

# Van beveiliging naar **INTEGRALE BEVEILIGING**

Door: Ronald Eygendaal,  
voorzitter Vakgroep ICT beveiliging.

## ORGANISATIE VAN BEVEILIGING

Het onderwerp beveiliging heeft door de aard van de verantwoordelijkheden van betrokken partijen een aantal tegenstrijdige belangen. Aan de ene kant zien we afdelingen als facilitair management of algemene zaken, waar beveiliging vaak ook onderdeel van uitmaakt. Aan de andere kant zien we de IT afdelingen waar informatiebeveiliging belegd is. Het beheer van communicatiemiddelen zoals telefoons, de PABX en autotelefoons is vaak bij een van beide afdelingen ondergebracht. Daarnaast spelen de gebruikers van een gebouw of computersysteem een zeer belangrijke rol. Zij willen ongestoord toegang tot hun (elektronische) werkplek hebben zonder moeilijke procedures.

## WAT IS NU EIGENLIJK BEVEILIGING?

Eerst maar even stelling nemen: 'De ultieme beveiliging bestaat niet'. Altijd zal er een manier zijn om een pc of netwerk, een toegangscode of een pinpas beveiliging op een of andere manier te misbruiken, dat wil zeggen het ergens anders voor gebruiken dan waarvoor het eigenlijk bedoeld en gedefinieerd is. Zoals bekend is bepaald de samenhang tussen de beveiligingsmaatregelen de uiteindelijke beveiliging. Een consistent bedrijfsbreed integraal beveiligingsbeleid is dus van cruciaal belang. Door concessies te doen aan het niveau van beveiliging ontstaan voortdurend discussies tussen de betrokken partijen. De gebruiker wil totaal vrije toegang. De beheerder wil volledige controle en de Security Manager wil een beveiligde omgeving. Compromissen zullen dus voor een aanvaardbare oplossing moeten zorgen.

## INTEGRAAL SECURITY MANAGER

Vanuit deze optiek moet het mogelijk zijn de verantwoordelijkheden over beveiligingsaspecten van beveiliging te beleggen bij een Integraal Security Manager in het bedrijf. Uiteraard blijft het lijn-

management eindverantwoordelijk. De Security Manager kan dan op alle niveaus van het bedrijf optimaal en onafhankelijk adviseren en opereren. Om dit te bereiken moet de Integraal Security Manager als staffunctionaris, direct onder de directie, in de organisatie zitten.

Voordat de Integraal Security Manager tot het innemen van een standpunt zal overgegaan, moet worden geïnventariseerd wat de belangen van de diverse groepen zijn; hoe legitiem ze zijn en wat de consequenties voor het bedrijfsproces zijn. Ook moet per belangengroep aangeven worden waar de verantwoordelijkheid van de groepen ligt. Het is zelfs mogelijk dat meerdere groepen over hetzelfde stuk verantwoording zullen moeten dragen en nemen.

Het risico dat door tijdsdruk, prioriteitsstelling, capaciteitsproblemen, kennisleemtes, vooroordelen en het klakkeloos overnemen van niet onderbouwde stellingen en dogma's, hele bedrijfsprocessen minder efficiënt kunnen werken of in het uiterste geval compleet worden lamgelegd, wordt hierdoor geminimaliseerd en zelfs beheersbaar.

## INFORMATIE EN COMMUNICATIETECHNOLOGIE

De Informatie en Communicatie Technologie (ICT) vakgroep van de VBN hoopt dat de Security managers van nu in de loop van de tijd kunnen groeien naar de Integraal Security manager. Belangrijk voor dit groeipad is de kennis en ervaring die de Integraal Security manager opdoet op gebied van ICT beveiliging.

De ICT vakgroep tracht dit te bereiken door het geven van lezingen, voorlichting en workshops over dit onderwerp.

Dit stuk is geschreven met het doel de verschillende standpunten en belangen, die waarde te geven die ze mijns inziens verdienen.

*'De ultieme  
beveiliging  
bestaat niet'*