



COMPUTER EMERGENCY
RESPONSE TEAM
VOOR DE ZORG



Cyber secure besturen in zorgnetwerken

Cyber secure besturen in zorgnetwerken





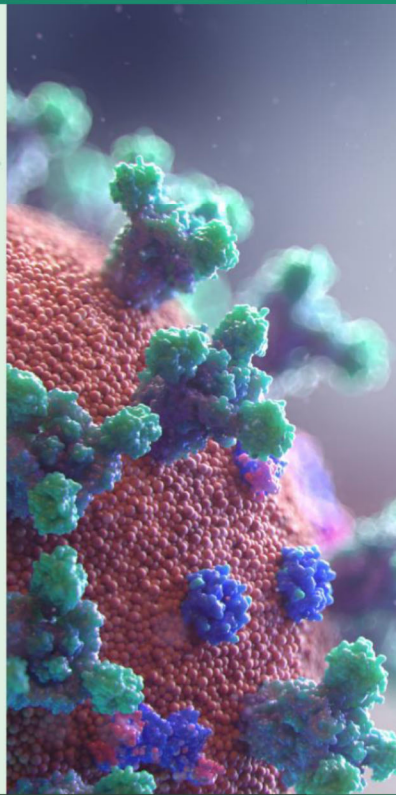
Wim Hafkamp
Directeur Z-CERT



**INFORMATIE
BERAAD**



**De missie van
Z-CERT is het
versterken van
de digitale
veiligheid van
de zorgsector**



START IN 2017

Team

1 januari 2020
13 medewerkers
2 externen

1 januari 2021
14 medewerkers
10 externen



Deelnemers

168*
in totaal

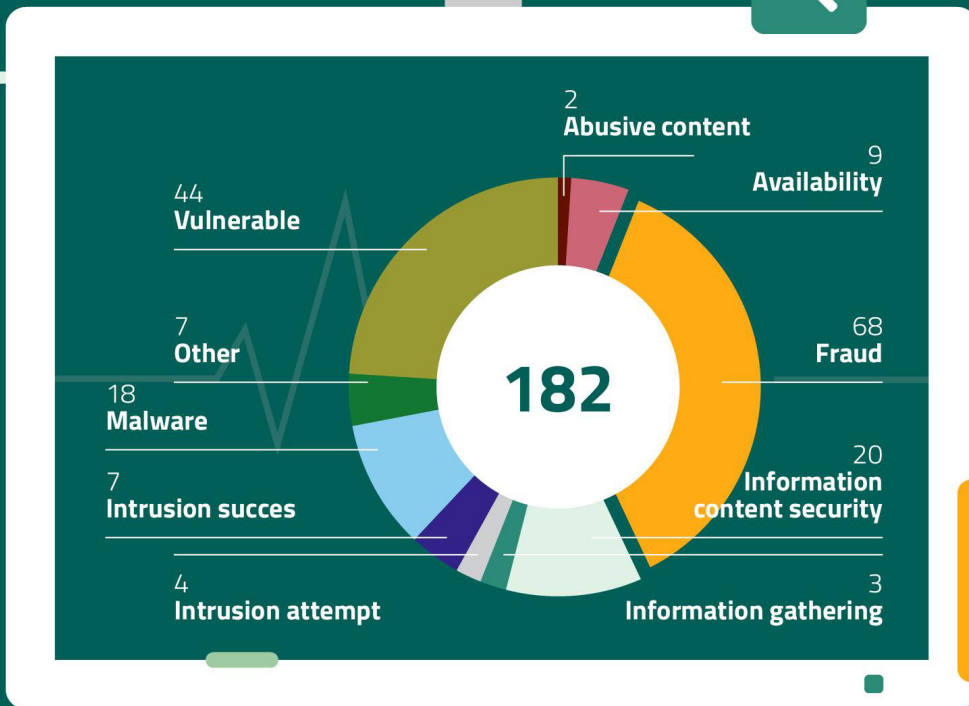


* Aantal deelnemers op 1 januari 2021



Incidenten

In 2020 hebben de deelnemers van Z-CERT **182 keer** een incident gemeld.



Zwakke beveiliging = achilleshiel van succesvolle digitalisering

Secretaresse van Bravis neust jarenlang in gegevens van bekende voor 'wraakroman' van partner

ROOSENDAAL - Een secretaresse van het Bravis Ziekenhuis in Roosendaal heeft jarenlang de medische dossiers van de ex van haar partner bekeken. Haar man gebruikte de informatie vervolgens voor het schrijven van een 'wraakroman'. Niemand had iets door. Dat meldt NRC.

Karen Luiken 07-12-20, 06:37 Laatste update: 08:02



RTLnieuws

Groot datalek bij Jeugdriagg: medische dossiers kwetsbare kinderen gelekt

01 oktober 2020 12:56

Aangepast: 01 oktober 2020 13:45

SolarWinds hack may be much worse than originally feared

Some 250 government agencies and businesses may have been affected

By Kim Lyons | Jan 2, 2021, 4:50pm EST

THE VERGE

'Hackers gemeente Hof van Twente eisen 750.000 euro losgeld'

Losgeld Hackers hebben vorige week systemen van het Overijsselse Hof van Twente gehackt. De gemeente is onder meer gegevens van burgers kwijt.

Anna Herter 7 december 2020 om 9:24 Leesijd 1 minuut

nrc.nl



NOS NIEUWS • BINNENLAND • TECH • 05-02-2020, 14:58

Hackers Universiteit Maastricht zaten maanden in netwerk; 200.000 euro betaald

News 24 10 2020 21:59 updated 25 10 2020 11:38

yle

Psychotherapy centre data breach victims receive extortion emails psychotherapy

The extortionist wants payments in Bitcoin.

tweakers

18-01-2021 • 14:52

Ransomware legt Belgisch ziekenhuis voor een groot deel lam

Het ziekenhuis CHwapi in Doornik in Wallonië is afgelopen zondag slachtoffer geworden van een ransomwareaanval. Artsen kunnen niet bij dossiers. Niet-urgente onderzoeken en afspraken zijn uitgesteld.

CYBERSECURITY
=
RISICOMANAGEMENT
=
KANS X IMPACT

STEL NIET DE VRAAG OF MAAR WANNEER EN HOE ERG.....

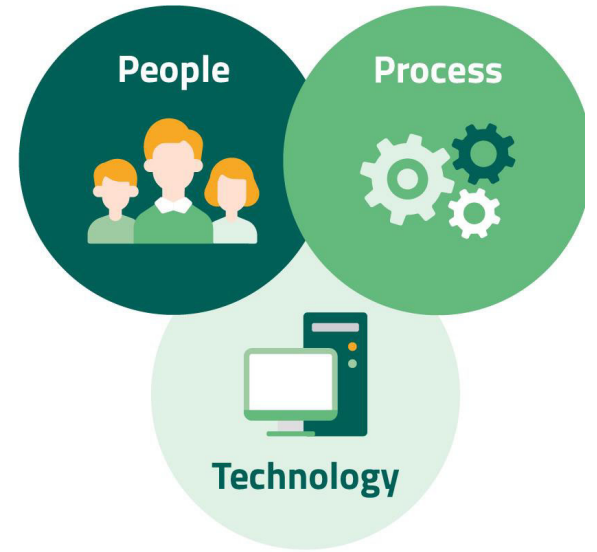


Cyberhygiene op orde

“Het is belangrijk dat zorginstellingen hun leveranciers niet blindelings vertrouwen maar eisen stellen aan hun **informatiebeveiliging**. Zo zou de leverancier periodiek moeten aantonen dat het informatiebeveiliging op orde heeft, voldoet aan de geldende wet- en regelgeving en, wanneer van toepassing, in het bezit is van certificeringen zoals bijvoorbeeld de **NEN 7510**. Ook zouden leveranciers periodiek **pentests en vulnerability scans** moeten uitvoeren als zij persoonsgegevens van zorginstellingen verwerken. Deze afspraken moeten de partijen vastleggen in een **verwerkersovereenkomst**.”

Cybersecurity Dreigingsbeeld Zorg 2020

People. Proces.
Technology.



People



Cyber Fit

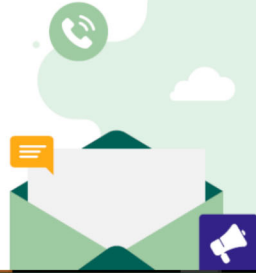
thuis en op het werk



Cyber awareness is niet alleen belangrijk op het werk, ook thuis is het van belang om zorgvuldig op de cyber veiligheid te letten. Juist nu thuiswerken zo gewoon is geworden zoeken criminelen naar de zwakste schakel van de medewerker om zo toegang te krijgen tot (bedrijfs-)systemen, e-mail accounts, login-gegevens en informatie.

Voorkom dat jij in je werk of privé slachtoffer wordt van een cyberaanval. Neem de onderstaande informatie tot je en maak het kwaadwillenden zo moeilijk mogelijk om bij jouw persoonlijke gegevens en bedrijfsgegevens te komen.

Cyber fit, thuis en op het werk.



Email en telefoon

- | Wantrouw e-mailberichten waarin je wordt gevraagd een **wachtwoord te wijzigen**. Helemaal wanneer je dit niet zelf hebt aangevraagd;
- | Pas op voor berichten van **onbekende afzenders**. Als je het niet vertrouwt klik dan niet op links en open vooral geen bijlagen. Heb je toch iets geopend of op een link geklikt en vertrouw je het alsnog niet? Waarschuw dan jouw helpdesk, IT manager of IT security manager;
- | Wees extra alert op verzoeken waarin je wordt gevraagd snel te beslissen of om **persoonlijke of gevoelige informatie** te delen of geld over te maken. Wees bewust van de waarde van informatie en overleg desnoods met een collega of leidinggevende. Durf 'nee' te zeggen tijdens een telefoongesprek.

Process



NEN
NEN 7510

NEN7510
stelt
eisen
Informatiebeveiliging
in de zorg



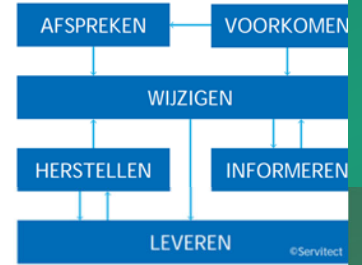
Uit rapportages
blijkt of en in welke
mate aan de norm
wordt voldaan



Aan eisen wordt
voldaan door
activiteiten



Activiteiten worden
georganiseerd in
het procesmodel



Activiteiten worden
ondersteund door
de helpdesk tool

Uit de helpdesk tool
komt data voor
rapportages



Technology



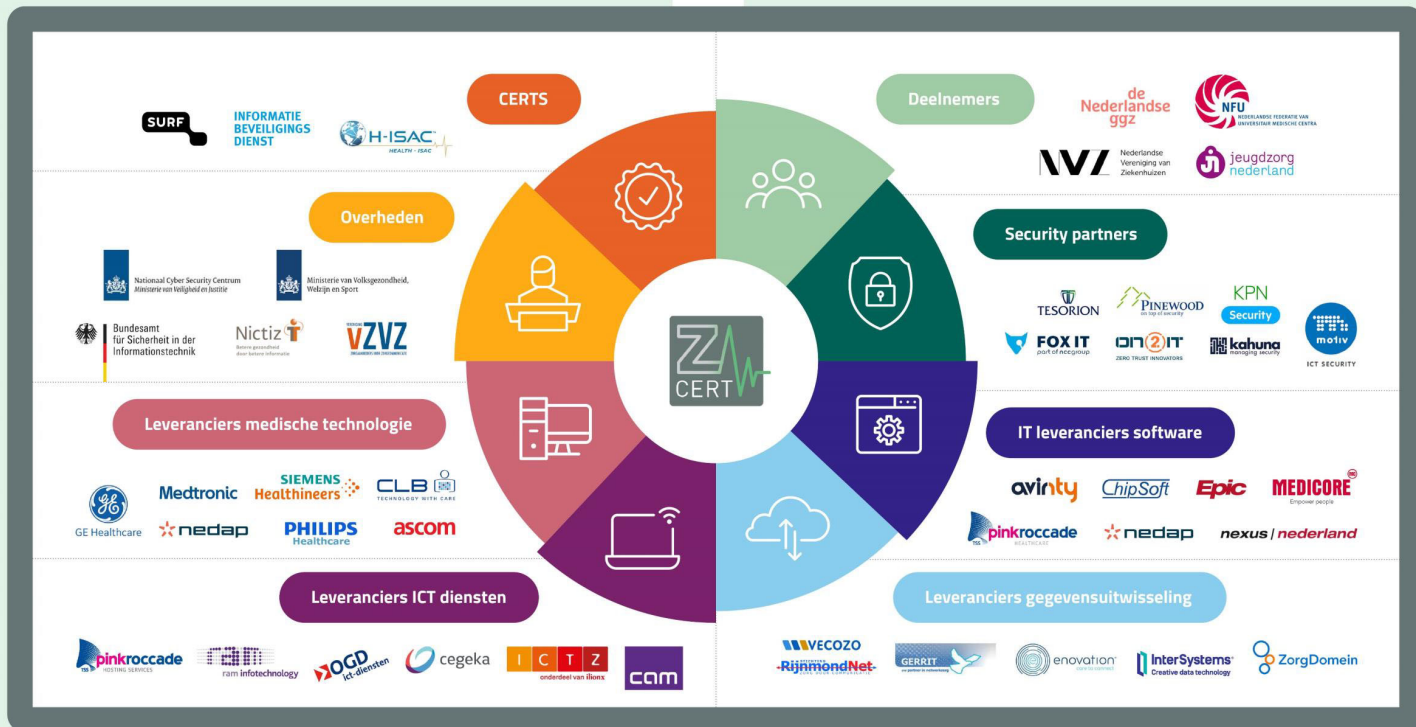
COMPLIANT ZIJN MET
NEN7510 IS NIET
VOLDOENDE !

TESTEN, TESTEN, TESTEN...



KETENAFHANKELIJKHEID
IS EEN RISICO VOOR DE
ZORGSECTOR





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.

“Informatiebeveiliging en cybersecurity is chefsache en hoort thuis in de bestuurskamers.”

Z-CERT symposium 1 februari 2021

Erik Gerritsen
SG VWS





Taken van de bestuurder

1. bewust worden
2. beveiligen
3. bewaken
4. blussen

100% veilig bestaat niet

Digitale weerbaarheid is en blijft samenspel van mens, proces en techniek



Cybersecurity Dreigingsbeeld Zorg 2020



COMPUTER EMERGENCY
RESPONSE TEAM
VOOR DE ZORG



Vragen?

Z-CERT

Expertisecentrum voor
cybersecurity in de zorg

Stationsplein 121
3818 LE AMERSFOORT
tel. 033 737 06 09
info@z-cert.nl



COMPUTER EMERGENCY RESPONSE TEAM VOOR DE ZORG

