INTRODUCTIE SPREKER:

SUZANNE VAN MIDDELKOOP

Suzanne van Middelkoop is adviseur informatiebeveiliging bij Topaz en werkte daarvoor in het Leids universitair medisch centrum. Een echte vakvrouw op het gebied van security in de zorg. Met haar consultancy-achtergrond heeft ze bij tal van zorgorganisaties een kijkje in de keuken genomen. Daardoor weet ze precies hoe je informatiebeveiliging niet alleen goed regelt, maar ook werkbaar maakt in de praktijk. Suzanne staat bekend om haar heldere en pragmatische aanpak, en weet zelfs de meest complexe vraagstukken begrijpelijk te maken voor iedereen binnen de organisatie – van werkvloer tot bestuur. Dat doet zij onder andere door bij te dragen aan projecten bij Sleutelnet. We legden haar 6 brandende vragen voor.

Wat is de belangrijkste les die jij hebt geleerd gedurende jouw carrière binnen informatiebeveiliging?

Dat informatiebeveiliging uiteindelijk altijd over mensen gaat. Natuurlijk is techniek belangrijk, maar de echte impact zit in hoe je medewerkers meeneemt, vertrouwen opbouwt en veiligheid onderdeel maakt van het dagelijks werk. Ik heb geleerd dat het vooral helpt om praktisch te blijven. Je hoeft niet meteen met een compleet beleidskader te komen — je kunt ook klein beginnen. Eén goede bewustwordingsactie of het verbeteren van een enkel proces kan al het verschil maken. Als je dat goed doet, volgt de rest vaak vanzelf.

Waar ben je het meest trots op in je werk van de afgelopen tijd?

Ik ben het meest trots op het feit dat we informatiebeveiliging tastbaar en werkbaar hebben gemaakt voor zorgprofessionals. Niet door met regels te zwaaien, maar door echt de verbinding te zoeken met de praktijk.

Als jij cybersecurity moest uitleggen met een metafoor uit de zorg, wat zou je dan zeggen?

Cybersecurity is als infectiepreventie in de zorg: je voorkomt dat kleine incidenten uitgroeien tot grote uitbraken. Je hebt beschermende maatregelen, alert personeel, en een goed protocol voor als het misgaat.

Waar krijg jij een beetje jeuk van als het over informatiebeveiliging gaat?

Als informatiebeveiliging wordt gezien als 'de afdeling die alles tegenhoudt'. Dan mis je de kern: goede informatiebeveiliging zit verweven in gedrag, keuzes en werkprocessen.

Het is niet iets wat de adviseur informatiebeveiliging of IT regelt of bepaalt.Het gaat juist om samen afwegingen maken: wat vinden we belangrijk om goed te beschermen? Welke risico's zijn we bereid te accepteren? Hoe behouden we een goede balans tussen werkbaar en veilig? Hiervoor is een goede dialoog cruciaal.

Wat vind jij momenteel de grootste blinde vlek op het gebied van informatiebeveiliging binnen de zorg?

Ketenafhankelijkheid, en dan niet alleen van IT-leveranciers, maar van álle partijen die essentieel zijn voor de continuïteit van zorg. Denk aan leveranciers van medische apparatuur, domotica, laboratoriumdiensten, of zelfs was- en maaltijdvoorzieningen. Veel van deze schakels zijn cruciaal, maar we hebben vaak beperkt zicht op hoe zij omgaan met informatiebeveiliging. Hoe goed zijn zij voorbereid op cyberdreigingen? Hoe snel kunnen zij herstellen bij een incident? Die kwetsbaarheid in de keten wordt nog te vaak over het hoofd gezien.

Wat kunnen deelnemers in het kort verwachten van de webinar?

In mijn deel van het webinar ga ik in op de praktische aanpak van incidentmanagement en leveranciersmanagement binnen de zorg. Ik laat zien hoe je je als organisatie kunt voorbereiden op incidenten zonder onnodig veel papierwerk, en hoe je op een werkbare manier grip houdt op leveranciers die belangrijk zijn voor de continuïteit van zorg. De focus ligt op toepasbare handvatten, gebaseerd op praktijkervaring.