Rick van der Kleij over cyberweerbare organisaties

“Cybersecurity is meer dan **technologie** alleen”

Cyberweerbare organisaties is hét thema voor de komende jaren. Dat is een van de redenen waarom Rick van der Kleij op 1 januari jongstleden is begonnen als lector cyberweerbare organisaties bij het Centre of Expertise Veiligheid & Veerkracht van Avans Hogeschool. We spreken met hem over zijn nieuwe functie en de taken die voor hem liggen.

Door Betty Rombout

Dacht je toen je jonger was al dat je in de cyberwereld terecht zou komen?
“Nee, niet direct. Maar het is natuurlijk wel een steeds belangrijker maatschappelijk thema, waar ook TNO, waar ik in deeltijd werk, zich op richt. Het is een gebied waarop ik denk met mijn expertise impact te kunnen maken. Het gaat vaak over technologie, maar met die technologie moeten mensen werken. Er dient nagedacht te worden over de rol van de mensen in dat systeem. Zo ben ik er dus als psycholoog ingerold.”

Waarom ben je de uitdaging bij Avans Hogeschool aangegaan?
“Enerzijds omdat Avans Hogeschool vindt dat er zo’n functie moet zijn. Kijk je naar het onderwerp cybersecurity, dan zijn volgens het CBS 2,2 miljoen mensen per jaar slachtoffer van cybercrime. Ook organisaties zijn slachtoffer van cyberincidenten. Ik heb hier onlangs zelf onderzoek naar gedaan. Dan zie je dat 11 procent van alle bedrijven aangeeft slachtoffer te zijn geweest van een cyberincident in het afgelopen jaar. Dit laat zien dat het best ‘groot’ is. Zeker als je het vergelijkt met traditionele criminaliteit, is het een onderwerp waar we iets mee moeten. Avans krijgt dan ook veel vragen over dit onderwerp. Een roep uit de praktijk dus. Om in de regio maar ook daarbuiten bedrijven meer cyberweerbaar te maken, heeft Avans besloten om daar toegepast onderzoek naar te gaan doen.
Anderzijds is de functie ook voor mij persoonlijk interessant. Ik ben cybersecurityonderzoeker. Mijn ambitie is om organisaties meer cyberweerbaar te maken. Dit is voor mij dan ook een mooie stap in mijn carrière. Ik krijg een onderzoeksgroep op dit onderwerp, zoals gezegd. Dit helpt om mijn ambitie waar te maken.”

Wat zijn cyberweerbare organisaties?
“Cyberweerbaarheid heeft te maken met het vermogen van organisaties om een aantal dingen te kunnen. Cybersecurity gaat meer over robuustheid, bescherming. Het zit meer aan de voorkant. We zien echter steeds meer dat incidenten niet te voorkomen zijn. Het idee van weerbaarheid is erop gebaseerd dat je leert omgaan met incidenten. Cyberweerbaarheid gaat dus enerzijds om het vermogen te anticiperen op dingen die gaan komen. Wat zijn de bedreigingen waar we iets mee moeten? Anderzijds gaat het om het vermogen te monitoren. Je moet weten dat het mis gaat, zodat je er

Cyberweerbaarheid gaat enerzijds om het vermogen te anticiperen op dingen die gaan komen en anderzijds om het vermogen te monitoren.

iets mee kunt doen. Ook dien je het vermogen te hebben om, als het mis gaat, adequaat te reageren. Ik merk in gesprekken dat hier niet altijd in geïnvesteerd wordt. Het gaat mis, wat ga je dan doen? Om cyberweerbaar te zijn, moeten organisaties ook het vermogen hebben om te leren. Gelukkig leren ze steeds vaker van incidenten. Er worden zelfs webinars gegeven door bedrijven die slachtoffer zijn geworden van ransomware. Ze zorgen niet alleen dat ze er zelf beter uitkomen, maar helpen ook andere partijen om cyberweerbaar te worden."

Wat zie je specifiek als jouw taak hierin?

"Kijkend naar de functie van lector sta ik voor het uitvoeren en initiëren van praktijkgericht onderzoek. Mijn kerntaken zijn hieraan gerelateerd. Maar ook onderwijs en de beroepspraktijk neem ik hierin mee. Ik heb een spilfunctie in de driehoek onderzoek, beroepspraktijk en onderwijs. Van belang voor de hogeschool is de professionalisering van docenten. Dat ik ze meeneem in het onderzoek. Dat ze competent worden in het doen van onderzoek. Datzelfde doe ik met studenten, waardoor we de kwaliteit van hen op een hoger plan kunnen krijgen. Dat ze later in hun werk onderzoek op waarde kunnen schatten, bijvoorbeeld. Ook als taak zie ik: studenten meegeven wat actueel is. Zorgen dat ze de juiste kennis en vaardigheden krijgen."

Centre of Expertise Veiligheid & Veerkracht

Het Centre of Expertise Veiligheid & Veerkracht onderzoekt samen met werkveldpartners hoe (aankomende) professionals weerbaar te maken zijn tegen allerlei vormen van criminaliteit. Directeur Nienke Fabries over de komst van de nieuwe lector: "Rick gaat zich primair richten op de digitale weerbaarheid van organisaties, in informele en formele netwerken, in branches en leveranciersketens. Samen met collega-lectoren en docent-onderzoekers vanuit de opleidingen Informatica, Bedrijfs- en Bestuurskunde, Integrale Veiligheidskunde en sociale en juridische studies gaat Rick werken aan het versterken van de cyberweerbaarheid van organisaties. Daardoor verbetert de betrouwbaarheid van informatiegestuurd werken en maatschappelijk en ethisch verantwoorde toepassingen van data en AI, in stedelijke en bedrijfsmatige omgevingen."

Hoe cyberweerbaar zijn organisaties?

"Ik heb al wat getallen genoemd. Soms maken bedrijven incidenten mee, maar leren ze er niet van. Andere daarentegen wel. Voor de overheid heb ik onlangs een onderzoek mogen doen. Is er een kloof tussen organisaties die het best goed doen, cyberweerbaar zijn, en die dat niet zijn? Ja,

Rick van der Kleij: "Bij de securitymanager zit veel specifieke vakkennis."

die kloof is er. De vragen in het onderzoek waren: 'Wie zijn die laatstgenoemde organisaties dan? Waarom nemen ze geen maatregelen om zichzelf beter te beschermen? Hoe kunnen we hierop reageren?' We hebben organisaties in Nederland gesegmenteerd op basis van psychografische kenmerken. Hoe verschillen bedrijven in gedrag en in belangrijke gedragsbepalers, zoals de overtuiging om zich wel of niet te beschermen. Je ziet vervolgens een grote groep van organisaties, voorlopers, die het wel op orde hebben. En ook gemotiveerd zijn om aan hun cyberweerbaarheid te werken. Maar 65 procent van de organisaties heeft dat nog niet. Je zou dit de achterblijvers kunnen noemen."

Verkort CV

Naam:	Rick van der Kleij
Geboren:	1973
Woonplaats:	Amersfoort
Opleiding:	PhD in psychologie
Functie:	Lector cyberweerbare organisaties, Centre of Expertise Veiligheid & Veerkracht van Avans Hogeschool (0,5 fte) en senior cybersecurity-onderzoeker bij TNO (0,5 fte)

Wat is daar dan de oorzaak van?

"Ze ondernemen niet digitaal veilig omdat ze niet altijd de kennis hebben om dat te kunnen doen. Of ze hebben de middelen niet. Of overtuigingen staan in de weg. Ze denken bijvoorbeeld dat ze niet in staat zijn om maatregelen te nemen. Of ze denken dat het toch niets uitmaakt. Die zijn juist onrealistisch optimistisch. Of vinden dat de overheid het maar moet regelen. Op deze 65 procent van de organisaties wil ik mij met mijn werk richten."

Hoe pak je dat dan aan?

"Ze helpen te investeren in genoemde vermogens om cyberweerbaar te worden. De vraag is: hoe krijg je ze zover dat ze dit ook doen? Door in te zetten op onderliggende gedragsbepalers. Denk bijvoorbeeld aan een bedrijf dat van mening is dat het hen niet overkomt. Dan zou je ze een soort van anticiperende spijt kunnen laten ervaren. Een collega-ondernemer laat je dan vertellen dat hij alles is kwijtgeraakt na een incident omdat hij of zij geen maatregelen had genomen. Zo laat je beslissers in bedrijven voelen hoe het is om slachtoffer te zijn."

Een hele klus dus...

"Dat wel, maar ik heb vooralsnog een aanstelling van acht jaar. Ik heb de tijd om samen met andere partijen in de regio en daarbuiten praktijkgericht onderzoek te gaan doen."

Is het niet moeilijk om dit voor elkaar te krijgen?

"Dat zou je kunnen zeggen. Maar er zijn gelukkig al heel wat samenwerkingsverbanden. Cybersecurity is in dit opzicht een kleine wereld. We kennen elkaar. De overheid investeert in cybersecurity. Er zijn een aantal onderzoeksgroepen op dit onderwerp. Bedrijven die er iets mee doen. We weten elkaar wel te vinden."

Betrekken jullie de securitymanager?

"Zeker. Bij die beroepsgroep zit veel specifieke vakkennis. En zie onze studenten, dat zijn straks de securitymanagers van de toekomst. We leiden ze op de juiste onderwerpen op. En ze leren dat cybersecurity meer is dan technologie alleen. Dat nemen ze mee naar de praktijk. We hopen dat die kennis dan ook weer terugvloeit naar het onderwijs, in de vorm van bijvoorbeeld gastcolleges."