Hij is door de wol geverfd in de security branche, als adviseur, publicist en gastdocent. Hij ontwikkelde een beveiligingsmethodiek en een softwaretool en nam het initiatief tot diverse overlegorganen. En dus is het eigenlijk niet meer dan logisch dat hij werd verkozen tot de vierde Security Professional van het Jaar. Hoogste tijd voor een gesprek met Arjen Appelman, van AES.

Arjen Appelman, Security Professional van het Jaar

‘Veiligheid begint bij jezelf’

■ Arjen Appelman: ‘Tien procent meer awareness zorgt voor zeventig procent meer veiligheid.’

Arjen Appelman volgde begin juni Harm van Dijk van de ING op als Security Professional van het Jaar. Die titel wordt eens in de twee jaar vergeven en is een initiatief van de VBN, de Vereniging Beveiligingsprofessionals Nederland. Dat is één van de twee beroepsverenigingen in de sector. Samen met ASIS Benelux vertegenwoordigt de VBN tussen de vijf- en zeshonderd professionals.

Hoe word je Security Professional van het Jaar?

‘Om te beginnen doordat je voorgedragen wordt door een lid of meerdere leden van de beide beroepsverenigingen. Een maand of twee voordat de verkiezing plaatsvindt worden de leden aangeschreven. Daaruit kwamen ongeveer 20 voordrachten. De jury, onder leiding van oud-minister Karla Peijs, pikte daar drie nominaties uit. Ik was één van die drie.’

Kende je de verkiezing?

‘Jazeker. Die wordt ook wel steeds bekender. Ik heb ook een goed contact met Harm van Dijk, mijn voorganger. Ik wist wel dat ik van de genomineerden waarschijnlijk de bekendste was. Ik publiceer regelmatig in Security Management, heb twee boeken geschreven en ben gastdocent op de HBO-opleiding Security Management. Uiteindelijk bleek dat een docent van die opleiding me heeft voorgedragen.’

Het winnen van deze titel behelst méér dan alleen een prijs ...

‘Als Security Professional van het Jaar word je automatisch voorzitter van de Nationale Denktank Integrale Beveiliging, de NDIB. Ik heb er vooraf al wel even over nagedacht of ik daar een mouw aan kon passen, mocht ik het worden. Ik wist van Harm dat hij daar veel tijd in heeft gestoken. En dat

moet natuurlijk wel te combineren zijn met mijn eigen bedrijf.'

Vertel daar eens wat meer over?

'AES (spreek uit: ees – red.) is behoorlijk bekend als adviesbureau, met name binnen de zorg en dan hoofdzakelijk in ziekenhuizen. Ik ben in 2001 voor mezelf begonnen en heb twee jaar later besloten me vooral op één sector te gaan richten. Dat werd de zorg. Daar was behoefte aan structuur, er waren veel incidenten en veel maatregelen, maar het ontbrak er aan visie en structuur. Ik heb inmiddels projecten uitgevoerd in 20 á 25 ziekenhuizen, waaronder vijf UMC's.'

Wat voor projecten zijn dat?

'Er is in de ziekenhuizen al veel gedaan aan beveiliging. Er is een afdeling beveiliging, er wordt gewerkt met pasjes, er hangen camera's. Maar het ontbreekt vaak aan een visie: hoe je al die maatregelen optimaal kunt laten samenwerken. Je moet ook bewust zijn van het feit dat je risico's veranderen. Wat ik dan doe is het ontwikkelen van een Security Management Systeem voor alle aanwezige maatregelen, waarmee een verbetertraject in gang wordt gezet.'

Die methodiek heb je zelf ontwikkeld?

'Ja. Daarbij werk ik volgens het principe: plan – do – check – act. Daarbij is er sprake van drie fundamenten: een risico-profiel, een beleidsplan beveiliging dat door de directie wordt vastgesteld en een meetinstrument, een incidentenregistratie en wachtrapportage systeem (database). Je moet zicht krijgen op wat er allemaal gebeurt. Lang niet alles wordt namelijk gemeld, dat is een issue waar heel veel organisaties mee kampen. Je moet middelen zoeken om de meldingsbereidheid te stimuleren.'

Je gaat uit van zes speerpunten. Zet die eens op een rijtje?

'Om te beginnen is er dus die informatievoorziening. Daarna komt de beveiligingsorganisatie. Iedereen moet zich ervan bewust zijn dat hij of zij een taak en een rol heeft op het gebied van veiligheid. Vervolgens krijg je de gedragscodes en huisregels, de kaders waar gasten en medewerkers zich aan moeten houden. Dan is er de awareness, de bewustwording dat er risico's zijn. Dit wordt vaak onderschat. Het is dan zaak om informatie te verstrekken en te confronteren. Dat sorteert het beste effect. Dit is het speerpunt waar we met z'n allen veel meer werk van moeten maken. Tien procent meer awareness zorgt voor zeventig procent meer veiligheid. Het vijfde speerpunt is het toegangsbeheer. Dit is eigenlijk het enige technische verbeterpunt waar we camera's, pasjes, sleutels tegenkomen. Ook voor dit speerpunt geldt dat toegangsbeheer méér is dan de technische oplossingen, waar nu de focus ligt. Die moet meer verschuiven naar de cultuur van de organisatie. Daar heb ik een visie voor uitgerold: een zoneringsplan, waarbij complete afdelingen en onderdelen afgesloten kunnen worden. Tot slot is er dan nog veilige zorg. Agressie en geweld vormen immers het voornaamste risico binnen de zorg. Met name de ernst van de agressie is daar fors toegenomen.'

'Toegangsbeheer is méér dan alleen technische oplossingen'

Hoe staan ziekenhuizen tegenover die maatregelen?

'Er zijn ziekenhuizen die niet of nauwelijks beeld hebben van wat er daadwerkelijk gebeurt. Maar er is al wel het nodige in gang gezet, met name door het CBRN-programma, voor het omgaan met gevaarlijke stoffen. Wij hebben daarbij veel ziekenhuizen, maar ook onderwijsinstellingen begeleid. Het is duidelijk zichtbaar dat met het CBRN-programma beveiliging naast patiëntveiligheid en informatiebeveiliging meer op de bestuursagenda terecht is gekomen. In een aantal gevallen hebben we dan ook CBRN-maatregelen zo breed uitgerold dat zij ook ondersteunend zijn aan de andere veiligheidsgebieden.'

Is die aanpak gemakkelijk door te voeren?

'Mijn aanpak staat wel bekend als 'het 7-stappenplan van Appelman'. Daar heb ik ook een boek over geschreven en verzorgen we workshops. Die stappen zijn: inventariseren, definiëren, concluderen, verbeteren, selecteren, implementeren en borgen. Zo ga je beveiliging als een continu proces zien. En dat is het ook. Dit is nooit af. UMC's zijn hier bijvoorbeeld nooit klaar mee. Het uitrollen van die trajecten kost tijd. Je bent zó een jaar bij een ziekenhuis bezig.'

En dan heb je ook nog een eigen softwaretool ontwikkeld?

'Dat is Syrus, een incidentenregistratie- en wachtrapportagesysteem, dat voor elke afdeling beveiliging grote voordelen heeft. Syrus wordt bijvoorbeeld gebruikt binnen de retail, het onderwijs, de overheid en natuurlijk ook de zorg. Syrus monitort onder andere alle incidenten binnen de organisatie. Daarmee kun je zo snel mogelijk daderpatronen en trends pinpointen, om ze te kunnen stoppen.'

In hoeverre opent je titel nu nieuwe deuren voor je?

'Ik ga er tijd en energie instoppen, probeer er het maximale uit te halen voor het vakgebied. Ik ga de dingen die ik naast mijn werk al deed nu doen als Security Professional van het Jaar. Ik moet als voorzitter mijn stempel op die Nationale Denktank gaan drukken. Wat mij betreft moet security naar de buitenwereld een wat minder afgesloten en behoudend gebied worden. Ik vind dat we meer transparant moeten zijn in wat er gebeurt.'

Waar ga je nog meer op inzetten?

'Ik vind burgerparticipatie een heel interessante ontwikkeling. Hoe kun je dingen die in de maatschappij gebeuren verhalen richting security. Veiligheid begint bij jezelf. Dat is ook mijn motto voor een workshop voor teamleiders facilitair van twee ziekenhuizen, die ik binnenkort mag geven. Wanneer een schoonmaker tijdens zijn werk iets ziet, moet hij dat melden bij de afdeling beveiliging. En andersom: als een beveiliger ziet dat er een lamp kapot is, moet die dat ook melden bij facilitair. Beveiligers krijgen meer taken en dat is prima, zolang dat maar niet ten koste gaat van hun primaire beveiligingstaken.' ■

TON DE KORT

verleng de levensduur van uw projectmeubilair

joustra

herstoffering

Voor:

Zorg

Kantoor

Overheid

Horeca

Onderwijs

U bent welkom op stand 3L.005

www.joustraherstoffering.nl

duurzaam - sociaal - besparen

EEN SPRONG VOORUIT **DOOR INNOVATIE**

Effectief | Betrouwbaar | Oplossingsgericht | Eenvoudig beheer | Eenvoudige installatie | Koppelingsmogelijkheden | Mifare/DESfire multiapplicatie kaarten

NIEUW

XS4mini

Modern design.
SALTO technologie.

SVN data-on-card ingebouwde technologie. Verlaag de onderhoudskosten door de noodzaak ervan weg te nemen.

Draadloos real-time controleren en beheren wie, welke deuren kan openen en op welk moment.

Gemakkelijke installatie en gebruik. De enige gaten die met de XS4 mini voor DIN sloten nodig zijn, zijn de twee naast het handvat.

Design. Klein en bescheiden van formaat in combinatie met een modern, helder LED-licht.

RFID. NFC & smartcard technologie maakt dat u alle fysieke behoeften van beveiliging in een enkele kaart kunt integreren.

Krachtige software om te bepalen wie door welke deur kan gaan en op welke tijden, terwijl hun toegang wordt geregistreerd.

Veiligheid & betrouwbare toegangscontrole 24/7. Beveilig en controleer vrijwel elke deur in uw gebouw.

SALTO
inspiredaccess

SALTO Systems - Amsterdam - Tel.: +31 206 353 100 - info.nl@saltosystems.com - **www.saltosystems.nl**