

Toekomstbestendige zorg begint met vertrouwen



De zorg digitaliseert in hoog tempo. Zorgtechnologie, gegevensuitwisseling en kunstmatige intelligentie bieden grote kansen om zorgprofessionals te ondersteunen en cliënten beter te helpen. Maar de afhankelijkheid van digitale systemen groeit ook. Daarom zijn informatiebeveiliging en privacy een voorwaarde voor veilige, toekomstbestendige zorg.

Volgens Joost Wagenaar, senior adviseur Informatiebeveiliging en Privacy bij het landelijke programma Start je Kickstart van de Nederlandse overheidsorganisatie ICTU, en David Bos, CISO bij zorgorganisatie Vanboeijen, begint toekomstbestendige zorg niet met techniek maar vertrouwen. “Bewoners, cliënten, verwanten en medewerkers moeten erop kunnen rekenen dat wij zorgvuldig omgaan met gegevens en technologie”, stelt Bos. “Alleen dan kunnen we digitale mogelijkheden verantwoord inzetten. Het gaat niet alleen om persoonsgegevens, maar ook om de systemen waarop de zorg draait. Die afhankelijkheid neemt toe. Domotica, medicatietoediening, nachtobservatie en alarmering zijn verweven met het primaire zorgproces. Die systemen moeten dus beschikbaar en betrouwbaar blijven.”

De risico’s zijn volgens Bos reëel, want hackpogingen en phishing worden door AI steeds overtuigender. “Als informatiebeveiliging niet op orde is, kunnen medische gegevens op straat komen te liggen. Ernstiger is dat een organisatie volledig kan stilvallen. Dat raakt direct de continuïteit, veiligheid en kwaliteit van zorg.”

Veiligheid werkbaar maken

Bos vindt dat informatiebeveiliging werkbaar moet blijven. “Je kunt technisch

gezien tien sloten op een deur zetten, maar als een zorgmedewerker er steeds tien moet openen, is het niet meer werkbaar. Je bent voortdurend op zoek naar de balans tussen veilig genoeg en praktisch uitvoerbaar.”

Informatiebeveiliging draait daarom niet alleen om techniek, maar ook om gedrag. “Hoe dichter een medewerker bij de cliënt staat, hoe vaker diegene met gevoelige informatie te maken krijgt. Het is daarom belangrijk dat informatiebeveiliging aansluit op de dagelijkse zorgpraktijk en medewerkers helpt, in plaats van belemmert.”

“Ik zou de mens niet de zwakste schakel noemen, maar de laatste”, vervolgt Wagenaar. “Probeer aan de voorkant de juiste maatregelen te nemen die medewerkers ontzorgen. Tegelijkertijd is het cruciaal dat zij weten waarop ze moeten letten en dat ook vertalen naar de praktijk.”

Vanboeijen kiest daarom voor ondersteuning in plaats van controle. “Je kunt phishingmails versturen en medewerkers op de vingers tikken als ze ergens op klikken. Daar leert niemand van. We willen juist laten zien dat we allemaal fouten maken en daarvan leren.” Ook digicoaches spelen daarin een belangrijke rol. “Dat zijn collega’s uit de zorg die medewerkers helpen technologie

begrijpelijk en toepasbaar te maken”, legt Bos uit.

Start je Kickstart

Veel zorgorganisaties willen aan de slag met informatiebeveiliging en privacy, maar zoeken naar een praktische manier om prioriteiten te stellen en voortgang aantoonbaar te maken. Vooral kleinere organisaties hebben behoefte aan overzicht, structuur en ondersteuning.

Daarom ontwikkelde ICTU, met financiering van het ministerie van Volksgezondheid, Welzijn en Sport, het kosteloze ondersteuningsprogramma Start je Kickstart voor organisaties in de langdurige zorg. “We beginnen vaak met de Quicksan informatiebeveiliging”, vertelt Wagenaar. “Vervolgens kijken we waar de grootste risico’s zitten, welke maatregelen het meeste effect hebben en wie daarvoor verantwoordelijk is. Het doel is niet een lijstje af te werken, maar organisaties te helpen een continu verbeterproces in te richten.”

Zo werkt Start je Kickstart toe naar aantoonbare naleving van onder meer NEN 7510, de AVG en Cyberbeveiligingswet. “Tijdens het traject ontstaat vaak precies de beweging die nodig is: van inzicht naar concrete actie”, aldus Wagenaar. Vanboeijen heeft het traject inmiddels doorlopen en is NEN 7510-gecertificeerd. “De risicoanalyse was voor ons het juiste vertrekpunt”, zegt Bos. “Je kijkt waar de grootste risico’s zitten, wie daar invloed op heeft en welke prioriteiten je stelt. Dat heeft geholpen scherpe keuzes te maken en het eigenaarschap goed te beleggen.”

Verantwoorde technologie

Volgens beiden wordt informatiebeveiliging de komende jaren alleen maar belangrijker. Niet als rem op innovatie, maar als voorwaarde om technologie verantwoord in te zetten. Bos: “Informatiebeveiliging en privacy moeten geen obstakels zijn, maar enablers. Als de basis op orde is, kunnen we verantwoord bouwen aan zorgtechnologie, gegevensuitwisseling, kunstmatige intelligentie en slimme ondersteuning. Technologie is een middel om medewerkers beter te ondersteunen, de zelfredzaamheid van cliënten te vergroten en zorg te verbeteren. Zo maken we innovatie mogelijk zonder concessies te doen aan veiligheid en vertrouwen.”

Start je Kickstart biedt organisaties structuur, begeleiding en praktische hulpmiddelen. Zo groeit informatiebeveiliging uit van een papieren verplichting tot een stevig fundament voor veilige, mensgerichte en toekomstbestendige zorg. Wagenaar benadrukt dat organisaties niet hoeven te wachten tot alles perfect is, maar dat er juist samengewerkt wordt aan continue verbetering. “Onze aanpak richt zich op concrete, behapbare stappen. We beginnen met de grootste risico’s en maatregelen die direct effect hebben. Voor zorgorganisaties die veilige gegevensuitwisseling, betrouwbare zorgtechnologie en aantoonbare informatiebeveiliging serieus willen oppakken, is dit het moment om te starten.”

Vanboeijen biedt ondersteuning en begeleiding aan kinderen, volwassenen en ouderen met veelal complexe zorgvragen in wonen, werken, leren en vrije tijd. Meer informatie is te vinden op vanboeijen.nl

Meer informatie over **Start je Kickstart** is te vinden op startjekickstart.nl
Volg ons op LinkedIn.



Joost Wagenaar,
Senior adviseur Informatiebeveiliging en Privacy, ICTU



David Bos,
CISO, Vanboeijen

