

Informatiebeveiliging én fysieke beveiliging

“de disciplines kunnen niet zonder elkaar”

In de zomernummers van Informatiebeveiliging, het maandblad van het Genootschap voor Informatiebeveiligers, zijn drie artikelen verschenen over raakvlakken tussen informatiebeveiliging en fysieke beveiliging. Beide beveiligingsdisciplines zijn van oorsprong verschillend maar krijgen in toenemende mate met elkaar te maken. Een systeembeheerder die ook informatiebeveiliging in zijn takenpakket heeft is in veel opzichten een andere vakman dan een facilitair manager die ook verantwoordelijk is voor de veiligheid van een gebouw. Informatiebeveiligers en security managers zijn verschillende specialisten die vanuit verschillende invalshoeken beveiligingstaken uitvoeren en in veel gevallen ook nog eens organisatorisch ver van elkaar af staan. Toch heeft het uiteindelijk resultaat, de verschillende beveiligingsplannen, raakvlakken.

En wat te denken van begrippen als integrale beveiliging en integrale veiligheid! Het mag dan een hype zijn, het geeft wel aan dat veiligheid en beveiliging van mens, gebouw en IT iets gemeenschappelijks hebben. Bijvoorbeeld gezamenlijke awareness-trajecten of beheerinstrucities waarbij rekening wordt gehouden met de veiligheid van werkplek(gebouw), middelen (IT) én de veiligheid van de mens (ARBO). Methoden en technieken voor beveiliging pretenderen steeds vaker een aanpalend gebied te bestrijken. Treffend voorbeeld is de titel van een artikel in Informatiebeveiliging Praktijkjournaal van 1999 waarin het gaat om een methode voor fysieke beveiliging: "De Haagse Methodiek omarmt informatiebeveiliging". In het algemeen zie je dat in informatiebeveiligingsperiodieken regelmatig aandacht wordt besteed aan fysieke beveiliging en andersom geldt dat ook. Daarbij moet wel worden aangetekend dat de hang naar een uitdijend vakgebied soms eerder voortkomt uit de behoefte om de markt uit te breiden dan dat het inhoudelijke relevantie heeft.

In een drietal artikelen zal worden ingegaan op de raakvlakken tussen informatiebeveiliging en fysieke beveiliging en de noodzaak om op zijn minst rekening met elkaar te houden en daar waar mogelijk samen te werken. Niet dat informatiebeveiliging en fysieke beveiliging even gelijktijdig kunnen worden aangepakt, wel moet worden gestreefd naar een zodanige vorm van samenwerking dat het resulteert in evenwichtige, op elkaar afgestemde beveiligings- en veiligheidsmaatregelen. Doel van de artikelen is om begrip voor elkaars denkwijze, betrokkenheid bij elkaars werkwijze en kennis van elkaars hulpmiddelen te stimuleren.

In de artikelen wordt uitgegaan van twee benaderingswijzen voor beveiliging: een benadering volgens methodisch onderzoek en een benadering volgens een basis beveiligingsniveau, de zogenaamde baselinebenadering. *Het eerste artikel* beschrijft enkele methoden die in gebruik zijn voor de fysieke beveiliging en vergelijkt die met de afhankelijkheids- en kwetsbaarheidsanalyse (A&K-analyse) voor de informatiebeveiliging. Het aspect 'mens' cq Arbo komt niet expliciet aan bod, anders dan als logisch vervolg op informatiebeveiliging of fysieke beveiliging.

Het tweede artikel gaat verder in op de methodische benadering. Uitgangspunt is dat vanuit de vaardigheden die in een bepaalde situatie aanwezig zijn ook het aanpalende vakgebied kan worden meegenomen. Wat het vertrekpunt is zal afhankelijk zijn van aard én ervaring van omgeving en betrokkenen. Dat de Security Management-opleiding in De Haagse Methodiek oog heeft voor informatiebeveiliging is van wezenlijk belang; de zogenaamde OBE-meetlat voor Organisatorische, Bouwkundig en Electronische maatregelen zou kunnen worden uitgebreid met de I-component van Informatietechnologie. Dit artikel heeft als vertrekpunt informatiebeveiliging en laat zien dat de A&K-analyse, een methodische aanpak voor informatiebeveiliging, ook kan worden gebruikt voor fysieke beveiliging. Daarbij worden nieuwe termen geïntroduceerd die meer aansluiten op de fysieke beveiliging; zo is het onderzoeksobject geen informatiesysteem maar een risicoplaats. Evenals in het Handboek A&K-analyse wordt ook hier aangegeven welke hulpmiddelen kunnen worden ingezet om het methodisch onderzoek te ondersteunen; die hulpmiddelen maken deel uit van de fysieke beveiligingsmethoden zoals in het eerste artikel zijn beschreven.

Een derde artikel is gewijd aan de baselinebenadering; aan de normering zowel voor fysieke beveiliging als informatiebeveiliging die ten grondslag ligt aan een basisbeveiligingsniveau. De overlap informatiebeveiliging en fysieke beveiliging wordt vanuit twee invalshoeken beschreven. In de eerste plaats door betrouwbaarheidseisen te vertalen naar veiligheidseisen en daar een basismaatregeleniveau aan te koppelen. In de tweede plaats vanuit de fysieke beveiliging; er zijn initiatieven om bij BORG-regelingen rekening te houden met informatiebeveiliging. Met andere woorden, bij de risicoklasse-indeling die de basis is voor de BORG-regelingen, niet alleen uit te gaan van bouwkundige, elektronische en compartimenteringseisen maar daar ook de IT bij te betrekken. Als een gebouw moet voldoen aan risicoklasse x is dat ook afhankelijk van de ICT-activiteiten die daar worden uitgevoerd.

Aanleiding voor de artikelserie is een aanpak bij de Nederlandse Politie waarbij vanuit de informatiebeveiliging aandacht is besteed aan fysieke beveiliging; de voorbeelden zijn dan ook ontleend aan de politie-omgeving.

In **Informatiebeveiliging 2002** zijn de artikelen verschenen onder de gemeenschappelijke titel:

Fysieke en informatiebeveiliging

In de edities 4, 5 en 6 met de volgende subtitels:

deel I - *"Methodes voor fysieke en informatiebeveiliging vergeleken"*
Douwe de Jong

deel II - *"A&K-analyse ook voor fysieke beveiliging"*
Douwe de Jong

deel III - *"BORG-regelingen en ICT"*
Ronald Eyendaal en Douwe de Jong