‘Informatie- en fysieke beveiliging onafscheidelijk’

Informatiebeveiligers en fysieke beveiligers lijken vaak in verschillende werelden te leven. Ze praten in de praktijk nauwelijks met elkaar. “Dat is niet goed”, meent VBN-er van de maand Douwe de Jong, die in het dagelijks leven zelfstandig beveiligingsadviseur is. De afgelopen jaren ontwikkelde hij verschillende initiatieven om ICT- en gebouwbeveiligers tot elkaar te brengen, maar het blijft vooralsnog een grote uitdaging.

Binnen de Vereniging Beveiligingsmanagers Nederland is Douwe de Jong een beetje een vreemde eend in de bijt. Hij heeft namelijk niet zoals verreweg de meeste leden fysieke beveiliging als achtergrond, maar informatiebeveiliging. Zijn interesse beperkt zich echter niet zoals bij de meeste ICT-beveiligers tot alleen het eigen gespecialiseerde vakgebied. Vandaar zijn lidmaatschap van de VBN.
De Jong is altijd actief geweest in de informatica en kreeg begin jaren negentig voor het eerst te maken met een beveiligingsvraagstuk. “Het uitvoeren van een risicoanalyse was een van de onderdelen van een automatiseringsklus op Schiphol. Dat boeide mij zodanig dat ik besloot mij verder in het vakgebied informatiebeveiliging te verdiepen.”

Haagse Methodiek Via beveiligingsconsultant Rinus Meelis maakte De Jong een aantal jaren later kennis met de Incidetar-aanpak uit de Haagse Methodiek van Ackx en Duijndam. “Bij de risicoafweging in de informatiebeveiliging kom je vaak niet verder dan wat kwalitatieve aanbevelingen, terwijl je bij fysieke beveiliging met meetbare grootheden werkt. Hoeveel minuten inbraakvertraging bereik je met het opwerpen van een bepaalde drempel? Dat intrigeerde mij bijzonder. Ik besloot dan ook de cursus aan de Haagse Hogeschool te volgen met als gevolg dat tijdens de rest van mijn carrière integrale beveiliging steeds belangrijker werd. Informatiebeveiliging en fysieke beveiliging mogen dan soms gescheiden werelden lijken, in de praktijk kunnen ze niet buiten elkaar.”
Om draagvlak voor zijn ideeën te creëren, richtte De Jong samen met VBN-lid Ronald Eygendaal van Getronics het PIB op, het Platform Integrale Beveiliging (*1) op. “Dat leek ons hard nodig, want als je met zowel fysieke als ICT-beveiligers te maken hebt, kun je niet anders concluderen dan dat die mensen moeizaam communiceren. Ons doel was een platform te bieden voor reeds bestaande integratie aspecten en het stimuleren van nieuwe initiatieven.”

Verantwoordelijkheid Voor informatiebeveiliging is een algemeen gangbare checklist van beveiligingsmaatregelen, de Code voor Informatiebeveiliging, uitgegroeid tot de internationale norm ISO27001. “Security-scans op basis van deze generieke indeling van beveiligingsmaatregelen zijn enorm behulpzaam voor iedereen die met beveiliging aan de slag wil.
Dat zie je weer niet in de wereld van de fysieke beveiliging. Daar doen vooral de onderzoeksbureaus geheimzinnig over hun security-scans en wordt dit hulpmiddel beschouwd als iets dat je vooral niet met anderen moet delen. De kennis over informatiebeveiliging bereikt echter niet het MKB altijd even goed. In die sector heeft fysieke beveiliging wel de aandacht, al of niet op last van verzekeraars, maar hangt informatiebeveiliging er een beetje bij. Grotere organisaties doen uiteraard wel aan informatiebeveiliging, maar dan staat dat weer los van de fysieke beveiliging. Meestal omdat beide taken onder de verantwoordelijkheid van verschillende personen vallen, die wat betreft mentaliteit weinig raakvlakken hebben. De interesses verschillen, er zijn andere opleidingstrajecten gevolgd en de gebruikte methodieken zijn nauwelijks te vergelijken. Toch is samenwerking tussen die twee partijen essentieel voor de continuïteit van de organisatie. Het is dus zaak om de beveiligingsdisciplines op de een of andere manier met elkaar te verbinden. Fysieke beveiliging, ICT-beveiliging, maar bijvoorbeeld ook arbo en bedrijfshulpverlening.”

Andere boeg Hoewel de BORG-regeling van het Centrum voor Criminaliteitspreventie en Veiligheid niet is ontworpen voor informatiebeveiliging, zag De Jong in deze systematische methodiek toch wel iets voor zijn primaire vakgebied. “Vanuit het PIB is een werkgroep opgericht die de BORG-regeling probeerde uit te breiden met aspecten voor informatiebeveiliging. Het bleek een moeizaam traject en het was alsof we appels met peren aan het vergelijken waren. Toen gooiden we het over een andere boeg. We gingen de structuur van BORG toepassen op informatiebeveiliging. We ontwikkelden analoog aan BORG een risicoklassenindeling voor informatiebeveiliging en een pakket maatregelen, dat vergelijkbaar met fysieke beveiliging (Organisatorisch, Bouwkundig en Elektronisch) was onder te verdelen in Organisatorische, Logische toegangs- en Continuïteitsmaatregelen. Elk van die maatregelen kreeg

'In de praktijk kom je de integrale aanpak van fysieke en informatiebeveiliging niet of nauwelijks tegen. En dat terwijl het zo belangrijk is dat beveiligingsmanagers weten wat er binnen de andere beveiligingstakken van hun organisatie gebeurt.'

een niveauaanduiding, als aansluiting op het tijdens de analyse vastgestelde risiconiveau. Als het op die manier lukt om risico's en maatregelen van beide disciplines naast elkaar te leggen en in elkaar te schuiven, kan je op beveiligingsgebied enorm veel bereiken. Ook bij grote organisaties trouwens. Bestudeer maar eens de werkwijzen bij fysieke en informatiebeveiliging en zoek naar de raakvlakken en de manier waarop beide disciplines elkaar zouden kunnen versterken."

Subsidieverhaal De activiteiten binnen het PIB en de genoemde werkgroep waren altijd 'liefdewerk oud papier'. "Op een gegeven moment hadden we er geen zin meer in. Het moet wel een keer opgepakt worden. Vorig jaar was er echter weer even een opleving. We hoorden van een subsidieregeling om een informatiebeveiligingsstandaard voor het MKB te ontwikkelen. Syntens heeft zich opgeworpen om betrokken partijen waaronder EZ, het MKB, VNO-NCW en ECP.nl bij elkaar te krijgen, maar het is niet gelukt, vooral door gebrek aan actieve betrokkenheid bij het MKB. Ook is het niet gelukt aan te sluiten op het programma Veilig Ondernemen van het CCV. Dat programma is gericht op vooral regionale en collectieve initiatieven om criminaliteit het hoofd te bieden. Informatie komt echter via de digitale snelweg binnen en het maken van afspraken met ICT-partners is complexer. Toch zie ik dit nog als een mogelijkheid; het is altijd makkelijker om aan een bestaand programma iets ▸

toe te voegen, dan van meet af aan te moeten beginnen. Een nieuw plan vanuit het Platform voor Informatiebeveiligers (PvIB, *2) is het opstellen van een zogenoemde Expertbrief over integrale beveiliging. Ik roep geïnteresseerde lezers op naar www.pvib.nl te kijken. Daar zijn voorbeelden te vinden van Expertbrieven en kunnen zij zich opgeven om een bijdrage te leveren."

Toenadering Van de initiatieven als het PIB, dat De Jong een beetje lachend als zijn hobby omschrijft, zou de gecertificeerde informaticadeskundige niet kunnen leven. Hij doet dat dan ook naast zijn reguliere werk dat bestaat uit informatiebeveiligingsprojecten voor overheden en ondernemingen met daarnaast serviceverlening voor in het verleden door hem ontwikkelde automatiseringsapplicaties voor onder andere de thuiszorgsector. Hoewel hij nog altijd de integrale aanpak omarmt, houdt hij zich hoofdzakelijk met informatiebeveiliging bezig. "Dat moet ik fysieke beveiligers nageven. Die doen meer aan informatiebeveiliging dan informatiebeveiligers aan fysieke beveiliging doen. Fysieke beveiligers zijn ook eerder geneigd om toenadering te zoeken tot informatiebeveiligers dan andersom. Ook de VBN kent een vakgroep informatiebeveiliging. Toch kom je de integrale aanpak van fysieke en informatiebeveiliging in de praktijk niet of nauwelijks tegen. En dat terwijl het zo belangrijk is dat beveiligingsmanagers weten wat er binnen de andere beveiligingstakken van hun organisatie gebeurt."

Toekomst De Jong durft geen toekomstvoorspellingen te doen. "Als ik nu terugkijk hadden onze beroepsgenoten vijftien jaar geleden met geen mogelijkheid kunnen bevroeden hoe de wereld er nu uitziet. Ik heb het dan vooral over internet. Ik denk dat ik nu van mijn stoel zou vallen als ik kon zien wat er over vijftien jaar gebeurt. Ik weet het niet, maar ik ben ervan overtuigd dat de maatschappij enorm zal veranderen. Zeker op het gebied van ICT. Wat de beveiliging betreft, wordt het alleen maar spannender. Mensen willen steeds meer controle, terwijl anderen zich daar zorgen over maken. Ik ben benieuwd wat er maatschappelijk staat te gebeuren. Wat kan je straks nog uit de openbaarheid houden en hoe zal de overheid omgaan met de bescherming van de burger? Wat wordt het leefbare compromis? De tijd zal het leren."

■ Vincent Vreeken
Vincent.Vreeken@beveiliging.nl

***1) Platform Integrale Beveiliging (PIB) is de benaming voor een groep security specialisten die tussen 2002 en 2005 op ad hoc basis bij elkaar zijn gekomen; vanuit dit platform is de werkgroep Borg & ICT actief geweest.**

***2) Platform voor Informatiebeveiligers (PvIB, www.pvib.nl). Deze beroepsvereniging bestaat sinds kort en is ontstaan uit het samengaan van het Genootschap voor Informatiebeveiligers (GvIB) en het Platform Informatiebeveiliging (PI).**

PERSONALIA

Douwe de Jong

Douwe de Jong heeft ruim 35 jaar ervaring met automatisering en is vanaf 1984 zelfstandig werkzaam. Hij is gecertificeerd informaticadeskundige en lid NVBI. De NVBI is een beroepsvereniging van onafhankelijke en deskundige professionals die werken op het snijvlak van IT, bedrijfskunde en recht. De laatste vijftien jaar ligt het accent op beveiligingsactiviteiten met aandacht voor een integrale benadering. Op dit moment is De Jong werkzaam als security adviseur bij een internationale bouwonderneming en als informatie specialist bij zorginstellingen met uiteraard aandacht voor informatiebeveiliging in de zorg, de NEN7510.