Jaarverslag 2025

De Nederlandse zorg digitaal veilig

Inhoudsopgave

Voorwoord

Het jaar 2025 stond voor Z-CERT in het teken van drie belangrijke ontwikkelingen. De digitalisering in de zorgsector nam verder toe en daarmee ook het risico op cyberincidenten. Tegelijkertijd groeide de organisatie in omvang en professionaliteit. Daarnaast werd er intensiever samengewerkt met partners binnen Nederland en daarbuiten, omdat de actuele dreigingen meer dan ooit vragen om gezamenlijke inspanningen.

De groei van de organisatie

In 2025 heeft Z-CERT veel geïnvesteerd in de voorbereiding op de Cyberbeveiligingswet (Cbw), die naar verwachting in 2026 van kracht wordt. Achter de schermen is de organisatie gegroeid, zowel in het aantal medewerkers als in volwassenheid en expertise. Een mijlpaal was de oprichting van de Ondernemingsraad, die in 2025 voor het eerst officieel operationeel was.

Deze ontwikkeling past binnen de bredere professionaliseringsslag die nodig is om de wettelijke taken als sectoraal CSIRT (Computer Security Incident Response Team) te kunnen blijven vervullen. Die rol is sinds de inwerkingtreding van de Europese NIS2-richtlijn verder aangescherpt, en met de naderende Cyberbeveiligingswet wordt die verantwoordelijkheid alleen maar groter.

Voorwoord - vervolg

Aanvallen in de zorg

De uitbreiding in kennis en capaciteit bleek in 2025 noodzakelijk, want de cyberdreiging voor de Nederlandse zorg is afgelopen jaar verder toegenomen. Criminelen maakten gebruik van steeds geavanceerdere methoden, waaronder zeer geloofwaardige phishingcampagnes. Daarnaast groeide de afhankelijkheid van clouddiensten voor het opslaan en verwerken van medische gegevens, waardoor aanvullende risico's ontstonden.

Een duidelijk voorbeeld was het datalek bij het laboratorium van Clinical Diagnostics Nederland. Dit incident benadrukte het belang van sterke cybersecurity binnen zorgorganisaties zelf, maar ook binnen de keten van leveranciers en partners. Het werd duidelijk dat een incident bij een externe partij aanzienlijke impact kan hebben op de continuïteit van de zorg.

Samenwerking is nodig

Om het brede zorgveld in Nederland nog beter te bereiken, heeft Z-CERT in 2025 nieuwe manieren ingezet. Zo maakten we twee podcastseries onder de titel *Zet 'm op* en trokken we met Z-CERT live! on tour het land in, waarbij kennisdeling centraal stond.

Ook internationaal hebben we belangrijke stappen gezet. In samenwerking met partnerorganisaties in België, Frankrijk en Denemarken is een Europees projectvoorstel ingediend onder de naam *NoMoreCyberincidentsInHealth*. Daarnaast is Z-CERT nog altijd een van de drijvende krachten van het European Health ISAC (Information Sharing and Analysis Center), waarmee we actief bijdragen aan kennisdeling en samenwerking op het gebied van internationale zorg en cybersecurity.

Begin 2025 presenteerden we ons jaarlijkse Cybersecurity Dreigingsbeeld voor de zorg aan Europarlementariër Bart Groothuis. Hij stond aan de basis van de NIS2-richtlijn, die in Nederland wordt ingevoerd als de Cyberbeveiligingswet. In 2026 treedt deze wet officieel in werking. Dat betekent dat duizenden Nederlandse organisaties verplicht worden hun digitale weerbaarheid aantoonbaar te versterken. Zorgorganisaties kunnen dat deels zelf, maar cyberweerbaarheid vraagt ook om gezamenlijke inspanningen. En daarbij willen we de Nederlandse zorg ook in 2026 weer volop ondersteunen.

Wim Hafkamp - Directeur Z-CERT

Over Z-CERT

Over Z-CERT

Computer Emergency Response Team

Z-CERT is het Computer Emergency Response Team (CERT) voor de Nederlandse zorgsector. De organisatie is in 2016 als stichting opgericht op initiatief van de Nederlandse Vereniging van Ziekenhuizen (NVZ), de Nederlandse Universitair Medische Centra (UMCNL), de Nederlandse GGZ (GGZ) en het ministerie van VWS.

De afgelopen jaren zijn wij zeer sterk gegroeid. Niet alleen is het aantal zorgorganisaties dat zich heeft aangesloten gegroeid, ook als organisatie is Z-CERT flink uitgebreid. Wij bedienen steeds meer grote en minder grote zorgorganisaties in Nederland waaronder de meeste ziekenhuizen, veel GGZ-instellingen, gehandicapten- en ouderenzorg en diverse koepelorganisaties in de zorg. We voorzien de zorgorganisaties van waarschuwingsberichten, bieden incident response en geven adviezen op het gebied van cybersecurity en informatiebeveiliging.

Door de komst van de Europese Network and Information Security Directive (NIS2-richtlijn) neemt het aantal zorgorganisaties dat bij Z-CERT is aangesloten het komend jaar fors toe.

Erkenning door de overheid

In 2024 heeft de minister van Volksgezondheid, Welzijn en Sport ons expliciet genoemd als een cruciale partner in het versterken van de digitale weerbaarheid van de zorgsector. In de Cyberbeveiligingswet worden wij aangewezen als het Computer Security Incident Response Team (CSIRT) voor de Nederlandse zorg. Als CSIRT krijgt Z-CERT een aantal wettelijke taken. Deze erkenning benadrukt het belang van onze voortdurende inzet en expertise op het gebied van cybersecurity binnen de gezondheidszorg. En het draagt in belangrijke mate bij aan onze missie: de Nederlandse zorg digitaal veilig.

Vanzelfsprekend is samenwerking voor Z-CERT daarbij belangrijk. We werken daarvoor onder andere samen met een professioneel netwerk van bij ons aangesloten organisaties en zorginstellingen, waaronder het Nationaal Cyber Security Centrum (NCSC), het ministerie van VWS, de Inspectie Gezondheidszorg en Jeugd (IGJ), Health-ISAC (Information Sharing and Analysis Center), brancheorganisaties en fabrikanten/leveranciers.

Raad van Toezicht

Z-CERT is een stichting zonder winstoogmerk die wordt ondersteund door een Raad van Toezicht (RvT). De RvT bewaakt het beleid en de algemene gang van zaken binnen de organisatie en voorziet de directie van strategisch advies. In 2025 bestond de RvT uit vier leden, allen met een achtergrond in de zorgsector of de Rijksoverheid.

Over Z-CERT - vervolg

De samenstelling van de Raad is als volgt:

- Evelien Bongers - lid Raad van Bestuur RIBW K/AM
- Remco van Lunteren - lid Raad van Bestuur UMC Utrecht
- Carlijn de Ruijter - lid Raad van Bestuur van het Máxima Medisch Centrum
- Michel van Leeuwen - directeur Artificiële Intelligentie bij het ministerie van Justitie en Veiligheid

In het afgelopen jaar is Evelien Bongers toegetreden tot de Raad van Toezicht. Zij vervangt daarmee Albert van Esterik die jarenlang in de Raad van Toezicht heeft gezeten. We bedanken Albert voor zijn waardevolle bijdrage en inzet voor Z-CERT. Carlijn de Ruijter heeft op 11 maart 2025 de voorzittersrol van Albert overgenomen.

De RvT komt ten minste vier keer per jaar bijeen.

Cybersecurity highlights

Cybersecurity highlights

Z-CERT draait om cybersecurity en onze experts op dat gebied zitten vooral in het team Operations. Het team is in 2025 gegroeid met 8 nieuwe collega's tot 29 mensen. Deze forse uitbreiding is belangrijk als voorbereiding op de uitvoering van de wettelijke CSIRT-taken die we krijgen vanwege de Cyberbeveiligingswet.

Het team Operations is in 2024 gestart met het werken in een Operationeel KernTeam (OKT). Deze manier van werken werpt zijn vruchten af omdat het ons helpt om sneller en efficiënter op incidenten en dreigingen te reageren. Naast het werken met een OKT, is daar in 2025 het werken in drie subteams bij gekomen. Het gaat om teams op het gebied van Incident Response & Testing, Monitoring & Scanning en Cyber Threat Intelligence.

De vorming van die teams is deels om de druk bij het management te verminderen, maar vooral ook om efficiënter te werken en specialisaties binnen het cybersecurity-terrein mogelijk te maken. De ontwikkelingen in cybersecurity en de steeds meer geavanceerde cyberaanvallen vragen om specialistische cybersecurity-kennis en -ervaring.

Incident response-inzet

In 2025 heeft Z-CERT een aanbesteding op het gebied van incident response

Cybersecurity highlights - vervolg

afgerond. Er zijn vier marktpartijen geselecteerd die zorgpartijen kunnen bijstaan op het gebied van incident response als er sprake is van een cyberincident.

Als er geen incidenten zijn, willen we de incident response-capaciteit binnen Z-CERT inzetten voor het uitvoeren en begeleiden van cybersecurity testen, zoals HART (Help Anderen Realistisch Testen) en ZORRO. Bij die laatste gaat het om een gesimuleerde aanval waarbij een externe partij onderzoekt hoe goed een zorginstelling, of een onderdeel daarvan, bestand is tegen hackers (red teaming).

HART is daarentegen speciaal bedoeld voor zorginstellingen die nog weinig ervaring hebben met beveiligingstesten. Tijdens een HART-sessie komt een team van Z-CERT op locatie en voeren we samen met een zorgorganisatie een eenvoudige test uit. Dit helpt zorginstellingen om beter te begrijpen waar hun kwetsbaarheden liggen en wat ze kunnen verbeteren.

Geautomatiseerd scannen

Het uitvoeren van cybersecurity testen is een belangrijk speerpunt geworden, net zoals het uitvoeren van geautomatiseerde scans bij zorginstellingen. Z-CERT heeft in 2025 ruime ervaring en kennis kunnen opdoen met het uitvoeren van de geautomatiseerde scanningdienst EASM (External Attack Surface Management). Hiermee zijn in 2025 ruim 2.000 issues aan het licht gebracht.

Omdat OpenKAT, de open-source variant van onze scantool, nog in ontwikkeling is en niet aan de specificaties voldeed zijn we in 2024 een EASM-dienst gestart met een alternatieve scanapplicatie. Z-CERT streeft ernaar om op de langere termijn een open-source-oplossing voor de EASM-dienst in te zetten.

Opvallende gebeurtenissen

Er zijn twee gebeurtenissen die veel tijd en capaciteit hebben gekost in 2025; dat waren de NAVO-top en het datalek bij Clinical Diagnostics.

In juli kreeg het medisch laboratorium Clinical Diagnostics te maken met een cyberaanval waarbij hackers toegang kregen tot een grote hoeveelheid gevoelige patiëntgegevens, waaronder naam- en adresgegevens, BSN-nummers en medische testuitslagen.

Dit was een uitzonderlijk incident omdat het heel veel mensen trof onder wie honderdduizenden vrouwen die hebben meegedaan aan het bevolkings-onderzoek naar baarmoederhalskanker. Hackers dreigden die gegevens

Cybersecurity highlights - vervolg

openbaar te maken via het dark web. Vanwege het incident werd er binnen Z-CERT in augustus opgeschaald. Z-CERT heeft extra capaciteit ingezet om zorginstellingen te ondersteunen bij het beoordelen van mogelijke risico's, het beantwoorden van vragen en het delen van actuele dreigingsinformatie.

De opschaling was voor onszelf en voor betrokken partijen een duidelijk signaal dat goede processen voor incident response van groot belang zijn. We hebben geleerd hoe belangrijk heldere communicatie, snelle coördinatie en nauw contact met ketenpartners in dergelijke situaties zijn. Deze inzichten nemen we mee in de verdere professionalisering van onze dienstverlening.

Z-CERT en de NAVO-top

Eerder in het jaar was Z-CERT druk met de voorbereidingen op de NAVO-top. Een groot internationaal evenement waar veel aandacht en belangstelling uit het binnen- en buitenland voor was.

In aanloop naar de NAVO-top in Den Haag op 24 en 25 juni heeft Z-CERT zich voorbereid op mogelijke cyberincidenten, met name bij de leden van het Netwerk Acute Zorg West (NAZW). Dit begon in januari 2025 door een dreigingsanalyse te schrijven voor de Nederlandse zorgsector. Hierin zijn de door het NCSC opgestelde meest waarschijnlijke en de worst-case scenario's vertaald naar de context van de nationale en regionale zorgsector. Deze scenario's zijn met leden van het NAZW via table-top sessies doorlopen, wat enkele nieuwe inzichten en knelpunten bij betrokken zorgorganisaties heeft opgeleverd. Daarnaast zijn binnen Z-CERT crisisplannen opgesteld en geoefend.

Tijdens de week van de NAVO-top zijn verschillende Z-CERT collega's volledig gefocust geweest op het monitoren van mogelijke dreigingen en incidenten rondom de NAVO-top. Dit had ook impact op de overige collega's die de dagelijkse operationele diensten bleven draaien. Gelukkig hebben zich tijdens de NAVO-top geen noemenswaardige cyberincidenten voorgedaan. Wel zorgde onder andere een telefoonstoring en een DDoS-aanval op niet-zorgentiteiten voor enige extra spanning.

We hebben organisaties die mogelijk doelwit konden zijn van ontwrichtende activiteiten geïnformeerd en dagelijks op de hoogte gehouden van de ontwikkelingen. Het resultaat van alle voorbereidingen was dat we met vertrouwen aan de NAVO-top begonnen en dit met enthousiasme hebben doorgemaakt.

Het cybersecurity jaar van Z-CERT in cijfers

5
operational alerts
(7 in 2024)

23
high/high alerts
(18 in 2024)

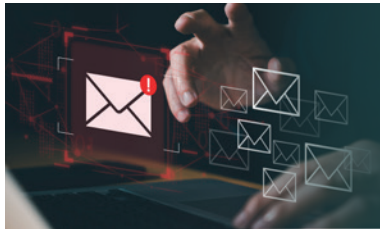
136
incidentregistraties
(139 in 2024)

92
CVD-meldingen
(155 in 2024)

183
onderzoeken
(266 in 2024)

460
basis advisories
(729 in 2024)

111
medische advisories
(48 in 2024)



48
infoberichten
(45 in 2024)

‘Een dienst op twee locaties tegelijkertijd laten draaien, is nog een behoorlijke klus’

Interview met Bart Orbons, Senior DevOps Engineer

Wat is jou opgevallen in het afgelopen jaar?

‘De groei van de organisatie is wel het meest markant. Maar er is meer veranderd binnen Z-CERT. Natuurlijk de overgang naar de verschillende Z-CERT labels, de wettelijke taak en de verantwoording die we moeten afleggen richting het ministerie van VWS. Dat heeft effect op de organisatie. Maar, en dat vind ik het mooie van deze organisatie, de sfeer van samenwerken en de gedrevenheid waarmee we allemaal de schouders eronder zetten, blijft onveranderd.’

Waar is het IT-team mee bezig geweest?

‘Als IT-team wilden we in 2025 ervoor zorgen dat we ons datacenter zouden verdubbelen. We vinden dat we onze dienstverlening veilig, vertrouwd en functioneel moeten leveren. Dus daarom moest het datacenter redundant worden. Dat klinkt als twee keer hetzelfde neerzetten en dan ben je er wel, maar helaas is dat echt wel een grote verandering. Ervoor zorgen dat een dienst op twee locaties tegelijkertijd draait, is nog een behoorlijke klus.’

Interview - vervolg

Wat merken jullie van de Cyberbeveiligingswet?

'We zijn nog bezig met de ontwikkeling van de Z-CERT portal die we grotendeels door externen hebben laten bouwen. Die portal heeft te maken met de aanmeldingen van Cyberbeveiligingswet-entiteiten die via het NCSC bij ons binnenkomen. Het is een voorbeeld dat laat zien dat de Cyberbeveiligingswet direct niet zoveel impact heeft voor ons team, maar dat de wensen die voortvloeien uit de Cyberbeveiligingswet indirect wel veel impact hebben.'

Wat zijn je ambities voor 2026?

'Mijn ambitie voor 2026 is om in het team te gaan werken aan het overdragen van kennis en kunde, zodat we elkaar beter kunnen ondersteunen in het werk dat we doen. En verder willen we andere teams helpen met hun uitdagingen. Het afgelopen jaar hebben we ons erg gericht op het verbeteren van onze eigen uitdagingen. Dat was nodig, maar soms wel hinderlijk voor de andere teams. Een voorbeeld is dat het af en toe zo druk is op kantoor dat je op zoek moet naar een werkplek op kantoor. Daar gaan we Z-CERT in 2026 mee helpen.'

In het **Cybersecuritybeeld voor de zorg 2025** bieden we inzicht in de huidige staat van cyberveiligheid in de zorg. We beschrijven de lessen die we het afgelopen jaar hebben geleerd en geven tips en handreikingen die kunnen helpen bij een beter digitaal beschermde zorgsector.

Deelnemers en samenwerkingen

Deelnemers en samenwerkingen

Het aantal zorginstellingen dat is aangesloten bij Z-CERT, door ons aangeduid als deelnemers, is in 2025 verder gegroeid. Het aantal betalende deelnemers steeg in één jaar tijd van 358 naar 391. Deze toename laat zien dat steeds meer zorgorganisaties het belang van cyberweerbaarheid inzien en er actief mee bezig zijn.

In 2025 heeft Z-CERT daarnaast voor het eerst te maken gekregen met zogenoemde entiteiten. Dit zijn organisaties die aan de Cyberbeveiligingswet (Cbw) moeten voldoen zodra deze in werking treedt. Omdat de NIS2-richtlijn op dit moment nog niet is omgezet in Nederlandse wetgeving, beschikken deze entiteiten wel over bepaalde rechten, maar nog niet over formele plichten. Om van deze rechten gebruik te kunnen maken, is registratie bij Z-CERT noodzakelijk.

Sinds 17 oktober 2024 hebben 153 organisaties zich bij Z-CERT geregistreerd als entiteit. Ongeveer de helft van deze organisaties (60) was al bekend bij Z-CERT als deelnemer. Deze zorginstellingen bereiden zich dus al tijdig voor op de aankomende wettelijke verplichtingen.

Wat vinden anderen van Z-CERT?

In 2025 hebben we voor de derde keer een klanttevredenheidsonderzoek (KTO) laten uitvoeren. De klanttevredenheid bleef ongeveer net zo hoog als vorig jaar: 8.4 (8.2 in 2024). De aangesloten zorgorganisaties zijn met name tevreden over de deskundige en betrouwbare dienstverlening van Z-CERT. Uit het onderzoek blijkt verder dat de Net Promoter Score (NPS) is gestegen naar 56, vergeleken met 48 in het jaar daarvoor. Als tip krijgt Z-CERT mee dat het 'vooral met praktische handvatten moeten blijven inspelen op de actualiteit, zoals de Cyberbeveiligingswet en AI Act'.

Kennisdeling

Een belangrijk deel van het werk van Z-CERT berust op kennisdeling. Een voorbeeld daarvan is de maturity scan die in 2025 is bijgewerkt en geactualiseerd volgens de nieuwe NEN 7510-2024 normering.

Kennisdeling gebeurt niet in de laatste plaats tijdens fysieke evenementen. We zijn in 2025 een aantal keer prominent naar buiten getreden. Dit hebben we gedaan met onder meer met een bierviltje waarop eenvoudig staat uitgelegd hoe zorginstellingen hun volwassenheid kunnen meten op het gebied van oefenen en testen van hun cybersecurity. De bierviltjes hebben we bijvoorbeeld uitgedeeld tijdens de beurs Zorg&ICT waar we voor het eerst aanwezig waren met een eigen stand.

In november hebben we Z-CERT live! on tour georganiseerd. Dit was voor het eerst een evenement dat op vier locaties tegelijk in Nederland plaatsvond.

Deelnemers en samenwerkingen - vervolg

Het thema was 'omgaan met kwetsbaarheden'. Vanuit Z-CERT wilden we het gesprek hierover op gang brengen, inzichten met elkaar delen en collega's verbinden en elkaar versterken op het gebied van security. Hoewel een evenement op deze manier een proef was, is het zo goed ontvangen dat we deze formule zeker gaan herhalen.

Samenwerkingen

Voor entiteiten en deelnemers hebben we diverse publicaties uitgebracht. Ook hebben we 11 webinars georganiseerd, samen met deelnemers en partners zoals de Autoriteit Persoonsgegevens en Informatieveilig Gedrag in de Zorg.

Samen met een aantal aangesloten zorginstellingen heeft Z-CERT een actieve rol gespeeld in de ontwikkeling van CYRA Zorg. Dit is een instrument waarmee zorginstellingen beter inzicht krijgen in de digitale weerbaarheid van hun leveranciersketen. We hebben in navolging van de eerdere pilot met CYRA (Cyber Rating) een uitbreiding mogelijk gemaakt waarmee het model specifiek voor de zorg toepasbaar is.

Vooruitblik 2026

Per 1 januari 2026 zijn we gestart met het werken met twee labels (CSIRT en Academy) in aanloop naar de Cyberbeveiligingswet. We zijn druk bezig om bestaande overeenkomsten met zorginstellingen om te zetten naar het nieuwe model van dienstverlening. Bij die nieuwe dienstverlening past ook een nieuwe rol van Z-CERT en daarbij passen nieuwe kernwaarden (verbindend en daadkrachtig).

Omdat belangrijke en essentiële entiteiten vanuit de Cyberbeveiligingswet bij Z-CERT aangemeld moeten zijn, zijn we druk bezig met de ontwikkeling van een selfservice portal, genaamd MijnZ-CERT. De aangesloten zorgorganisaties moeten via de selfservice portal zelf hun gegevens en diensten bij Z-CERT kunnen beheren. Met deze portal willen we meer diensten aan een groter aantal organisaties kunnen aanbieden. En we werken aan een heel nieuwe dienst namelijk een simulatie waarmee je cyber-investeringsscenario's kunt simuleren.

‘De hype rondom de NAVO-top en het continu waakzaam zijn was leuk’

Interview met Bas Molenaar, Security Support Specialist

Bas is Security Support Specialist bij Z-CERT. Dat betekent dat hij regelmatig contact heeft met zorginstellingen bij cyberincidenten of juist om ze te helpen deze te voorkomen met een van de adviezen of diensten van Z-CERT.

Hij werkt nu bijna vier jaar bij Z-CERT en in die tijd is er veel veranderd in de organisatie, vertelt hij. ‘Sinds ik bij Z-CERT werk, is er al heel veel veranderd. We zijn bijvoorbeeld in die tijd naar een andere verdieping in Amersfoort verhuisd en bijna elke maand verwelkomen we nieuwe collega’s omdat we ons voorbereiden op onze wettelijke taak.’

‘Gelukkig is Z-CERT nog wel het bedrijf gebleven waar iedereen normaal met elkaar kan praten. Je leest vaak dat kleine bedrijven die ‘snel’ groeien hun identiteit kwijtraken. Ook bestaat het gevaar dat het persoonlijke verdwijnt of dat de korte lijntjes vervagen. Dat vind ik bij Z-CERT niet het geval.’

Preventie

Bij Z-CERT maakt Bas allerlei situaties mee waaronder ook crisissituaties bij zorginstellingen die te maken hebben met cyberdreigingen. ‘Niet alleen zorginstellingen kunnen oefenen om voorbereid te zijn op crisissituaties.’

Interview - vervolg

Bij Z-CERT doen we dat zelf ook. Een goed voorbeeld daarvan was in 2025 de NAVO-top in Den Haag. 'De hype die eromheen zat en het continu waakzaam zijn om direct in actie te kunnen komen als dat moet, dat was leuk. Het was gewoon speciaal.'

Bas is binnen Z-CERT ook een van de preventiemedewerkers die erop let dat de werkomgeving veilig en gezond is. 'In dat kader hebben we in 2025 in ieder geval bereikt dat we voor iedereen die dat wilde een Preventief Medisch Onderzoek hebben geregeld.'

Als hij kijkt naar 2026 verwacht Bas bijna net zo'n grote verandering als in de aanloop naar de Cyberbeveiligingswet. 'We zullen een meer gestructureerde werkwijze moeten hanteren en daarvoor is ons team de afgelopen tijd al hervormd.'

Eenvoudige tips

Als we Bas vragen naar een gouden advies, dan weet hij direct iets. Het gaat over de contacten die Z-CERT met de zorginstellingen onderhoudt. 'Zorg dat je contactgegevens in ons systeem bijgewerkt zijn. In tijden van acute dreiging is het zeer vervelend als de contactgegevens niet blijken te kloppen. Het hebben van de juiste contactgegevens kan kostbare tijd schelen in crisissituaties.'

Dat kan al heel eenvoudig, legt hij uit. 'Leg bijvoorbeeld ook een notitie neer bij de receptie met de boodschap dat als Z-CERT belt, dat er standaard door-verbonden moet worden met afdeling X.'

'Tot slot vinden wij het ook fijn om reacties op e-mails te ontvangen. Een reactie op een mail kan ook al zijn 'Dankjewel, gelezen, gaan ermee aan de slag'. Het hoeven geen hele boekwerken te zijn.'

Interne ontwikkelingen

Interne ontwikkelingen

Het jaar 2025 stond voor Z-CERT in het teken van verdere professionalisering en versterking van onze organisatie. We hebben belangrijke stappen gezet om onze interne processen, governance en systemen toekomstbestendig te maken. Deze ontwikkelingen dragen bij aan onze rol als vertrouwde partner in cybersecurity voor de zorgsector. En het is onderdeel van onze voorbereiding op de wettelijke taken die in werking treden als de Cyberbeveiligingswet van kracht wordt. Stichting Z-CERT is hierbij formeel aangewezen als CSIRT voor de zorg.

Medezeggenschap en informatieveiligheid

De verdere professionalisering blijkt onder meer uit de Ondernemingsraad die per 1 januari 2025 formeel van start is gegaan. Medezeggenschap is daarmee een structureel onderdeel van onze organisatieprocessen geworden. Bovendien draagt het bij aan de transparantie van de organisatie en betrokkenheid van collega's.

Als expertisecentrum voor cybersecurity is onze eigen informatieveiligheid uiteraard een topprioriteit. In 2025 hebben we een interne crisisoefening uitgevoerd om goed voorbereid te zijn op eventuele crisissituaties. Daarnaast zijn er meerdere sessies over verschillende security-onderwerpen geweest om de kennis en de bewustwording van de medewerkers hoog te houden.

In 2025 hebben wij binnen de organisatie een nieuwe beveiligingsmaatregel geïmplementeerd: de introductie van FIDO2 voor aanmeldingen binnen onze eigen netwerkomgeving. Hiermee versterken we de authenticatieprocessen en verhogen we de algehele digitale weerbaarheid.

Z-CERT heeft het afgelopen jaar ook weer een tussentijdse audit voor ISO 27001 doorlopen. De maatregelen die we nemen om aan de ISO-norm te voldoen, maken ons beter bestand tegen risico's en laten zien dat we blijven werken aan goede naleving van de regels (compliance). Daarnaast zijn we sinds 2025 ook houder van een SIM3-certificaat, wat ons niveau als CSIRT (internationaal) erkent. SIM3 staat voor Security Incident Management Maturity Model. Deze certificering wordt sinds 2010 onder andere gebruikt in het Europese CSIRT netwerk. Het wordt wereldwijd erkend door bijvoorbeeld ENISA en FIRST.

Wij hebben de kennis en kunde van onze medewerkers ingezet voor een Bug Bounty hunt (=pentest) op onze eigen website. Dit heeft een aantal inhoudelijke en soms onverwachte resultaten opgeleverd. De bevindingen zijn inmiddels verwerkt en opgelost. Al onze beveiligingsmaatregelen hebben geleid tot een 100% score op internet.nl waarmee we opnieuw een oorkonde hebben verdiend.

Interne ontwikkelingen - vervolg

Technologische verandering

Als voorbereiding op de wettelijke taak die Z-CERT krijgt met de invoering van de Cyberbeveiligingswet, hebben we hard gewerkt aan het verhogen van de beschikbaarheid van de on-premise IT-omgeving. Er is een tweede datacenter waar de volledige, geautomatiseerd beheerde infrastructuur draait, zodat we beter zijn voorbereid op storingen. Diverse applicaties zijn nu redundant uitgevoerd en kunnen benaderd worden op twee locaties.

Nieuw is ook dat het IT-team het procesmatig werken met Integrated Service Management (ISM) heeft geïmplementeerd. ISM is een populaire gestandaardiseerde managementmethode om onze IT-dienstverlening en IT-servicemanagement beter te organiseren. Hierdoor wordt onze dienstverlening meer voorspelbaar en aantoonbaar. Om klaar te zijn voor de Cyberbeveiligingswet heeft het IT-team veel tijd en aandacht besteed aan de ontwikkeling van de selfservice portal MijnZ-CERT en met het automatiseren van de instroom van entiteiten die zich bij het NCSC hebben aangemeld. En met het oog op de geopolitieke ontwikkelingen, is er een plan gemaakt om onze afhankelijkheden te verminderen van grote aanbieders van clouddiensten die gevestigd zijn buiten de EU. We verwachten in 2026 te starten met het uitvoeren van dat plan.

Data & analytics

In 2025 heeft Z-CERT stevige stappen gezet in het professionaliseren van het datalandschap. We willen een toekomstbestendig Data & Analytics-fundament bouwen en hebben de basisprincipes van datagovernance neergezet. Het afgelopen jaar heeft het IT-team gewerkt aan een eerste, heldere en bruikbare versie van Kernregistraties Z-CERT. Hiermee is een structurele beweging gestart richting datagedreven werken binnen de organisatie.

We hebben in 2025 belangrijke stappen gezet om onze gegevens beter en slimmer te organiseren. Daarnaast is er gewerkt aan de opbouw van een samenhangend datalandschap. We hebben een eerste duidelijke beschrijving gemaakt van de belangrijkste gegevens die we binnen Z-CERT gebruiken en wie waarvoor verantwoordelijk is. Ook is in kaart gebracht welke informatie het management nodig heeft. Vervolgens hebben we een passend platform gekozen om met data te werken en hebben daarop de eerste versie van een organisatiebreed datamodel ontwikkeld. De eerste dashboards op dit nieuwe fundament zijn al in gebruik, en we bereiden nu de stap naar meer automatische en actuele rapportages voor. Zo groeien we stap voor stap naar een organisatie die steeds beter wordt ondersteund door betrouwbare informatie.

HR en organisatieontwikkeling

In de loop van het jaar is het personeelsbestand verder gegroeid door gerichte werving en selectie. Dankzij een zorgvuldig ingericht onboarding-proces is deze uitbreiding soepel in de organisatie geïntegreerd.

Interne ontwikkelingen - vervolg

Daarnaast blijft veilig en gezond werken een belangrijk aandachtspunt. In 2025 resulteerde dit onder meer in het aanbieden van het eerste Preventief Medisch Onderzoek (PMO), waaraan enkele tientallen medewerkers hebben deelgenomen.

Instroom:
16 medewerkers

Uitstroom:
Geen vaste medewerkers

Totaal aantal vaste medewerkers*:
65 medewerkers 28% vrouw / 72% man

* = Totaal aantal vaste medewerkers op 31 december 2025.

Inkoop en professionalisering

Z-CERT heeft in 2025 de inkoopprocessen naar een hoger niveau getild. Zo is er een inkoopbeleid opgesteld en zijn er aanbestedingstrajecten gestart en uitgevoerd. Daarnaast is een Dynamisch Aankoopsysteem (DAS) ingericht en in gebruik genomen. Daarmee wordt het inkoopproces voor inhuurkrachten flexibeler en transparanter en kunnen opdrachten sneller en efficiënter worden gegund.

Bedrijfsvoering, financiën en systemen

In het vierde kwartaal van 2025 heeft PwC een zogenoemde uitvoeringstoets uitgevoerd. Het doel van deze toets is om op objectieve wijze vast te stellen wat de financieringsbehoefte van Z-CERT is, rekening houdend met de wettelijke taken die in het kader van de Cyberbeveiligingswet aan ons worden toegewezen. Een uitvoeringstoets biedt inzicht in de benodigde middelen om de organisatie haar taken effectief en efficiënt te laten uitvoeren. Het vormt daarmee een belangrijke basis voor toekomstige besluitvorming en verantwoording richting stakeholders.

Afsluiting

Met deze interne ontwikkelingen heeft Z-CERT in 2025 een solide basis gelegd voor de toekomst. We zijn beter voorbereid op onze wettelijke taak onder de Cyberbeveiligingswet en blijven investeren in professionalisering, veiligheid en transparantie. Deze inspanningen stellen ons in staat om onze missie - het digitaal veiliger maken van de zorg - met nog meer kracht en effectiviteit uit te voeren. Per 1 januari 2025 is een nieuw systeem in gebruik genomen, waarmee financiële, HR- en CRM-processen beter worden ondersteund. Gedurende het jaar is de functionaliteit verder doorontwikkeld en geoptimaliseerd. Ook is een basis-urenregistratie ingevoerd om verantwoording en transparantie in projecten te verbeteren.

‘Z-CERT werkt toe naar een volwassener aanpak’

Interview met Kriston Verkerk, Business Consultant

Kriston is een van de nieuwe Business Consultants. Hij is in september 2025 bij Z-CERT gekomen. En hoewel hij relatief kort bij de organisatie zit, heeft hij al heel wat meegekregen van de veranderingen die zich voltrekken. ‘We zijn overgegaan naar twee labels (CSIRT en Academy) en het Operations team werkt nu met drie subteams.’

Wat maakt het jaar 2025 bijzonder bij Z-CERT?
‘Ik zie nog altijd veel ad-hocwerk, maar tegelijkertijd wordt er stevig ingezet op een meer pragmatische werkwijze. Z-CERT werkt toe naar een volwassener aanpak, waarbij de onderscheidende rol van de twee labels het meest opvalt. Deze nieuwe werkwijze is noodzakelijk vanwege de sterke toename van het aantal entiteiten dat op ons af komt.’

Wat voor uitdaging levert dat op?
‘Door de komst van de Cyberbeveiligingswet sluiten organisaties (entiteiten) zich bij ons aan uit bepaalde subsectoren uit de zorg die tot nu toe nog wat minder bekend bij ons waren, zoals de medische technologie en de farmaceutische bedrijven.’

Als jij één advies aan zorginstellingen mag geven, welk advies zou dat zijn?
‘Begin met een goede basisbeveiliging voordat je je gaat verdiepen in specialistische beveiligingsmaatregelen. Dit bespaart veel tijd en geld op lange termijn.’

Merk, beleving en media

Merk, beleving en media

In 2025 hebben wij verdere stappen gezet in de professionalisering van onze communicatie, voortbouwend op de basis die in 2024 is gelegd. Het jaar stond in het teken van afronden, voorbereiden en verstevigen. Enerzijds rondden we de interne verandercommunicatie af die hoorde bij de voorbereiding op de nieuwe wettelijke taak onder de Cyberbeveiligingswet en de introductie van de labels CSIRT en Academy. Anderzijds werkten we gericht toe naar de toekomst van Z-CERT, waarin merkpositionering een steeds belangrijkere rol speelt.

Intern lag de focus in 2025 op verdere professionalisering en het aanbrengen van focus. De organisatie bereidde zich voor op grotere veranderingen in 2026, terwijl de dynamiek van het cybersecurity-domein onverminderd hoog bleef. Incidenten van toenemende schaal en complexiteit vroegen regelmatig om snelle en zorgvuldige communicatie. Met name het datalek bij Clinical Diagnostics Nederland heeft duidelijk gemaakt hoe belangrijk het is dat Z-CERT zichtbaar, herkenbaar en inhoudelijk sterk gepositioneerd is, zowel richting de zorgsector als in het publieke debat.

Merk

In 2025 zijn we gestart met een intensief traject voor merkpositionering. Dit traject is volledig intern uitgevoerd, met betrokkenheid van het managementteam en een brede werkgroep, onder begeleiding van de senior communicatieadviseur. Op basis van onderzoek, verkenning en toetsing is gewerkt aan het scherp formuleren van het merkverhaal en de positionering van Z-CERT.

In deze positionering is een bewuste beweging gemaakt om een organisatie te zijn die niet alleen ondersteunt, maar ook richting geeft. We staan naast de zorgsector, maar durven ook duidelijk te zijn wanneer dat nodig is. Vanuit onze expertise nemen we verantwoordelijkheid, geven we duiding bij complexe vraagstukken en maken we cybersecurity begrijpelijk en hanteerbaar voor de zorg.

In het verlengde van de merkpositionering zijn in het najaar van 2025 twee kernwaarden vastgesteld: daadkrachtig en verbindend. Deze kernwaarden geven richting aan hoe wij onze rol invullen. Daadkrachtig in ons handelen en in het tijdig en helder communiceren over dreigingen en incidenten. Verbindend in de manier waarop wij samenwerken met zorginstellingen, partners en elkaar, vanuit het besef dat digitale veiligheid in de zorg een gezamenlijke verantwoordelijkheid is. De merkpositionering is in 2025 vastgesteld en verkend en vormt een stevig inhoudelijk fundament. In 2026 brengen we deze positionering verder tot leven en maken we deze zichtbaar en voelbaar in communicatie, middelen en gedrag.

Merk, beleving en media - vervolg

Beleving

In 2025 lag de focus nog niet op cultuur- of gedragsverandering, maar wel op het versterken van consistentie en herkenbaarheid in onze communicatie. De in 2024 geïntroduceerde huisstijl en aangescherpte communicatiestijl zijn in 2025 verder doorgevoerd en beter geborgd in de organisatie. Dit zorgde voor meer samenhang in onze uitingen en een professionelere uitstraling naar buiten. Daarnaast is verder gewerkt aan de kwaliteit en samenhang van content. Door bewuste keuzes te maken in toon, vorm en inhoud ontstond meer rust en duidelijkheid in onze communicatie. Deze consistentie vormt een belangrijke randvoorwaarde voor het laden van het merk in de komende jaren.

Media

In 2025 was Z-CERT meer dan ooit zichtbaar in de media. Door het toenemende aantal ernstige cybersecurity-incidenten in de zorg werd onze expertise regelmatig gevraagd door journalisten en vakmedia. Z-CERT wordt steeds vaker gezien als een betrouwbare en inhoudelijke gesprekspartner bij actuele ontwikkelingen op het gebied van digitale veiligheid in de zorg.

De casus rondom het datalek bij Clinical Diagnostics Nederland was voor Z-CERT een belangrijk moment. De omvang en impact van dit incident vroegen om zorgvuldige en heldere communicatie. Het incident zorgde ervoor dat Z-CERT

Merk, beleving en media - vervolg

langdurig in de schijnwerpers kwam te staan als expertisecentrum. Met brede aandacht in landelijke kranten, online media en televisieprogramma's zoals EenVandaag en RTL Nieuws.

Social media

Ook op social media is in 2025 verder gebouwd op de ingezette professionalisering. LinkedIn bleef het belangrijkste kanaal, met een duidelijke focus op inhoudelijke en relevante content voor de zorg- en cybersecurity-sector. Voor het eerst is structureel ingezet op videocontent. Deze vorm van communicatie sluit goed aan bij onze doelgroep en draagt bij aan grotere zichtbaarheid en betrokkenheid. Daarnaast maken we actief gebruik van Mastodon en BlueSky.

Social media werd in 2025 vooral ingezet om de bestaande communicatiestijl vast te houden en verder te verfijnen.

Website

De in 2024 gelanceerde website is in 2025 inhoudelijk verder aangescherpt en strategischer ingezet. Er is meer dynamische content toegevoegd, onder andere in de vorm van blogs, waardoor actuele thema's en ontwikkelingen beter konden worden geduid.

Onze eerste podcast-reeks

In het voorjaar van 2025 is de Z-CERT-podcast *Zet 'm op* gelanceerd. Het eerste seizoen werd positief ontvangen binnen de cybersecurity-wereld met veel enthousiaste reacties. Tijdens het WHY hackerskamp zijn speciale zomerafleveringen opgenomen en in het najaar volgde een tweede seizoen. Voor 2026 is een derde seizoen in voorbereiding.

Conclusie en vooruitblik

2025 was een jaar van afronden, verstevigen en koers bepalen. De basis voor een duidelijke merkpositionering is gelegd en de communicatieve randvoorwaarden zijn verder op orde gebracht. Met een scherpere positionering, vastgestelde kernwaarden en een steeds sterkere zichtbaarheid in media en sector is Z-CERT goed voorbereid op de volgende fase. In 2026 brengen we het nieuwe Z-CERT-merk tot leven en zorgen we voor een consistente toepassing in communicatie, middelen en gedrag.

‘Het is gelukt om de beoogde groei te realiseren én mensen te behouden’

Interview met Eline Huijzendveld, Senior HR-Consultant

Eline werkt sinds oktober 2024 als Senior HR-Consultant bij Z-CERT. ‘Z-CERT is een organisatie die volop in beweging is. Niet alleen richting de deelnemers, maar ook intern in aanloop naar de Cyberbeveiligingswet en de labels. Die groei en professionalisering maakt het een mooie organisatie’, zo beschrijft ze. ‘We zijn dynamisch en toekomstgericht en het is fantastisch om daaraan bij te dragen.’ Het jaar 2025 staat voor haar vooral in het teken van samenwerking. ‘Bij belangrijke momenten, zoals incidenten of de NAVO-top, zie je hoe collega’s schouder aan schouder staan. Het is indrukwekkend om te zien met hoeveel passie en toewijding zij hun werk doen.’

Als HR-consultant weet Eline als geen ander dat Z-CERT in korte tijd flink is gegroeid in het aantal medewerkers. ‘Die snelle groei vraagt om aandacht voor onze cultuur. We willen de prettige werksfeer behouden en nieuwe collega’s goed laten landen. Bestaande medewerkers zetten zich daar graag voor in. Er is veel collegialiteit en betrokkenheid.’

Daarom is ze trots op wat er in 2025 is bereikt. ‘Het is gelukt om de beoogde groei te realiseren én mensen te behouden. Dat is te danken aan onze verbindende cultuur en fijne werkomgeving. Dat doen we echt samen.’

Ze kijkt dan ook met veel enthousiasme vooruit naar 2026. ‘Het wordt een jaar van verdere professionalisering, nieuwe dienstverlening en interne versterking van teams. Een jaar vol groei, verbinding en impact.’

Blik op de toekomst

Blik op de toekomst

Voor Z-CERT staat 2026 in het teken van volwassenwording. De basis staat. De keuzes zijn gemaakt. In dit jaar plukken we zichtbaar de vruchten van het intensieve opbouw- en veranderwerk van de afgelopen periode. We groeien naar een stabiele, volwassen organisatie met een duidelijke rol en verantwoordelijkheid in het zorglandschap.

Met de inwerkingtreding van de Cyberbeveiligingswet in 2026 gaat onze positie blijvend veranderen. In 2026 vervullen wij onze wettelijke taak als sectoraal CSIRT met overtuiging. Die wettelijke verankering geeft richting en vergroot onze impact. Tegelijkertijd vraagt het om een andere manier van werken: meer daadkracht, meer verbinding in de keten en een heldere afbakening van verantwoordelijkheden. Die verschuiving omarmen wij, met oog voor de praktijk van zorgorganisaties en het gezamenlijke doel: een digitaal veilige zorg.

In nauwe afstemming met het ministerie van VWS en in verbinding met Europese en internationale partners dragen wij bij aan een samenhangende aanpak van cyberweerbaarheid. Waarbij nationale én internationale ontwikkelingen elkaar versterken.

Dit jaar pakt Z-CERT nadrukkelijk positie als het expertisecentrum voor digitale veiligheid in de zorg. Een plek waar zorgorganisaties niet alleen terecht kunnen bij incidenten, maar ook voor duiding, kennis en inspiratie. De Z-CERT Academy draagt bij aan structurele kennisopbouw en professionalisering binnen de sector. Daarnaast zetten we de eerste gerichte stappen op innovatie, onder meer via Labs. Waar we samen met (internationale) partners vooruitkijken en nieuwe oplossingen verkennen.

Hand in hand

Intern is Z-CERT in 2026 een organisatie die weet waar zij vandaan komt en waar zij naartoe gaat. We zijn trots op wat is opgebouwd, op de mensen die dit mogelijk hebben gemaakt en op de energie waarmee we vooruitkijken. Professionaliteit en betrokkenheid gaan daarbij hand in hand. We blijven leren, verbeteren en onszelf bevragen. Juist omdat onze rol ertoe doet.

Het nieuwe jaar is daarmee geen eindpunt, maar een moment van stevigheid. Een jaar waarin Z-CERT staat als autoriteit, richting geeft waar nodig en verbindt waar het kan. Vanuit vertrouwen, met kennis van zaken en met een heldere opdracht: samen werken aan een digitaal veilige zorg. Nu en in de toekomst.

Financieel overzicht

Financieel overzicht

Aanbestedingsplicht

In 2025 is het team Bedrijfsvoering versterkt met de aanstelling van een controller en een inkoper. Deze uitbreiding van de organisatie is nodig geweest vanwege de voorbereiding op de Cyberbeveiligingswet en om een toekomstbestendige inrichting van de organisatie te garanderen. Daarnaast is de planning- en controlcyclus verder uitgebouwd, waardoor de basis voor sturing en verantwoording stevig is neergezet. Ook is in 2025 een administratiesysteem succesvol geïmplementeerd. Deze ontwikkelingen markeren een belangrijke stap in de verdere professionalisering van de financiële functie en ondersteunen een efficiënte en transparante bedrijfsvoering.

Omdat het merendeel van onze inkomsten afkomstig is uit subsidies zijn wij gehouden aan de verplichtingen die voortvloeien uit de Aanbestedingswet 2012. We passen daarom deze wet- en regelgeving structureel toe binnen onze inkoop- en aanbestedingsprocessen om transparantie, rechtmatigheid en doelmatigheid te waarborgen. Wanneer opdrachten boven de wettelijke drempelbedragen uitkomen wordt er Europees aanbesteed.

In het jaar 2025 zijn twee aanbestedingen succesvol afgerond. Voor de aanbesteding van inhuur van tijdelijk personeel gebruiken we het Dynamisch Aankoop Systeem (DAS). Dit proces verloopt soepel en er is een gezond aanbod aan kandidaten, waarvan inmiddels meerdere goede matches zijn geselecteerd. De tweede aanbesteding betrof dienstverlening voor AFAS ondersteuning en optimalisatie. Dankzij duidelijke wensen van Z-CERT heeft dit geleid tot scherpe aanbiedingen en aanzienlijke kostenbesparing.

Bekijk het overzicht op de volgende slide

Financieel overzicht - vervolg

Inkomsten

Overheidssubsidies	9.305.628
Deelnemersgelden	1.921.131
Totaal	11.226.759

Lasten

Personele lasten	
Loonlasten eigen personeel (incl. sociale lasten en pensioenlasten)	5.936.563
Vacatiegelden Raad van Toezicht	13.895
Totaal	5.950.458

Afschrijvingen materiële vaste activa	
Gebouwen en -terreinen	18.586
Inventarissen	11.542
Totaal	30.128

Overige lasten	
Overige personeelsbeloningen	790.920
Huisvestingslasten	190.098
Verkooplasten	37.324
Autolasten	14.600
Kantoorlasten	1.932.863
Algemene lasten	233.543
Activiteitenlasten	1.217.035
Totaal	4.416.383

Financiële baten en lasten	
Rentebaten	9.674

Totaal saldo van baten en lasten	**839.464**

Colofon

Colofon

De inhoud van dit jaarverslag 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.

We danken iedereen binnen Z-CERT die aan dit document heeft meegewerkt.

Redactie:
Edwin Feldmann, Tim Heijltjes, Wim Hafkamp, Daan Brinkhuis, Inge Timmerman, Elibart Gerritsen en Erik Burger

Vormgeving:
Björn Lansink - ontwerp & illustratie

Fotografie:
Evert van de Worp en Neeltje Meijler

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