zorg wordt gebruik gemaakt van Chinese apparatuur, zoals echoapparatuur en patiënt-monitoring systemen [103].

Wat zijn de risico's van afhankelijkheid

De toenemende afhankelijkheid in relatie tot de toenemende dreiging hebben diverse risico's tot gevolg. Hieronder de belangrijkste:

- Onvoldoende regie over eigen processen: Zorginstellingen bouwen hun digitale infrastructuur op technologieën waarvan zij de werking niet volledig kunnen controleren, zoals software, AI-tools, domotica en cloudopslag. Dit zorgt voor beperkt inzicht en controle. Er is onvoldoende zicht op hoe digitale technologie functioneert binnen zorgprocessen, wat leidt tot afnemende grip op beveiliging en privacy.
- Processen kunnen afhankelijk zijn van één of enkele grote bedrijven. Er is een groeiend risico op vendor lock-in en beperkte innovatie, waarbij koppelingen met andere systemen onmogelijk zijn. Dit maakt dat zorgorganisaties afhankelijkheid ervaren en daardoor zowel technisch als organisatorisch beperkte mogelijkheden zien om te kunnen overstappen naar andere leveranciers.
- Amerikaanse wetgeving (zoals de CLOUD Act) zal ertoe leiden dat niet-Europese overheden toegang krijgen tot patiënt/cliënt data, zelfs als die data in Europa is opgeslagen. Dit heeft effect op vertrouwelijkheid van data. Qua beschikbaarheid van systemen kan de Amerikaanse overheid dienstverleners opdragen bepaalde diensten voor personen of organisaties uit te schakelen. Daarom ontstond discussie toen in de zomer van 2025 Zivver werd overgenomen door Kiteworks [104].
- Acute technische storingen bij externe dienstverleners (zoals bij de Crowdstrike-storing [105]) kunnen directe gevolgen hebben voor de beschikbaarheid van cruciale zorgsystemen. Dit heeft effect op de beschikbaarheid/ continuïteit van zorg dienst-verlening. Een belangrijke nuance hierbij is dat een alternatief in eigen beheer niet hoeft te betekenen dat de oplossing van de storing eenvoudiger of sneller opgelost is.
- Onvoldoende voorbereiding op ICT-uitval: Veel zorginstellingen zijn zich bewust van de afhankelijkheid, maar niet voldoende voorbereid op de gevolgen van uitval. Zo zijn zij onvoldoende weerbaar om kritieke zorgprocessen voort te zetten en het tijdig beschikbaar zijn van patiëntinformatie.

Voor de sector als geheel geldt dat veel zorgaanbieders afhankelijk zijn van dezelfde leveranciers. Daarom heeft een dreiging of uitval bij die leverancier direct impact op een groot deel van de zorgsector. Daardoor wordt mogelijk de druk op capaciteit in de rest van de sector groot.

Digitale autonomie: Regie over je digitale afhankelijkheid

Risicoanalyse en maatregelen

Om inzicht en overzicht te krijgen binnen de eigen organisatie en in de keten is het uitvoeren van een risicoanalyse voor de eigen processen een belangrijke eerste stap. Voorbeeldvragen zijn:

- In hoeverre is jouw ICT-infrastructuur, software en data, maar ook domotica, sensoren (OT) afhankelijk van technologie die door uitval van een dienst/leverancier verminderd beschikbaar zouden kunnen worden?
- Hoe groot acht je de kans dat die uitval zich voor zou doen (daarbij óók kijkend naar niet-technische aspecten, zoals onverwachte geopolitieke situaties)?
- Welke impact zou een onderbreking van deze toeleveringen hebben op jouw bedrijfscontinuïteit?
- Welke andere risico's levert dit op?
- Zijn er alternatieve leveranciers of technologieën beschikbaar als noodscenario?

Op basis van deze analyse kunnen zorgorganisaties een risicogebaseerde aanpak ontwikkelen. Deze zou maatregelen zoals bewustwording, business continuity management, cloud exit-strategieën, leveranciersmanagement en dataportabiliteit kunnen bevatten.

Eerste handvatten: leveranciersmanagement en exit-strategie

Een belangrijk aandachtspunt waar inzicht en regie mee start is de relatie die een organisatie heeft met haar leveranciers. Vereisten op het vlak van onafhankelijkheid kunnen in het programma van eisen opgenomen te worden. Zo zou van een ECD-leverancier het faciliteren van offline back-ups geëist kunnen worden. Zo zijn er ziekenhuizen die een 'nood' EPD hebben. Zij maken dagelijks een kopie van het EPD en hebben een aantal laptops in de kluis liggen om in te zetten in geval van nood.

Een exit-strategie is belangrijk omdat je daarmee regelt op welke wijze je de continuïteit waarborgt bij beëindiging contract en/of stoppen dienstverlening (om welke reden dan ook). De VNG heeft hier goede hulpmiddelen voor gemaakt, geschreven voor gemeenten maar ook bruikbaar in de zorg. Een ESCROW regeling of het gebruik van open-source kan een deel vormen van een exit-strategie. Bedenk daarbij wel goed dat je in voorkomende gevallen wel over de broncode beschikt, maar daarmee niet per definitie de kennis in huis hebt om die broncode snel genoeg opnieuw in te zetten in een nieuw of ander product.

Bibliografie

[100] **Rathenau Instituut**, [Online]. Available: https://www.rathenau.nl/nl/digitalisering/naar-een-nieuwe-verhouding-tot-technologiebedrijven/koers-zetten-richting-digitale-autonomie

[101] **Algemene Rekenkamer**, [Online]. Available: https://www.rekenkamer.nl/publicaties/rapporten/2025/01/15/het-rijk-in-de-cloud

[102] **AIVD**, [Online]. Available: https://www.aivd.nl/actueel/nieuws/2024/03/01/clingendael-brengt-rapport-uit-over-veiligheid-europees-internetverkeer

[103] **Een Vandaag**, [Online]. Available: https://eenvandaag.avrotros.nl/artikelen/chinees-techbedrijf-maakt-opmars-in-zorgsector-zorgen-om-privacy-patienten-niemand-heeft-er-echt-zicht-op-147529

[104] **FTM**, [Online]. Available: https://www.ftm.nl/artikelen/vertrouwelijke-zaken-te-grabbel-na-overname-zivver-door-kiteworks

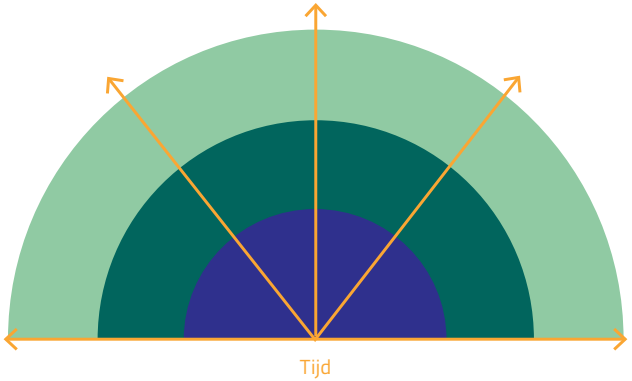
[105] **NOS**, [Online]. Available: https://nos.nl/artikel/2529477-wat-is-crowdstrike-en-hoe-kon-het-zo-misgaan-dit-is-wat-we-nu-weten

Uitleg bij dreigingsradar

Uitleg bij dreigingsradar

De dreigingsradar is gebaseerd op het Factor Analysis of Information Risk-framework (FAIR) in combinatie met een model dat een dreigingsscore berekent. Het model is ontwikkeld in het Shared Research Programma (SRP) Cyber Security dat is gecoördineerd door TNO. Hieraan hebben ook partners als ING, ABN AMRO, Rabobank, Volksbank en Achmea deelgenomen.

Het is verdeeld in een 3x3 matrix en geeft de tijd en impact weer van cyberdreigingen in de zorg. De impact van een dreiging kan laag/middel/hoog zijn. De tijdlijn is verdeeld in de situatie op het moment van schrijven, de situatie die is te verwachten op korte termijn (binnen 1 jaar) of de dreigingen die in de toekomst (over meer dan 1 jaar) impact kunnen gaan hebben.



Figuur 1a: Weergave van tijd in de 3x3 matrix (verloop).

De positionering van de diverse bolletjes (met impact laag/middel/hoog) in de radarfiguur hangt samen met de weging van de dreiging in relatie tot de tijd. Is er op dit moment een bepaalde dreiging te signaleren, dan zal de dreiging met het daaraan verbonden nummer gepositioneerd worden in het radargedeelte van actuele dreigingen. Is een bepaald type dreiging op korte termijn te verwachten, binnen nu en één jaar, dan zal de betreffende dreiging worden gepositioneerd in de tweede ring. Tenslotte blikken wij ook vooruit en dreigingen die Z-CERT verwacht over meer dan 1 jaar zullen geplaatst worden in de buitenste ring.

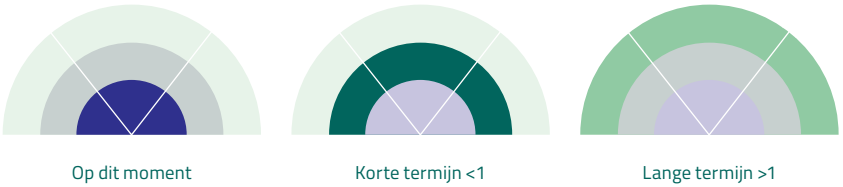
De plaatsing van de bolletjes geeft bovendien de ernst van de dreiging aan. In de rechter taartpunt staan de ernstigste dreigingen. Hoe meer de bolletjes naar links staan, hoe lager de dreiging is die ervan uitgaat.

Kleur	Impact
	Hoog
	Gemiddeld
	Laag

Tabel 1: Aanduiding van kleur en bijhorende impact.

Uitleg bij dreigingsradar, vervolg

Figuur 1b: Weergave van tijd in de 3x3 matrix (ringen).



De inschaling van de impact en de positie van de dreiging is gebaseerd op een rekenmodel van TNO. De geschatte tijd is gebaseerd op kennis van experts.

Actortypologie

Voor het Cybersecuritybeeld wordt voor de actortypologie aangesloten bij het daderspectrum uit het Cybercrimebeeld Nederland (CCBN) 2024 van de politie en het Openbaar Ministerie [106]. Dit spectrum classificeert actoren op basis van technische vaardigheden, de mate van organisatiegraad en het onderliggende motief.

De indeling, van laag naar hoog niveau, luidt als volgt:

1. Cybercriminelen zonder technische ervaring
2. Hacktivisten
3. Cybercriminelen met technische ervaring
4. Georganiseerde cybercrime
5. Statelijke actoren

Het bepalen van de actor of het actorniveau achter cyberaanvallen is in de praktijk niet altijd eenduidig. Attributie ontbreekt vaak of is onvoldoende betrouwbaar om specifieke incidenten aan een actor of aan een actorcategorie uit het daderspectrum te koppelen. Z-CERT kiest daarom voor een praktische aanpak. Er wordt gekeken naar het totaalbeeld van meldingen en naar de impact van wat er heeft plaatsgevonden. Op basis daarvan wordt een waarschijnlijke actortypologie bepaald die past bij het actuele dreigingsbeeld. Deze indeling is geen formele attributie, maar biedt organisaties wel houvast bij risicoanalyses en het bepalen van passende maatregelen.

Bibliografie

[106] **Openbaar Ministerie**, [Online]. Available: https://www.om.nl/onderwerpen/c/cybercrime/cybercrimebeeld-cybercrimebeeld-ccbn

Dankwoord

Dankwoord

We danken iedereen die heeft meegewerkt aan de productie van dit Cybersecurity Beeld Zorg 2025, onder wie een aantal reviewers van zorginstellingen, CISO's en security specialisten van verschillende zorginstellingen.

We willen met name onze dank uitbrengen aan:

Entrea Lindenhout	Ferry Schopman
Partners voor Jeugd	Ferdy van der Hurk en Hans-Cees Speel
Cello	Peter Brus
Leger des Heils	Hugo Gerritsen en Kevin Schepers
Coöperatie Cohesie U.A.	Robin Oomens
Abrona	Largoen Tamana en Jan Willem van der Grift
ORO	Bettina van Poppel en Marina van Bekkum
Star-shl	Rudi Brence
DrechtDokters	Alex Beckers
GGZ Westelijk Noord-Brabant	Bianca Bogers
HKN Huisartsen	Matthijs Leentvaar
KleinGeluk	Jaap de Leeuw
Ambulancezorg Nederland	Anno van Dijke

Parlan	Ron Ploeg, Thom Bennink en Richel Stuijt
Timon	José Hol en Parastu Zahib
Boba Zorg	Remco Veens
Maasstad ziekenhuis	Dennis Verschuuren en John Verschoor
Amsterdam UMC	Ewald Beekhuis
Catharina Ziekenhuis	Erick van Veghel
DEKRA	
KIWA	
DNV	
Orange Cyberdefense	

Vormgeving: Björn Lansink - ontwerp & illustratie | Copyright © Z-CERT, februari 2026.

De Nederlandse zorg digitaal veilig

Stichting Z-CERT - Stationsplein 121, 3818 LE Amersfoort

033 737 06 09 - info@Z-CERT.nl - Z.CERT.nl - LinkedIn.com/company/z-cert