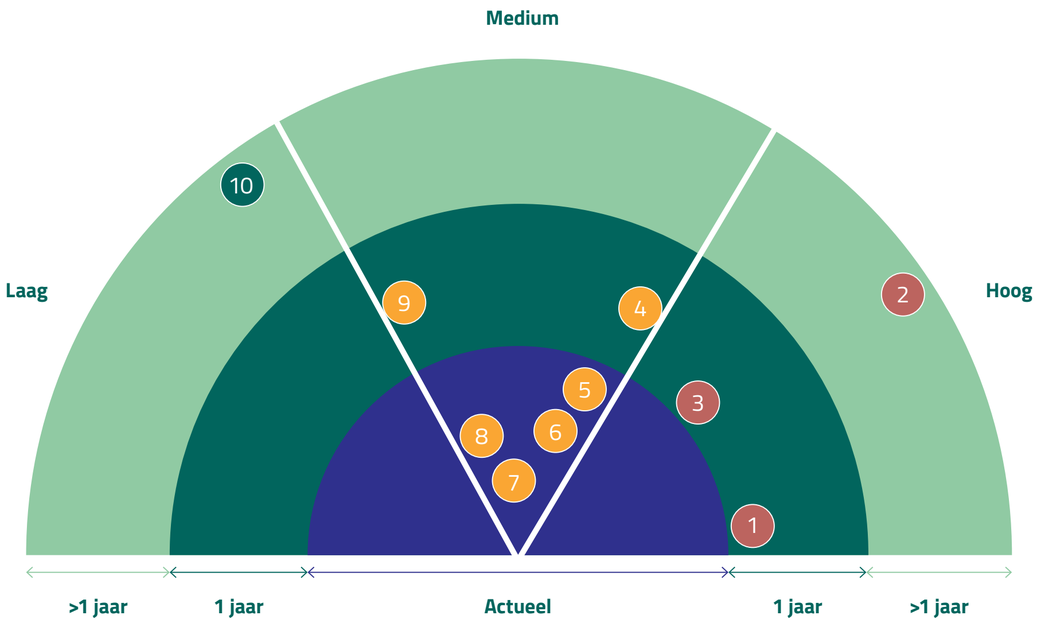
Cybersecuritybeeld 2025



Dreigingsradar

De dreigingsradar geeft de tijd, de impact en daarmee de ernst van de dreiging weer voor de zorg. De plaats van de diverse bolletjes in de binnenring, middenring of buitenste ring zegt iets over wanneer iets een dreiging zal zijn.

Kleur	Impact
	Hoog
	Gemiddeld
	Laag

Op dit moment | Korte termijn <1 | Lange termijn >1

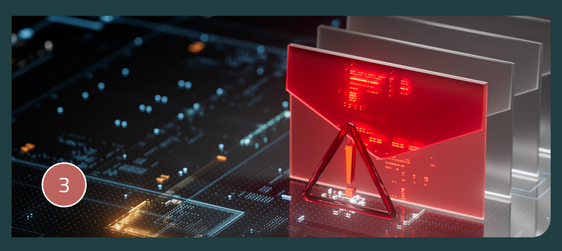
Dreigingen - Trends en ontwikkelingen

Ransomware en afpersing met datalek

Deze dreigings is onverminderd hoog. Enkelvoudige afpersing waarbij gedreigd wordt met openbaarmaking van gestolen data wint terrein. Het versleutelen blijft dan achterwege.

Spionage bij onderzoeksinstellingen

De Nederlandse zorgsector is interessant voor statelijke actoren vanwege hoogstaand wetenschappelijke onderzoek, intellectuele eigendommen en grote datasets aan medische- en persoonsgegevens. In enkele gevallen passen de actoren naast spionage ook ransomware toe, als afleiding of voor persoonlijk gewin.



Ransomware bij leverancier

Een aanzienlijk aantal leveranciers van Europese zorgorganisaties is getroffen. Ransomware heeft processen verstoord, daarnaast is er vertrouwelijke data gelekt. In Nederland viel vooral de casus bij Clinical Diagnostics op.

DDoS bij leverancier

Verschillende sectoren die aan de zorg leveren waren doelwit, zoals telecom- en serviceproviders en informatietechnologie- en dienstverlening. Dit had tot gevolg dat enkele digitale services een tijd lang niet of verminderd beschikbaar waren.

Malware

In veel gevallen is de impact van malware-incidenten beperkt en wordt de infectie snel opgeruimd. Cybercriminelen maken meer gebruik van infostealers om wachtwoorden te stelen of om een aanval voort te zetten. Dit jaar viel op dat sommige (goedkope) Android-apparaten werden geleverd met malware.

Credential Phishing

MFA is belangrijk maar geen garantie. Niet alle MFA oplossingen zijn bestand tegen de nieuwste phishing technieken, waardoor kwaadwillenden toegang kunnen krijgen tot mailboxen, en andere aan deze inloggegevens gekoppelde platforms. Meerdere zorgorganisaties werden hierdoor getroffen, waarbij de phishingmail vaak vanuit een gecompromitteerde mailbox van een leverancier verstuurd werd.

Insider threats

De frequentie varieert sterk per type insider threat. Als het gebeurde betrof het vaak tientallen geraakte systemen per organisatie. Met name onopzettelijke datalekken komen regelmatig voor. Incidenten die dit jaar opvielen waren ex-medewerkers of ex-inhuurkrachten die data hebben gestolen of daar mee dreigden.

DDoS

Geopolitieke ontwikkelingen hebben niet geleid tot een toename van het aantal incidenten.

Financiële fraude

De impact van financiële fraude was groter dan in 2024. Dit jaar betrof het vooral nagemaakte facturen, verstuurd vanuit gecompromitteerde mailboxen van een bekende collega of organisatie.

Spionage bij zorgaanbieders

Landen met een offensief cyberprogramma hebben vooral interesse in het stelen van wetenschappelijk onderzoek of persoonsgegevens van voor hen interessante doelwitten. Daarom is het onwaarschijnlijk dat zorginstellingen die hier niet over beschikken een doelwit worden.

De Nederlandse zorg digitaal veilig

Blijf een stap voor met het Z-CERT Cybersecuritybeeld Zorg 2025

In dit Cybersecuritybeeld voor de zorg 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.

Download via **Z-CERT.nl/cybersecuritybeeld2025**