‘Zorgverlening betekent óók de digitale weerbaarheid samen actueel houden’

De zorgsector maakt steeds meer gebruik van digitale systemen en technologie. Dat betekent kansen om de zorg toegankelijk te houden, maar het brengt ook risico’s met zich mee: met name op het gebied van cyberbeveiliging. Digitale weerbaarheid is cruciaal om de continuïteit en de kwaliteit van zorg te kunnen blijven waarborgen, weet ook Marcel Floor, MT-lid bij de Directie Informatiebeleid van het ministerie van VWS.

& DOOR ANNEMARIE LAMAIN

“De maatschappelijke opgave die er ligt, zit hem meer in weerbaarheid in algemene zin dan alleen in de cybersecurity”, stelt Floor. “Die opgave naar weerbaarheid hoor je terug in de woorden van het kabinet: we zijn niet in oorlog maar zeker ook niet in vrede. Dat geldt wat mij betreft ook zeker voor de zorg. Gelukkig hoor ik steeds vaker als ik bij zorgaanbieders kom dat ze ‘weerbaarheid’ hoog op de agenda hebben staan. Maar wat mij betreft gaat dit niet alleen over de technische infrastructuur van zorgaanbieders. Het gaat over ons allemaal. Als digitale voordeuren niet goed worden beveiligd en het gaat mis, dan raakt het iedereen en dus ook de continuïteit van de zorg.”

Digitale weerbaarheid betekent dan ook veel meer dan je inzetten voor cybersecurity. Volgens Floor heeft het ook te maken met ‘preventie’ en de vraag hoe snel je je als organisatie kan herstellen na een cyberaanval. Dus is het belangrijk om te investeren in bewustwording, processen, gedrag en technologie.

“Ik vergelijk het wel eens met de voordeur van je huis. Daar zit toch ook een slot op dat je kunt dichtdraaien als je bijvoorbeeld op pad gaat. Waarom denken we dan nog te gemakkelijk over onze digitale voordeur? We liggen permanent onder vuur in de digitale wereld, ook in de zorg. Dat vraagt in de eerste plaats om het vergroten van de bewustwording hiervan. Vanuit het ministerie proberen we die bewustwording te vergroten, bijvoorbeeld via webinars en bezoeken op locatie. Van topklinische zorg tot de individueel vrijgevestigde zorgverlener: allemaal willen we ze attenderen op het belang van het organiseren van een goede digitale weerbaarheid.”

Op orde krijgen en houden

Volgens Floor zijn er minstens twee zaken die organisaties helpen om planmatig hun weerbaarheid op orde te krijgen én te houden. Zo wordt in de tweede helft van 2025 de Network and Information Security directive, ook wel de NIS2 genoemd, van kracht. Deze richtlijn, vastgesteld door de Europese Unie (EU), is bedoeld om de cyberbeveiliging en weerbaarheid van essentiële diensten in EU-lidstaten te verbeteren. De NIS2-richtlijn richt zich op risico's die netwerk- en informatiesystemen bedreigen, zoals cyberbeveiligingsrisico's.

"De NIS2 is de opvolger van de NIS1", legt Floor uit. “In de vorige richtlijn was de sector zorg in Nederland geen onderdeel van de wetgeving, omdat de zorg geen vitale sector zou zijn. Niets is minder waar. De zorg is juist een speelveld waarin (internationaal) steeds meer gegevens worden uitgewisseld."

De Europese richtlijn wordt in Nederland omgezet in de Cyberbeveiligingswet. De coördinatie daarvan ligt bij het ministerie van Justitie en Veiligheid. Vakdepartementen zijn verantwoordelijk voor hun sector, zoals het ministerie van VWS dat is voor de zorgsector. VWS helpt zorgorganisaties met praktische ondersteuning en duidelijk informatie zodat ze op tijd kunnen voldoen aan de nieuwe verplichtingen van de Cyberbeveiligingswet.

Inrichten informatiebeveiliging

Floor doelt verder op de NEN7510, de norm voor informatiebeveiliging in de zorg. Hierin staat hoe organisaties in de zorg hun informatiebeveiliging moeten inrichten. In januari van dit jaar heeft de organisatie NEN tijdens het NEN-congres het eerste exemplaar van de herziene NEN7510 overhandigd aan VWS, waarbij de norm is aangepast om beter aan te sluiten op nieuwe dreigingen, technologische ontwikkelingen en wetgeving. In tegenstelling tot de NIS2 is de NEN7510 een nationale norm die door de zorg en voor de zorg is ontwikkeld.

Floor hierover: “De herziene NEN7510 is een goede basis voor zorgorganisaties om te voldoen aan de eisen van NIS2. Maar dat is echt niet toereikend. Zorgorganisaties moeten extra stappen gaan zetten om aan de NIS2-richtlijn te kunnen voldoen.” Zo moet de governance-structuur van organisaties glashelder zijn en incidentmeldingen worden geformaliseerd. Ook moeten bestuurders zorgen dat ze jaarlijks getraind worden op het gebied van digitale weerbaarheid en cybersecurity.

> “CYBERBEVEILIGING IS NOOIT AF, DAT IS EEN PERMANENTE BEWEGING”

Betekent dat ook dat als je als zorgorganisatie voldoet aan de regels van de NIS2 en NEN7510, je digitale weerbaarheid in orde is? Volgens Floor is dat niet het geval en zit de kwetsbaarheid ook in de zorgketen. Het gaat wat hem betreft bij digitale weerbaarheid niet alleen om een goede, digitale beveiliging per zorgorganisatie.

“De mogelijke kwetsbaarheid zit in de onderlinge keten: digitale gegevensuitwisseling tussen bijvoorbeeld zorgorganisaties, ICT-leveranciers, digitale platforms. Dat is een kwestie van goed samenwerken in de keten. Er is sterke samenwerking nodig tussen zorginstellingen, leveranciers, toezichthouders, en overheidsinstanties. Dat is ook een van de belangrijkste pijlers van de NIS2. Daarin staat een uniforme aanpak centraal om zo de verschillen tussen de lidstaten te voorkomen. Want juist omdat er nu nog verschillen zijn in de digitale weerbaarheid van landen, maak je ze kwetsbaar voor cyberdreigingen. Hoewel het nu vaak nog ieder voor zich is, zullen zorgorganisaties met de komst van NIS2 meer oog moeten hebben voor de hele keten als het gaat om digitale weerbaarheid.”

Nederland als doelwit

De cybercriminaliteit neemt toe en Nederland is wat dat betreft een gegevensrijk doelwit. Het is volgens Floor een kwestie van tijd tot we grote incidenten op dat gebied zien. “Cyberbeveiliging is nooit af, dat is een permanente beweging. Er moet voortdurend aan de bewustwording worden gewerkt bij zorgpersoneel. Veiligheidsvraagstukken moeten top of mind zijn bij personeel, ook op digitaal gebied. Zowel in de boardroom als op de vloer van de verpleegafdeling. En met het voldoen aan een NIS2 of een vernieuwde NEN7510 alleen kom je er niet.”

Een NEN7510-certificering is voor iedere zorginstelling of -verlener al verplicht. De nieuwe Cyberbeveiligingswet – de NIS2 – wordt naar verwachting in de tweede helft van 2025 van kracht en markeert het begin van een transitieperiode waarin zorgorganisaties hun cyberbeveiliging op orde moeten hebben. Het doel is om de steeds complexer wordende cyberdreigingen gezamenlijk het hoofd te kunnen bieden.

“Maar laat het feit dat de NIS2 pas later dit jaar ingaat alsjeblieft geen uitnodiging zijn om nu achterover te gaan leunen”, benadrukt Floor. “Met investeren in digitale weerbaarheid hadden we al veel eerder moeten beginnen. De vraag is niet óf het misgaat, maar wanneer. Je kunt naar de vernieuwde NEN7510 en de NIS2 kijken als twee instrumenten die je helpen om aan je verplichtingen te voldoen. Maar je kunt het ook benaderen vanuit zorgzaamheid. Want basale zorg betekent wat mij betreft niet alleen de zorg aan het bed en voor de patiënt, maar is ook de zorg voor de veiligheid van je gegevens.” ■

CV

Marcel Floor is MT-lid bij de directie Informatiebeleid van het ministerie van Volksgezondheid, Welzijn en Sport (VWS). Floor startte zijn loopbaan bij VWS in 2001. Hij vervulde verschillende (internationale) beleids- en managementfuncties. Het meest recent was dat als kwartiermaker/ Gezondheidsraad op de Nederlandse ambassade in Delhi. Hiervoor was hij Programmamanager eHealth zonder grenzen bij de Directie Informatiebeleid VWS.