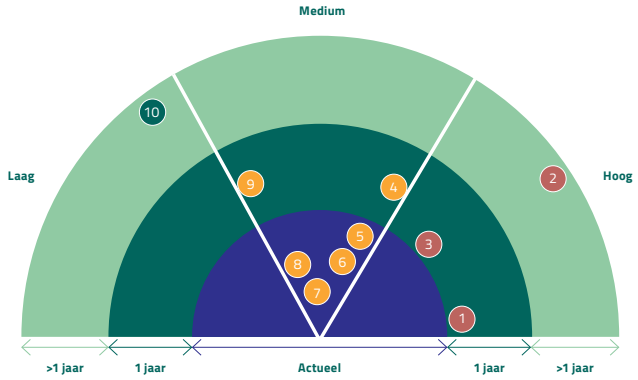
Cybersecuritybeeld 2025



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.

Dreigingen - Trends en ontwikkelingen

Dreiging	Niveau	Duiding
1. Ransomware en afpersen met datalek		Deze dreigings is onverminderd hoog. Enkelvoudige afpersing waarbij gedreigd wordt met openbaarmaking van gestolen data wint terrein. Het versleutelen blijft dan achterwege.
2. 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.
3. 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. Beschouw deze dreiging ook in (regionale) samenwerkingsrelaties met andere zorgaanbieders.
4. DDoS bij leverancier		Verschillende sectoren die aan de zorg leveren waren doelwit, zoals telecom- en serviceproviders en informatietechnologie & diensten. Dit had tot gevolg dat enkele digitale services een tijd lang niet of verminderd beschikbaar waren.
5. 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.
6. 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.
7. 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-inhuur die data hebben gestolen of daar mee dreigden.
8. DDoS		Geopolitieke ontwikkelingen hebben niet geleid tot een toename van het aantal incidenten.
9. 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.
10. 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.

Blijf een stap voor en download het Cybersecuritybeeld Zorg 2025 op **z-cert.nl/cybersecuritybeeld2025**