TLP:GREEN

Netwerk en Informatie Beveiliging 2 – NIB2/NIS2

ZCERT
COMPUTER EMERGENCY RESPONSE TEAM VOOR DE ZORG

Mijn naam is

Auke Nicolaï

Business Consultant

- NFU, NVZ, ZKN, AZN, DCHA & pilot 1e lijn
- Secretaris Zorg-ISAC
- Secretaris European Health-ISAC

Inhoud

- Wie is Z-CERT
- Wat is de NIS2 en waarom is deze nodig
- Impact op zorginstellingen
- Impact op het CERT stelsel in Nederland
- Impact op Z-CERT en haar dienstverlening

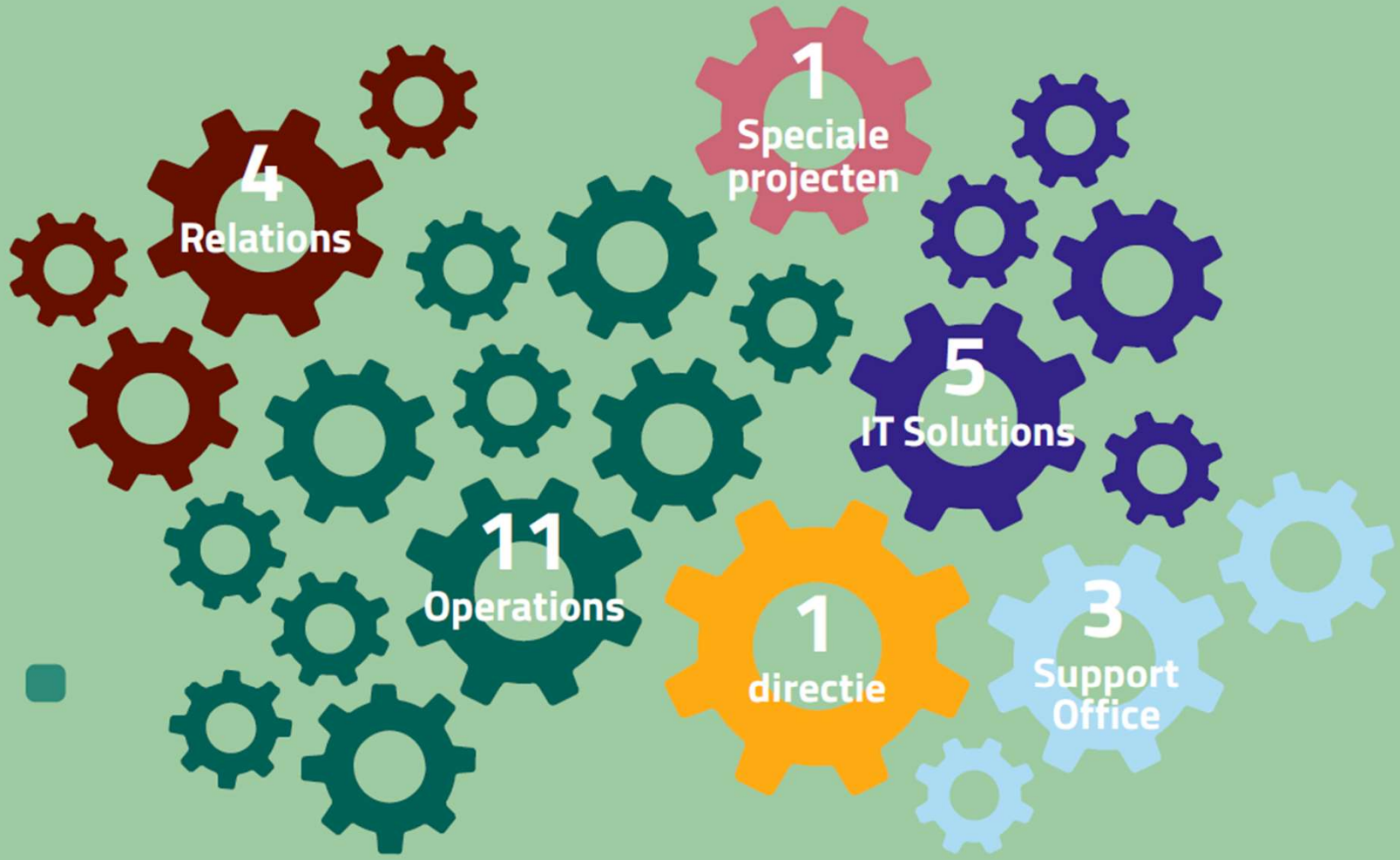
Z-CERT

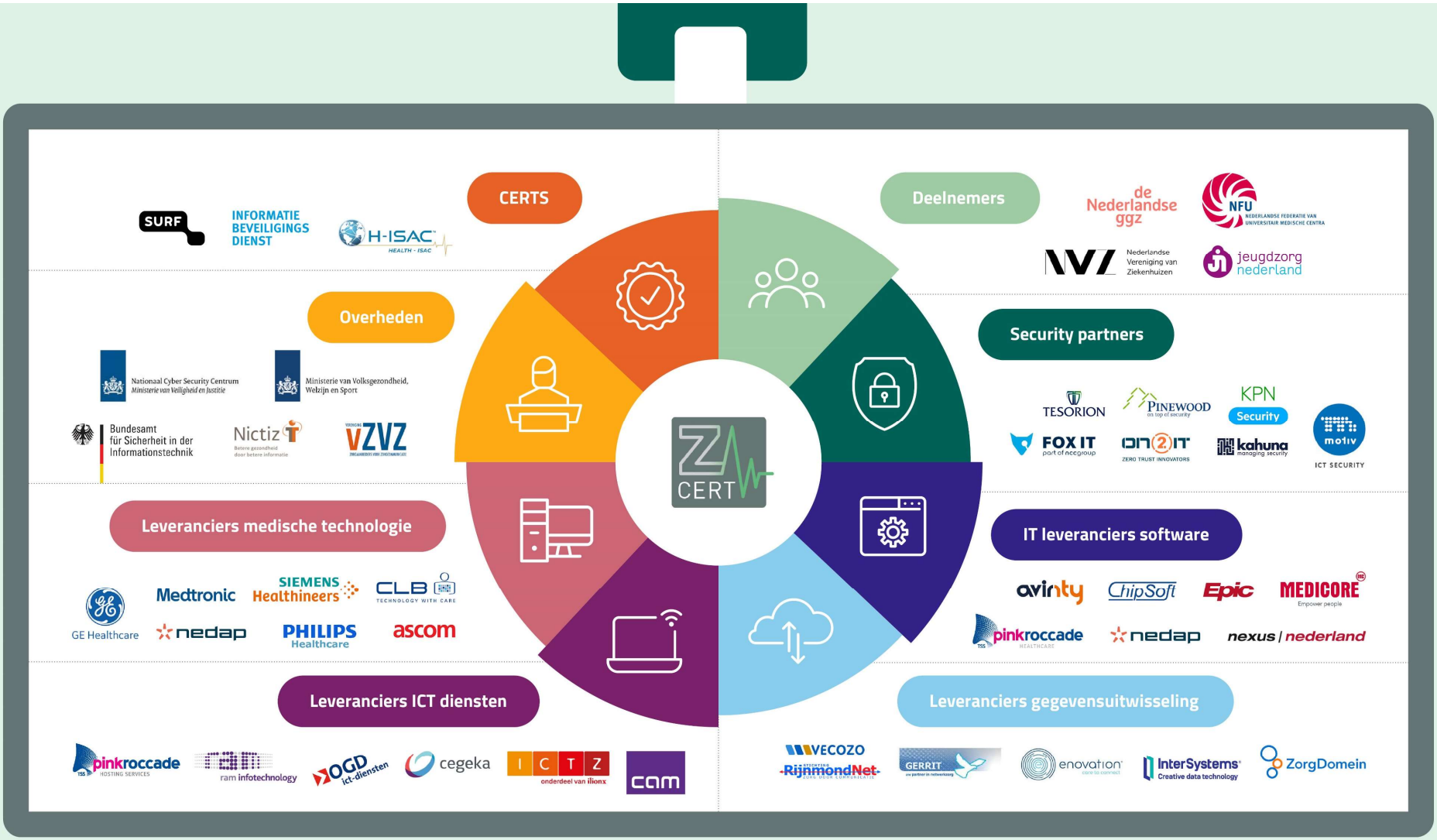
- is een onafhankelijke stichting zonder winstoogmerk
- opgericht in 2017 door en voor de zorgsector NFU, NVZ & De NL GGz
- nauwe betrokkenheid en stimulans vanuit VWS
- is aangemerkt als het expertisecentrum cybersecurity in de zorg
- versterkt de digitale veiligheid van de Nederlandse zorgsector door:
  - het verhogen van het beveiligingsbewustzijn
  - het duiden van cyber-dreigingen
  - voorkomen van cyber-incidenten
  - het mitigeren van de effecten van cyber-incidenten

Team

1 januari 2023
25 medewerkers
8 externen

1 januari 2022
20 medewerkers
7 externen





Disclaimer: aan de afbeelding kunnen geen rechten worden ontleend. De afbeelding geeft het speelveld weer waarin Z-CERT zich begeeft. Z-CERT heeft niet de intentie een compleet beeld te geven of het beeld te scheppen dat Z-CERT een (contractuele) samenwerking met genoemde partijen heeft.

Deelnemers

315
in totaal

- **UMC** (7)
- **Ziekenhuizen** (70)
- **Categoraal + Revalidatie** (34)
- **GGZ** (64)
- **Gehandicaptenzorg** (10)
- **Ouderenzorg** (26)
- **Jeugdzorg** (39)
- **Ambulancezorg** (4)
- **Diagnostische laboratoria** (7)
- **GGD** (27)
- **DCHA*** (6)
- **Zelfstandige klinieken** (6)
- **Atypisch**** (11)
- **Overig** (4)

Wat is de NIS2

- Network and Information Security 2 Directive (Wbni)
- Wetgeving om de EU veiliger te maken op cybersecurity gebied
- Nationale cybersecurity strategie en kaders voor crisisbeheer
- Samenwerking nationaal en internationaal niveau
- Maatregelen en rapportageverplichtingen voor ‘belangrijke en essentiële entiteiten’

Waarom een NIS 2

NIS1 is anders gevallen dan gehoopt

- Vrijblijvendheid invulling van NIS1 lidstaten
- Onvoldoende toekomstig bestendig (supply chain risico's / leveranciers) en te weinig specifieke maatregelen
- Te weinig toezicht / onvoldoende meldingen
- Te weinig samenwerking

Voor wie geldt de NIS2

- NIS2 geldt voor **alle instellingen > 50 FTE en/of > 10 miljoen omzet** in een aantal belangrijke sectoren, waaronder **de zorg**, ongeacht of de sector wel of niet vitaal is verklaard volgens de Nederlandse vitaal systematiek.
- Uitbreiding van sectoren waarvan entiteiten onder de richtlijn vallen
- Onderscheid essentiële & belangrijke entiteiten
- Verplichtingen en toezicht nader voorgeschreven
- Verantwoordelijkheid bestuur

Impact op zorginstellingen

- Verplichte maatregelen
- Meldplicht van incidenten
- Risico op boetes
- Mogelijke verplichting gebruik van gecertificeerde ICT-producten en diensten

Impact op zorginstellingen - maatregelen

Artikel 21, lid 1: De lidstaten zorgen ervoor dat essentiële en belangrijke entiteiten passende en *evenredige technische, operationele en organisatorische maatregelen nemen* om de risico's voor de beveiliging van de netwerk- en informatiesystemen die deze entiteiten voor hun werkzaamheden of voor het verlenen van hun diensten gebruiken, te beheren en om incidenten te voorkomen of de gevolgen van incidenten voor de afnemers van hun diensten en voor andere diensten te beperken.

Kijkende naar de AVG zal de toezichthouder zeer vermoedelijk de NEN 7510 aanhouden om te beoordelen of '*evenredige technische, operationele en organisatorische maatregelen*' genomen zijn.*

* https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/besluit_haga_-_ter_openbaarmaking.pdf - pagina 11

Impact op zorginstellingen – maatregelen

Beleid risicoanalyse- en beoordeling

Incidentbehandeling

Bedrijfscontinuïteit/back-ups

Toeleveringsketen

Kwetsbaarheden

Cyberhygiëne / basispraktijken

Cryptografie / encryptie

Assetmanagement / toegangsbeleid

Multifactor

Impact op zorginstellingen - maatregelen

Overweging 89 - basismaatregelen: Essentiële en belangrijke entiteiten moeten een breed scala aan basispraktijken op het gebied van cyberhygiëne toepassen, zoals:

- *zero trust-beginselen*
- *software-updates*
- *configuratie van apparaten*
- *netwerksegmentatie*
- *identiteits- en toegangsbeheer of gebruikersbewustzijn*
- *opleidingen voor hun personeel organiseren*
- *en het bewustzijn van cyberdreigingen, phishing of social engineering technieken vergroten*

Meldplicht incidenten

- Significante incidenten, als het:
  - Een ernstige operationele verstoring van de diensten of financiële verliezen voor de betrokken entiteit veroorzaakt of kan veroorzaken;
  - Andere natuurlijke of rechtspersonen heeft getroffen of kan treffen door aanzienlijke materiële of immateriële schade te veroorzake
- 1e ‘waarschuwing’ binnen 24 uur, melding binnen 72 uur, volledige rapportage binnen een maand
- Meldplicht van maatregelen aan dienstenontvangers (patiënten/cliënten) die ‘mogelijkerwijs door een significante cyberdreiging worden getroffen’ *

* Interessant feitje: In de draft NIS2 stond: ‘De lidstaten zorgen ervoor dat essentiële en belangrijke entiteiten de bevoegde autoriteiten of het CSIRT onverwijld in kennis stellen van **elke significante cyberbedreiging** die deze entiteiten vaststellen en die tot een significant incident **had kunnen leiden**. ’

Risico op boetes

- De toezichthouder, vermoedelijk de IGJ, anders de Rijksdienst Digitale Infrastructuur, mag:
  - Inspecties uitvoeren, scans, verzoeken om informatie, en meer
  - Specifieke maatregelen opleggen (bijv. gebruik MFA)
  - Een zorginstelling verplichten de aanbevelingen van een audit binnen een bepaalde termijn uit te voeren
  - Boeten opleggen

- Geldboeten van 10 miljoen of 2% van de totale wereldwijde omzet, afhankelijk van welk bedrag hoger is

Gecertificeerde ICT-producten en diensten

- Lidstaten *kunnen* eisen dat men gebruik maakt van gecertificeerde ICT-producten en diensten
- Met deze producten kunnen zorginstellingen aantonen dat ze voldoen aan maatregelen die worden geëist

Leveranciers, MSP’s, MSSP’s en meer

- Uitbreiding van essentiële aanbieders met ‘Aanbieders van beheerde (beveiligings)diensten’
- Informatie-uitwisseling tussen zorginstellingen, leveranciers en Z-CERT wordt daarmee een stuk makkelijker
- Makkelijker om eisen aan leveranciers te stellen
- Boetedruk ook op die leveranciers, en:
    - Referentielaboratoria
    - Onderzoeks- en ontwikkelingsactiviteiten m.b.t. geneesmiddelen
    - Vervaardigers van farmaceutische basisproducten en bereidingen
    - Vervaardigers van medische hulpmiddelen in het kader van volksgezondheid

Impact op het CERT-stelsel in Nederland

- Aantal organisaties onder WBNI van XXX naar 4500~
    - Waarvan zorg: 1500~
- Uitbreiding aantal subsectoren – zie vorige slide
- Verdeling van taken is nog onduidelijk
    - De ene sector is al beter gedekt door een CERT dan de ander (bijv. zorg vs ruimtevaart)
    - Verschillen tussen CERT's (bijv. hulp bij incident management vs forensisch onderzoek)

Impact op Z-CERT haar dienstverlening

- Forse toename deelnemers
- Financiering voor het uitvoeren van taken vanuit de overheid
- Op punten uitbreiding/verduidelijking van taken:
    - Verzamelen en analyseren van forensische gegevens, bovenop het verlenen van bijstand bij incidenten
    - Proactief scannen van zorginstellingen
    - Coördinatie van bekendmaking kwetsbaarheden aan zorginstellingen en leveranciers

Bijlage – koppeltabel maatregelen NIS2 – NEN 7510

NIS2	NEN 7510
beleid inzake risicoanalyse en beveiliging van informatiesystemen	7510-1 6.1 Maatregelen om risico's te beperken en kansen te benutten 7510-1 8.2 Risicobeoordeling van informatiebeveiliging
incidentenbehandeling	7510-2 16 Beheer van informatiebeveiligingsincidenten
bedrijfscontinuïteit, zoals back-upbeheer en noodvoorzieningenplannen, en crisisbeheer	7510-2 12.3 Back-up - volledig 7510-2 16.1.2 Rapportage van informatiebeveiligingsgebeurtenissen - gedeeltelijke dekking van crisis- en continuïteitsbeheer 7510-2 17 Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer - gedeeltelijke dekking crisis- en continuïteitsbeheer 7510-2 12.1.2 Wijzigingsbeheer - gedeeltelijke dekking crisis- en continuïteitsbeheer
de beveiliging van de toeleveringsketen, met inbegrip van beveiligingsgerelateerde aspecten met betrekking tot de relaties tussen elke entiteit en haar rechtstreekse leveranciers of dienstverleners	7510-2 14.2.7 Uitbestede softwareontwikkeling 7510-2 15.1.3 Toeleveringsketen van informatie- en communicatietechnologie
beveiliging bij het verwerven, ontwikkelen en onderhouden van netwerk- en informatiesystemen, met inbegrip van de respons op en bekendmaking van kwetsbaarheden	7510-2 14 Acquisitie, ontwikkeling en onderhoud van informatiesystemen 7510-2 12.6 Beheer van technische kwetsbaarheden
beleid en procedures om de effectiviteit van maatregelen voor het beheer van cyberbeveiligingsrisico's te beoordelen	7510-1 6.1 Maatregelen om risico's te beperken en kansen te benutten
basispraktijken op het gebied van cyberhygiëne en opleiding op het gebied van cyberbeveiliging	7510-2 bevat legio maatregelen, een groot deel waarvan als basispraktijken zouden kunnen worden bestempeld
beleid en procedures inzake het gebruik van cryptografie en, in voorkomend geval, encryptie	7510-2 10 Cryptografie
beveiligingsaspecten ten aanzien van personeel, toegangsbeleid en beheer van activa	7510-2 7 Veilig personeel 7510-2 8 Beheer van bedrijfsmiddelen 7510-2 9 Toegangsbeveiliging
wanneer gepast, het gebruik van multifactor-authenticatie- of continue-authenticatieoplossingen, beveiligde spraak-, video- en tekstcommunicatie en beveiligde noodcommunicatiesystemen binnen de entiteit	7510-2 9.4.1 Beperking toegang tot informatie (MFA) 7510-2 9 Toegangsbeveiliging Het tweede gedeelte (spraak, video, tekst) wordt niet in zoveel specifieke woorden gecovered in de 7510. Een deel kan je nog zien onder: 7510-2 15.1.3 Toeleveringsketen van informatie- en communicatietechnologie

Vragen?

Stichting Z-CERT
www.z-cert.nl

Bijlage impact op zorginstellingen – maatregelen*

a) beleid inzake risicoanalyse en beveiliging van informatiesystemen;

b) incidentenbehandeling;

c) bedrijfscontinuïteit, zoals back-upbeheer en noodvoorzieningenplannen, en crisisbeheer;

d) de beveiliging van de toeleveringsketen, met inbegrip van beveiligingsgerelateerde aspecten met betrekking tot de relaties tussen elke entiteit en haar rechtstreekse leveranciers of dienstverleners;

e) beveiliging bij het verwerven, ontwikkelen en onderhouden van netwerk- en informatiesystemen, met inbegrip van de respons op en bekendmaking van kwetsbaarheden;

f) beleid en procedures om de effectiviteit van maatregelen voor het beheer van cyberbeveiligingsrisico's te beoordelen;

g) basispraktijken op het gebied van cyberhygiëne en opleiding op het gebied van cyberbeveiliging;

h) beleid en procedures inzake het gebruik van cryptografie en, in voorkomend geval, encryptie;

i) beveiligingsaspecten ten aanzien van personeel, toegangsbeleid en beheer van activa;

j) wanneer gepast, het gebruik van multifactor-authenticatie- of continue-authenticatieoplossingen, beveiligde spraak-, video- en tekstcommunicatie en beveiligde noodcommunicatiesystemen binnen de entiteit.

Nuttige linkjes

- Tekst: https://eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=CELEX:32022L2555
- NCSC Impact Study: https://www.ncsc.nl/documenten/publicaties/2022/oktober/13/index
- EU Briefing: https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689333