



COMPUTER EMERGENCY
RESPONSE TEAM
VOOR DE ZORG

Producten en Diensten

Stichting Z-CERT is hét expertisecentrum op het gebied van cybersecurity in de zorg. Z-CERT heeft specifieke kennis van medische hard- en software, ondersteunt zorgorganisaties bij een digitaal incident en vergroot de weerbaarheid van de sector op het gebied van cybersecurity.



Informatieberichten en alertering

Z-CERT ontvangt informatie van het Nationaal Cyber Security Centrum, andere (inter)nationale CERTS en partners. Z-CERT vertaalt deze informatie naar de volgende producten.



(Medische) Advisories

± 50 per maand

Advisories met handelingsadvies over ontdekte kwetsbaarheden in (medische) hard- / software.



Infoberichten

± 7 per maand

Informatie over lopende security incidenten met sector brede impact.



Operational alerts

± 1 per maand

Informatie over actuele en urgente dreigingen waarbij Z-CERT de ontvanger oproept direct te handelen (bijv. patchen).



End-of-week

Een wekelijks overzicht van alle verzonden advisories, (relevante) mediaberichten en links naar websites met achtergrondinformatie.



End-of-month

Een maandelijks overzicht van relevante ontwikkelingen en actualiteiten met een duiding door de experts van Z-CERT.



Kennisdeling

Z-CERT nodigt haar deelnemers uit om actief kennis te delen over hun aanpak van cybersecurity en waargenomen dreigingen.

Community

Z-CERT biedt een online platform aan waar deelnemers op een beveiligde omgeving onderling informatie kunnen uitwisselen. Z-CERT heeft hierin zowel een faciliterende als inhoudelijke rol. Tevens organiseert Z-CERT netwerkbijeenkomsten.



Informatieverzoeken

Deelnemers kunnen een niet-urgente security vraag via e-mail of een beveiligd chatkanaal voorleggen aan de specialisten van Z-CERT.

Publicaties

Z-CERT deelt verdiepende kennis over cybersecurity onderwerpen zoals ransomware via whitepapers en factheets.



Monitoring IP-adressen en domeinnamen

Z-CERT controleert elke werkdag of IP-adressen en domeinnamen van deelnemers op blacklists voorkomen. Daarnaast ontvangt Z-CERT regelmatig lijsten met kwetsbare systemen van zorginstellingen, zoekt proactief naar kwetsbare systemen of stelt deze lijsten zelf samen.

ZorgDetectieNetwerk (ZDN)

Deelnemers kunnen kiezen voor een aansluiting op het ZDN. Het ZDN deelt realtime 'indicators of compromise' met deelnemers. Deze informatie vormt een collectief geheugen voor digitale dreigingen met als doel een weerbare zorgsector.

Afhandeling en coördinatie incidenten

Wanneer een deelnemer te maken heeft met een IT-beveiligingsincident, adviseert Z-CERT bij de aanpak en het oplossen van het incident. Tevens kan Z-CERT ondersteuning bieden bij forensisch onderzoek.



Coordinated Vulnerability Disclosure

Kwetsbaarheden in websites van deelnemers en in (medische) apparatuur of programmatuur, die door derden zijn ontdekt, kunnen bij Z-CERT worden gemeld.