Cyberveiligheid in de gezondheidszorg

Voorkomen is beter dan genezen, óók als het om cyberaanvallen gaat

Vrijwel alle zorgverleners in Nederland werken met het elektronisch patiëntendossier (EPD). Daarnaast zijn ze aan de achterkant digitaal verbonden met soms wel honderden leveranciers. Dit maakt de sector een geliefd doelwit. Systeembeschikbaarheid is cruciaal in de zorg. Vitaal zelfs, want mogelijk een zaak van leven en dood. Dit vergroot de kwetsbaarheid van zorgorganisaties als het gaat om ransomware en financiële fraude. En daarmee hun bereidheid om te betalen.

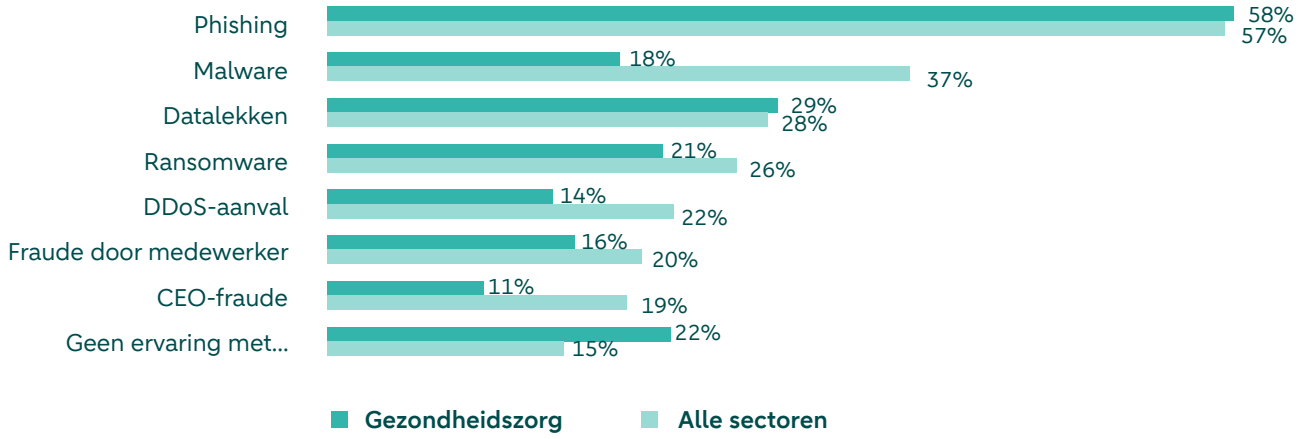
Recente cyberaanvallen in de sector

- In maart 2023 was het flink schrikken in België. Een cyberaanval dwong het Brusselse Saint-Pierre ziekenhuis om zijn eerste hulp te sluiten. Ambulances werden gedwongen omgeleid naar andere ziekenhuizen en het zorgpersoneel kon de medische administratie alleen nog met pen en papier bijhouden. De eerste signalen? Traag werkende servers en 'abnormale activiteit' op het netwerk. Daarop trad onmiddellijk een noodplan in werking, waarbij alle servers offline werden gehaald. Uiteindelijk duurde de aanval nog geen dag en werden er geen patiëntengegevens gestolen. Toch had het ziekenhuis lang nodig om de zaak te onderzoeken en bleven de praktische naweeën – bijvoorbeeld geen wifi voor patiënten – nog een flinke tijd voelbaar.
- Als vergelding voor onze hulp aan Oekraïne, veroorzaakte de pro-Russische hackersgroep Killnet begin 2023 flink wat digitale onrust in Nederland. Vooral ziekenhuizen bleken het doelwit. Zo lanceerden ze een DDoS-aanval op het Universitair Medisch Centrum Groningen (UMCG), waarbij het systeem een tsunami aan automatische aanvragen te verwerken kreeg. Ook al ging de website van het ziekenhuis tijdelijk op zwart, de impact viel mee en de patiëntenzorg kon gewoon doorgaan. Killnet riep sympathiserende hackers overigens op om meer aanvallen uit te voeren op prominente ziekenhuizen, waaronder UMC Utrecht, Erasmus MC en Radboudumc.
- In 2023 wist hackersgroep LockBit in te breken in het computersysteem van Joris Zorg – een zorginstelling uit het Brabantse Oirschot. De hackers hebben cliënt- en medewerkersgegevens gestolen en online gedeeld. Waarschijnlijk ging het onder andere om namen van bewoners en informatie over hun medische toestand. De zorginstelling heeft de Autoriteit Persoonsgegevens en de politie op de hoogte gesteld.

ABN·AMRO

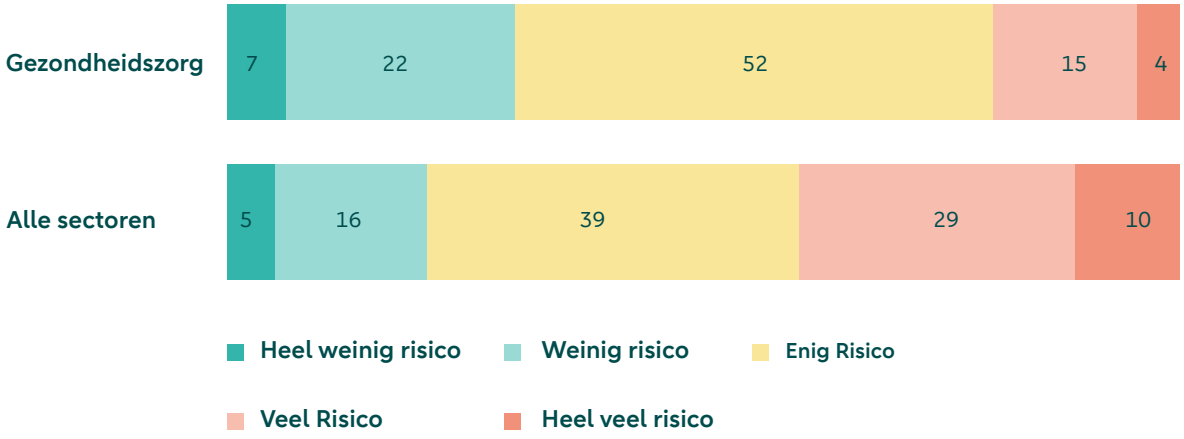
Cybercrime in de zorg: gemiddeld – ondanks hoge scores voor datalekken en phishing

*Met welke van de volgende vormen van cybercriminaliteit heeft u binnen uw organisatie weleens te maken gehad?**



Zelf schat de sector de kans op een digitale aanval gunstiger in: iets minder dan gemiddeld

*In welke mate denkt u dat cybercriminaliteit een risico is voor uw organisatie?**



* Bron: enquête van ABN AMRO en MWM2 onder 895 Nederlandse organisaties, maart 2024

NIS2: nieuwe Europese wetgeving moet cyberweerbaarheid verbeteren

Om de cyberveiligheid in Europa te verbeteren, gaat in oktober 2024 een nieuwe wet in: NIS2, de opvolger van de Network and Information Security Directive (NIS). De NIS2-wetgeving geldt voor bedrijven met minimaal vijftig werknemers, of een jaaromzet en balanstotaal van meer dan € 10 miljoen. Organisaties die belangrijk of essentieel zijn voor de maatschappij, moeten zich aan deze richtlijn houden om de impact van cyberaanvallen en -verstoringen te beperken. Dit geldt ook voor bedrijven in de keten van deze vitale organisaties, zoals klanten, partners en toeleveranciers.

Het is de bedoeling dat Europese lidstaten de richtlijn naar landelijke wetgeving vertalen, maar Nederland loopt hierbij vertraging op. Toch is het verstandig om uw organisatie al op de invoering voor te bereiden. Omdat de wet er hoe dan ook komt, maar ook omdat klanten of leveranciers in andere Europese landen de richtlijn wél vanaf oktober 2024 volgen.

In de zorg vallen diverse organisaties onder de nieuwe NIS2-regelgeving: van ziekenhuizen, jeugdzorg-instellingen en revalidatiecentra tot ¬(bijvoorbeeld) fysiotherapeuten binnen een netwerk met meer dan € 10 miljoen omzet. Dit maakt NIS2-regulering – naast bestaande NEN 7510-normering – heel belangrijk. Meer focus op veiligheid is ook noodzakelijk in de toeleveringsketen; denk aan wasserijen, catering of leveranciers van voedingssupplementen.

Benieuwd of uw organisatie onder de NIS2-richtlijn valt?
Lees ons rapport: **Steeds verfijndere cyberaanvallen schudden ondernemers nog lang niet altijd wakker,**
of vul de **Zelfevaluatie NIS2** van het Nationaal Cyber Security Centrum in.

Verhoog de cyberveiligheid van uw organisatie

Steeds meer organisaties worden slachtoffer van cybercriminaliteit – criminelen hebben maar een kleine ingang nodig. Mogelijk loopt u nu al risico. Daarom is het belangrijk om passende maatregelen op het gebied van cyberveiligheid te nemen. Om u en uw mensen daarbij te helpen, zetten we verschillende oplossingen en downloads op een rij.

Cyberveiliger in drie stappen

1 Maak een risico-analyse

Breng de 'kroonjuwelen' van uw organisatie in kaart. Welke zaken zijn cruciaal voor uw bedrijf of dienstverlening? Denk aan klantgegevens, productiemethoden of intellectueel eigendom. Identificeer vervolgens welke dreigingen deze kroonjuwelen in gevaar kunnen brengen: bijvoorbeeld kwetsbaarheid in software of een medewerker die op een malafide link klikt. Nu kunt u de risico's analyseren. Wat is het gevolg van deze risico's, hoe waarschijnlijk zijn ze en wat doet u al om ze te beperken?

2 Neem adequate maatregelen

Uw risico-analyse bepaalt welke maatregelen de juiste zijn. De basismaatregelen van het Nationaal Cyber Security Centrum en de basisprincipes van het Digital Trust Center vormen in ieder geval een goed startpunt. Daarnaast kunt u:

- veilig gedrag van uw medewerkers stimuleren;
- bepalen en vastleggen wie de eigenaar van bepaalde gegevens is;
- risico's met uw partners en leveranciers bespreken.

Een cybersecurity-specialist kan u helpen om de juiste maatregelen te nemen.

3 Stel een Cyber Response Plan op

Ten slotte is het essentieel om procedures te ontwikkelen waarmee u cyberincidenten detecteert en afhandelt. Deze legt u vast in een Cyber Response Plan.

Whitepaper over Employee Awareness (Download onze whitepaper)
Cybercriminelen komen vaak via medewerkers uw digitale systemen binnen. Houd uw medewerkers scherp en maak ze bewust van de risico's van cybercrime. U leest er alles over in ons whitepaper.

Checklist: Third-Party Risk Management (Bekijk de checklist)
Als u met partners en leveranciers samenwerkt, kunnen er veiligheidsrisico's optreden. Met Third-Party Risk Management brengt u deze in kaart.

- Identificeer mogelijke cyberrisico's
- Deel de checklist met uw klanten en leveranciers voor meer veiligheid

Cyber Response Plan (Maak uw Cyber Response Plan)
Een Cyber Response Plan helpt u om cybercrime-incidenten op te sporen, af te handelen en eventuele schade te herstellen.

- Stel uw eigen Cyber Response Plan op
- Bereid uw bedrijf en medewerkers voor op een cyberaanval

Cyberveiligheidsrapport (Lees het complete rapport)
Afgelopen jaar kreeg bijna driekwart van de Nederlandse bedrijven te maken met een cyberaanval. Lees alle feiten en ontwikkelingen in het jaarlijkse rapport 'Steeds verfijndere cyberaanvallen schudden ondernemers nog lang niet altijd wakker'.

NIS2-praktijkgids (Check onze NIS2-praktijkgids)
Elke sector kent verschillende cyberrisico's. In de industriële sector is vaak de productie het doelwit van cybercriminelen, terwijl ze in de gezondheidszorg uit zijn op patiëntgegevens. Benieuwd naar de risico's en dreigingen in uw sector?

Zo helpt ABN AMRO

Cyber Veilig & Zeker van MMOX

Voor een midden- en grootbedrijf dat zoekt naar ontzorging in cyberveiligheid.

- 24/7 proactief beschermd tegen cyberdreigingen
- Helpdesk voor cyberveiligheidsvragen

Bekijk Cyber Veilig & Zeker

Cyberverzekering

Voor zakelijke klanten die zich willen indekken tegen cyberschade.

- Bescherming via onze cyberverzekering
- Uitgebreide dekking
- 24/7 hulp van onze specialisten

Ontdek onze cyberverzekering

Vrijblijvend cybergesprek

Voor ondernemers die willen weten hoe ze ervoor staan op het gebied van cyberveiligheid.

- Informatie over tools en oplossingen
- Samen logische vervolgstappen bepalen

Plan vrijblijvend een gesprek in

Op de hoogte blijven van de laatste ontwikkelingen en artikelen? Meld u aan voor onze nieuwsbrief