Ministerie van Volksgezondheid,
Welzijn en Sport

Real-Time DDoS Attack Map | NETSCOUT Cyber Threat Horizon

https://cybermap.kaspersky.com/

15 juni 2026

Samen gezond, fit en veerkrachtig

Ministerie van Volksgezondheid,
Welzijn en Sport

Data voor de zorg.
Zorg voor de data.

Breakoutsessie Cybersecurity & weerbaarheid

Marcel Floor
MT-lid VWS Directie informatiebeleid en CIO

11 juni 2026

Samen gezond, fit en veerkrachtig

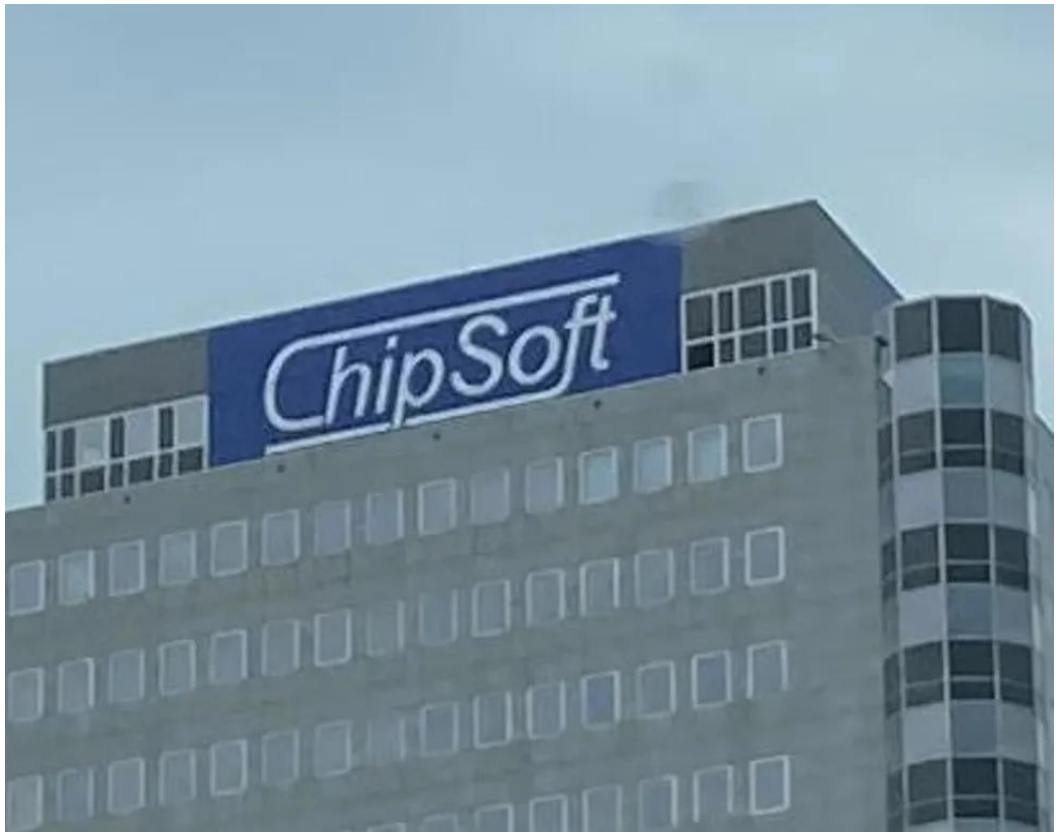
Je denkt dat het bij jou niet gebeurt...

...tot het wél gebeurt.

11-6-2026

Je denkt dat het bij jou niet gebeurt...

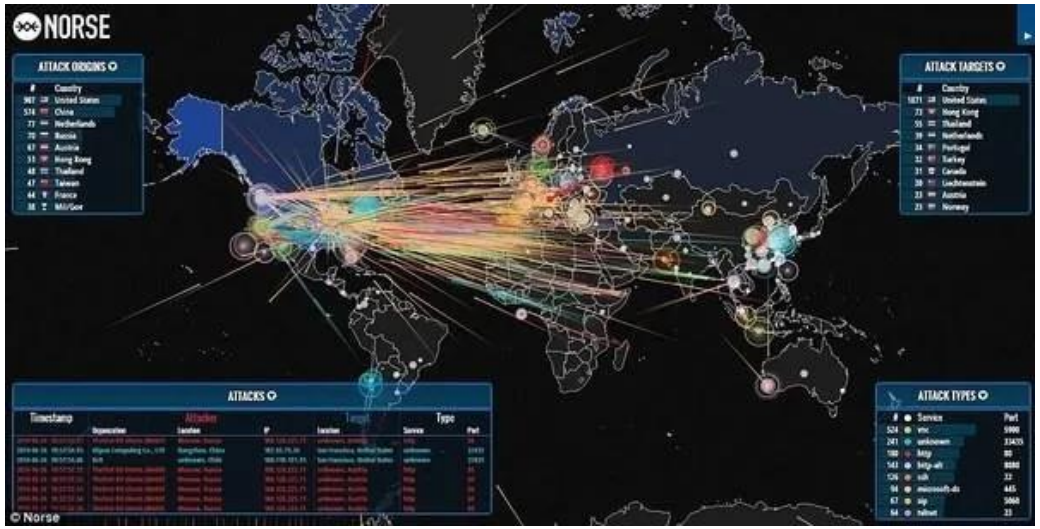
...tot het wél gebeurt.



Dreigingsbeeld in de zorg

Digitale dreigingen raken de zorg – direct en structureel

- Datalekken en ransomware-aanvallen nemen sterk toe. Ook kleinere zorginstellingen zijn steeds vaker slachtoffer
- De zorgsector is aantrekkelijk voor cybercriminelen vanwege de waardevolle en gevoelige data
- Hybride oorlogsvoering brengt nieuwe risico’s met zich mee, zoals sabotage van vitale zorginfrastructuur
- Phishing en social engineering: medewerkers worden benaderd om toegang te verkrijgen
- Verouderde systemen vergroten kwetsbaarheid
- IT-uitval leidt direct tot verstoring van de zorgverlening en kan patiënten ernstig treffen



Real-Time DDoS Attack Map | NETSCOUT Cyber Threat Horizon

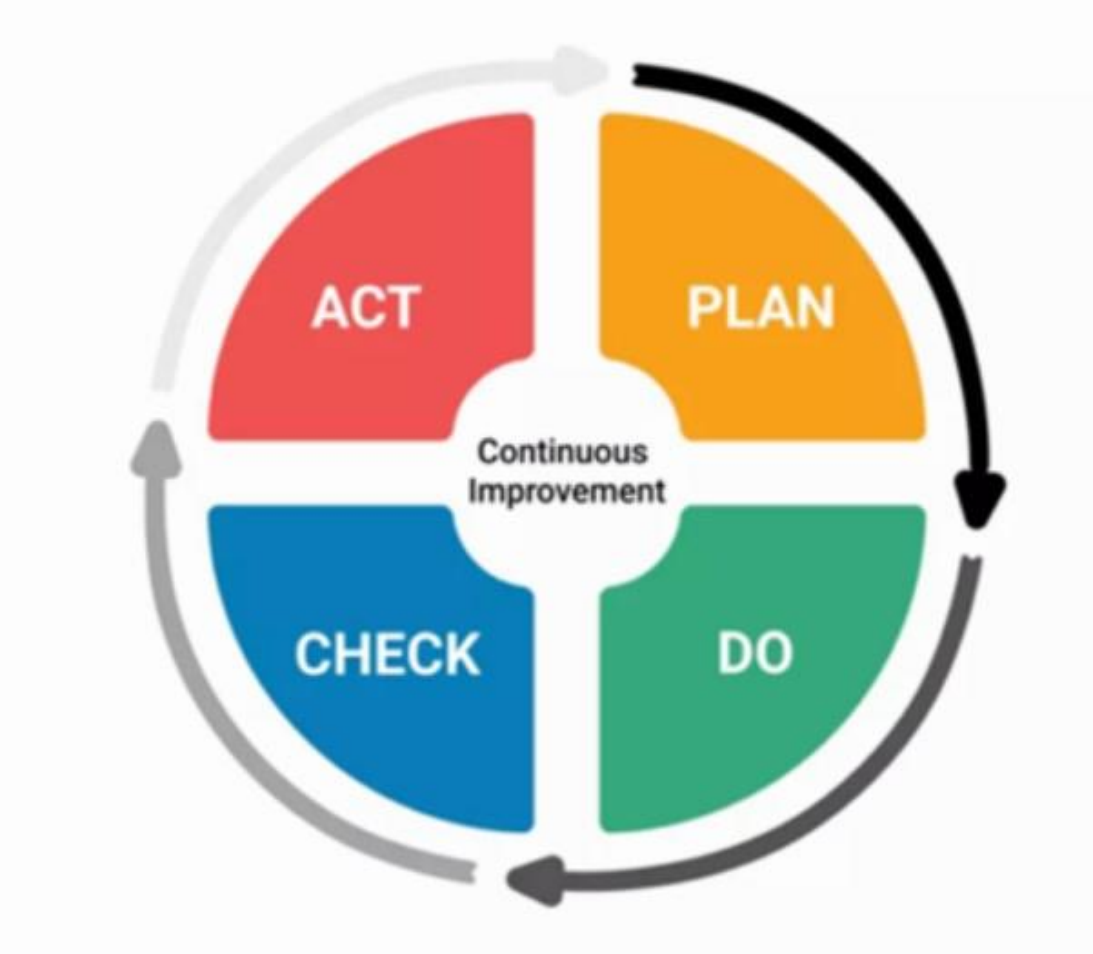
De basis staat. Wat doen we nu al?

- **Wettelijke verplichte NEN-normen** 7510, 7512, 7513 en 7516 zijn ontwikkeld in nauwe samenwerking met het zorgveld
- De **Inspectie Gezondheidszorg en Jeugd** (IGJ) ziet toe op naleving van deze normen
- **Z-CERT** ondersteunt bij cyberincidenten en geeft preventief advies
- Diverse programma's stimuleren **informatieveilig gedrag**, zoals webinars en leergangen
- **Quick scans** en **hulpmiddelen** helpen organisaties met het in kaart brengen en verbeteren van hun beveiliging

Wat leren we van eerdere incidenten?

Van incident naar inzicht: leerpunten uit de praktijk

- **Dataminimalisatie**: verwerk alleen wat nodig is – minder data = minder risico
- **Ketenverantwoordelijkheid**: leveranciers en partners zijn onderdeel van jouw beveiliging
- **Informatiebeveiliging** is continu proces: blijf verbeteren met de PDCA-cyclus



Hoofdstuk 5 - Leiderschap

- Beleid
- Rollen en verantwoordelijkheden
- Risicomanagement

Daarna

- Maatregelen 7510-2
- Organisatie
- Bewustzijn
- Techniek
- Processen
- Leren en verbeteren

Wat betekent dit voor mij?

Start met de norm, de NEN 7510

Nog meer normen….?

De Cyberbeveiligingswet

Wat is het doel?

De Cbw is de Nederlandse uitwerking van de EU-richtlijn NIS2 en richt zich op het versterken van de digitale weerbaarheid in Nederland.

- Het vergroten van de digitale paraatheid, doordat de reikwijdte is uitgebreid met extra sectoren zoals de zorg
- Extra sectoren die vitaal zijn voor maatschappij en economie zijn toegevoegd
- Focus op het versterken van cyberweerbaarheid op sectorniveau
- Beperken van de gevolgen van cyberincidenten door tijdige meldplicht en monitoring van dreigingen voor een snelle respons, zowel binnen als tussen sectoren.

Plichten Cyberbeveiligingswet

Registratieplicht

Meldplicht

Zorgplicht

Informatieplicht

Governance

Training voor Raden van Bestuur

Voor wie?

- De bestuurlijke verantwoordelijkheden onder de Cyberbeveiligingswet liggen bij de uitvoerende bestuurders van een organisatie. Zij zijn verantwoordelijk voor het nemen van passende maatregelen en het waarborgen van de naleving van de wet.

Wat?

- Uitvoerende bestuurders moeten een opleiding of training over cyberbeveiliging volgen. In het Cyberbeveiligingsbesluit wordt vastgelegd welke eisen hier precies aan worden gesteld. De toezichthouder kan om dit certificaat vragen.
- Belangrijke termijnen:
  - uiterlijk twee jaar na inwerkingtreding van de wet dient de training gevolgd te worden
  - nieuwe bestuurders binnen twee jaar na benoeming
  - kennis moet na de training aantoonbaar actueel blijven

- **Vragen om als bestuurder te stellen aan de CISO**

Dit artikel van het NCSC helpt jou als bestuurder om het juiste gesprek te hebben met de CISO en zo grip te krijgen op de cyberveiligheid van je organisatie.

Centrum voor criminaliteitspreventie en veiligheid CYRA-Zorg voor zorginstellingen - Het CCV

Wacht niet af

- Breng in kaart hoe je organisatie er nú voor staat
- Plan een gesprek met je CISO, CIO of IT-manager
- Agendeer informatiebeveiliging structureel op bestuursniveau
- Check of je voldoet aan NEN-normen als eerste stap om te voldoen aan de Cyberbeveiligingswet
- Investeer in bewustwording: ook op bestuursniveau (wettelijke verplichting uit de Cbw)
- Maak van dataveiligheid een strategische prioriteit

Wat ga je morgen doen?

Hulpmiddelen

- Z-CERT
- Quickscan informatiebeveiliging voor (kleine) zorgorganisaties
- NEN hulpmiddelen bij NEN7510 (maak eerst een gratis account aan)
- Informatieveilig gedrag in de zorg
- Cyberbeveiligingswet
- AVG helpdesk zorg
- Cbw - Zorgplicht
- Ketenbeveiliging - Good Practices

Bedankt!

Neem gerust contact met ons op.

www.gegevensuitwisselingindezorg.nl

?