Integrale beveiliging

Dikke muren en *firewalls*

Informatiebeveiliging, fysieke beveiliging en personele beveiliging hebben hetzelfde doel: bescherming van de bedrijfsprocessen. Integraal beveiligen is meer dan een optelsom van deze drie beveiligingsdisciplines. Als men in een vroeg stadium de veiligheidseisen van deze drie disciplines op elkaar afstemt, ontstaat een evenwichtig maatregelenpakket.

Auteur **Douwe P. de Jong RSE**, beëdigd informaticadeskundige NVBI en ingeschreven in het Register Security Experts Nederland (SERN)

In reclame-uitingen, publicaties of aankondigingen van seminars komen we steeds vaker de begrippen 'integrale beveiliging' of 'integrale veiligheid' tegen. De betekenis van deze begrippen is verre van eenduidig. Integrale *veiligheid* wordt veelal gebruikt als het gaat om arbeidsomstandigheden. Bij integrale *beveiliging* is het vertrekpunt meestal informatiebeveiliging en fysieke (object)beveiliging, met aandacht voor het personele aspect in relatie tot een incident. In dit artikel richt ik mij op de integrale beveiliging van object, informatie en mens.

'Integreren' is volgens het woordenboek 'het maken, groeien, samenbrengen tot of opnemen in een groter geheel; het maken tot een eenheid'. Om te kunnen integreren, is aanpassing nodig van het te integreren deel in het grotere geheel. Integreren is niet simpelweg een optelsom van disciplines.

Beveiliging van object, informatie en mens heeft eenzelfde doel: de bescherming van de bedrijfsprocessen. Bedrijfsprocessen zijn afhankelijk van het goed functioneren van informatiesystemen, de beschermende werking van objecten als terrein, gebouw en afgesloten ruimte, en het welbevinden van de medewerkers. Dit alles komt ook de kwaliteit van het bedrijfsproces ten goede.

Afstemming

De drie beveiligingsdisciplines resulteren in een stelsel van maatregelen dat is afgestemd op de te beschermen belangen. Men maakt risicoafwegingen door het onderkennen van afhankelijkheden en dreigingen, rekening houdend met wet- en regelgeving. Bij informatiebeveiliging spreekt men over de betrouwbaarheidseisen, fysieke beveiliging kent veiligheidscriteria en bij de personele beveiliging gaat het om de wettelijke Arbo-eisen. Door in een vroeg stadium de eisen voor informatiesystemen, gebouw en personeel op elkaar af te stemmen, ontstaat 'als vanzelf' een evenwichtiger maatregelenpakket.

Ter illustratie het volgende. Het stellen van veiligheidseisen aan ruimten kan tot gevolg hebben dat men een gebouw indeelt in zones, waarbij de verschillende zones worden afgeschermd door een elektronisch toegangsbewakingssysteem. Betrouwbaarheidseisen voor informatiesystemen kunnen leiden tot zowel fysieke als logische toegangsbeveiligingsmaatregelen. Voor ICT-werkstations in een zone waartoe alleen medewerkers met een

persoonlijke, geautoriseerde pas toegang hebben, kan de fysieke toegangsbeveiliging tot het werkstation wat minder zwaar zijn. Bovendien kan men de fysieke toegang tot ruimte én werkstation integreren. Maar extra beveiligde zones mogen dan zijn voorzien van geavanceerde, elektronische toegangsdeuren, men moet wel voldoen aan de Arbo-eis van een onbelemmerde vluchtweg in geval van een calamiteit.

Informatiebeveiliging

In zijn algemeenheid geldt dat vanuit de technische beveiligingshoek meer behoefte is aan integrale beveiliging dan vanuit de invalshoek informatiebeveiliging. Beveiligingstechniek raakt steeds meer verweven met informatietechnologie, en daarmee is de overstap naar informatiebeveiliging al snel gemaakt. Informatiebeveiliging kent weliswaar de component fysieke beveiliging, maar het accent ligt op de fysieke bescherming van de ICT-componenten. De behoefte om 'over de schutting' te kijken, is minder groot.

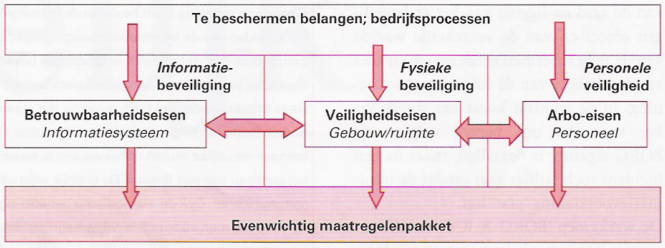
Bij de overheid is in grote lijnen sprake van de volgende situaties:

- Bij instellingen waar informatietechnologie een grote rol speelt en fysieke beveiliging geen aparte functie is maar tot het takenpakket van de informatiebeveiliger behoort, is men geneigd om fysieke beveiliging onder te brengen bij de informatiebeveiliging door gebruik te maken van dezelfde gestructureerde aanpak.
- Daarnaast zijn er instellingen waar fysieke beveiliging expliciet op de agenda staat en waar *security managers* worden opgeleid om fysieke beveiliging methodisch op te pakken. De fysieke beveiliging en informatiebeveiliging zijn hier aparte trajecten en eventuele integratie is afhankelijk van persoonlijke initiatieven. De in dit artikel opgenomen praktijkvoorbeelden (zie kader, pag.18) geven aan wat hiervan het effect kan zijn. Het integrale aspect wordt steeds vaker al verankerd in het beleid en in enkele gevallen wordt gewerkt aan een integraal beoordelingskader.

Platform Integrale Beveiliging

De integrale beveiliging bij een overheidsinstelling heeft geleid tot de artikelenserie 'Informatiebeveiliging én fysieke beveiliging; de disciplines kunnen niet zonder elkaar'.[1] Reacties op deze artikelen

Figuur 1. De drie beveiligingsdisciplines



waren de aanleiding voor de oprichting van het Platform Integrale Beveiliging.[2] De doelstelling van het Platform is om initiatieven rond integrale beveiliging te verzamelen en te stimuleren.

Voor grote bedrijven is moeilijk aan te geven hoe men omgaat met integrale beveiliging, maar wellicht is dit in grote lijnen zoals is beschreven voor de overheid. Naarmate bedrijven kleiner worden, ontstaat wel een duidelijke trend. Omdat men voor de fysieke beveiliging gewend is uit te gaan van normen en standaarden en dergelijke middelen onvoldoende beschikbaar zijn voor de informatiebeveiliging, is een veelgehoorde klacht dat de ICT-beveiliging onder de maat is en met name het midden- en kleinbedrijf (MKB) de kop in het zand steekt.[3] Hier ligt de grote uitdaging voor een integrale aanpak.

Een stap verder dan integrale beveiliging is integrale *kwaliteit*. In een uitgave van het Nederlands Normalisatie-Instituut worden managementsystemen voor kwaliteit (beveiligingscriteria maken deel uit van de kwaliteitscriteria), arbo (veiligheid) en milieu met elkaar vergeleken, inclusief een praktische handleiding voor integratie van de drie systemen.[4]

Normen en standaards

Vanuit het eerder genoemde Platform probeert de werkgroep 'Borg & ICT' een vertaalslag te maken van de BORG-regeling voor de fysieke beveiliging naar de Code voor Informatiebeveiliging. Het ziet ernaar uit dat de Code voor Informatiebeveiliging een geaccepteerde standaard wordt voor het hele werkgebied informatiebeveiliging. De brontekst is zelfs een wettelijk vastgelegde wereldwijde standaard. De Code bevat een groot aantal beveiligingsmaatregelen; het eerste deel kan worden gebruikt als leidraad voor implementatie, het tweede deel als norm. Dit tweede deel is van belang voor controle en certificering.

De Code is omvangrijk en algemeen geaccepteerd bij grote instellingen. Al jaren worden initiatieven ontplooid om de Code ook toegankelijk te maken voor het MKB en de iets grotere bedrijven, maar het effect is nog minimaal. Over de Code is erg veel geschreven. Aanbevelenswaardig is de Praktijkgids Code, met speciale aandacht voor auditing en certificatie.[5]

Het Nationaal Centrum voor Preventie (NCP) neemt een centrale plaats in als het gaat om normering en regelgeving voor fysieke beveiliging. Het NCP is het publiek-private samenwerkingsverband voor veiligheid en beveiliging in Nederland en stelt zich 'kwaliteitshandhaving en verbetering van beveiliging en veiligheid in brede zin' ten doel. Het NCP heeft diverse producten en certificatieregelingen ontwikkeld en op de markt gebracht, zoals de BORG-regelingen voor technische bedrijven. Binnen deze BORG-regelingen zijn er richtlijnen voor woningen, winkels, showrooms, onderwijsinstellingen en installatievoorschriften voor alarmapparatuur.

Op basis van een risicoklassenindeling wordt het risico ingeschaald in een risicoklasse (1,2,3 of 4). Voor elke risicoklasse is een (standaard) beveiligingsklasse weergegeven waarin de (samenhang) van de niveaus van de te treffen beveiligingsmaatregelen wordt omschreven. Binnen deze samenhang dient het BORG-beveiligingsbedrijf aan te geven welke beveiligingsmaatregelen worden ingezet voor het onderhavige risico. Zo is een rechtstreeks verband gelegd tussen de vereiste beveiligingsklasse en de bijbehorende combinatie van beveiligingsmaatregelen.

Maar waar blijft bij BORG de informa- >>

tiebeveiligingscomponent? Het probleem is dat de risicoklassenindeling wel uitgaat van de aard en ligging van het te beveiligen object en van de verzekerde waarde van de te beschermen goederen, maar niet van het belang van de informatievoorziening. In de praktijk komt het steeds vaker voor dat een bedrijf volgens de BORG-regeling is beveiligd, maar na een incident toch failliet gaat omdat de informatievoorziening 'plat' ligt.

De werkgroep 'BORG & ICT' wil dit najaar tot een aanpak komen waarbij de risicoklassenindeling niet alleen rekening houdt met het belang van de informatievoorziening maar ook – afhankelijk van het gewenste beveiligingsniveau – de link legt naar beveiligingsproducten voor informatiebeveiliging. De basis voor het benoemen van productclusters is de Code

voor Informatiebeveiliging. Zo worden twee geaccepteerde elementen van de verschillende disciplines aangepast en op elkaar afgestemd.

Tips

Beveiliging integraal benaderen is geen hoogstandje, maar een manier van denken en werken waarmee men direct kan beginnen. Enkele praktische tips:

- Bedenk dat het voor iemand die informatie wil stelen wel eens eenvoudiger kan zijn om een fysieke inbraak te plegen (PC of informatiedragers meenemen), dan in te dringen in een informatiesysteem. Beveiligingsmaatregelen staan niet op zichzelf; het is bijna altijd een samenspel van technische, bouwkundige en vooral organisatorische maatregelen. In dit verband ook de boodschap: geen beveiligingsmaatregelen zonder nalevingsmechanisme.
- Stem een eventuele zone-indeling en ICT-toegangsbeveiligingsmaatregelen op elkaar af. Dit voorkomt overlap van technische en bouwkundige maatregelen.
- Voer beveiligingsactiviteiten die herkenbaar moeten zijn voor de medewerkers op de werkvloer gezamenlijk uit. Denk daarbij aan bewustwordingsactiviteiten en veiligheidsprotocollen. Maak voor werkplekken uniforme, op elkaar afgestemde instructies als het gaat om afsluitdiscipline voor ruimtes, *clear-desk policy* voor ICT-apparatuur en veiligheid in het kader van de Arbo-wet.
- Overweeg een centraal meldpunt voor alle beveiligingsincidenten. Het moet voor betrokkenen uitnodigend zijn om incidenten te melden. Maak 'misbruik' van incidenten door de effecten breed uit te meten en geef aan hoe men het had kunnen voorkomen. Schroom niet gebruik te maken van andermans leed. De aanslagen van 11 september 2001 hebben in beveiligingsland heel wat teweeg gebracht.
- Voer kostenbesparing en efficiëntie aan als argumenten om integrale beveiliging op de agenda te krijgen. <<

Praktijkvoorbeeld 1

Casus: Een instelling heeft besloten de beveiliging integraal aan te pakken. Er is veel geïnvesteerd in het opleiden van de informatiebeveiligingsspecialist en de security manager. Beide specialisten krijgen de opdracht gezamenlijk een integraal beveiligingsconcept te ontwikkelen.
Resultaat: Van samenwerking komt niets terecht: er is geen affiniteit met elkaars werkwijze, er ontstaan irritaties, ieder trekt zich terug op zijn eigen (vertrouwde) vakgebied en alles blijft bij het oude.
Reden: Beide beveiligingsdisciplines zijn totaal verschillend; je wapenen tegen boeven door het aanbrengen van dikke muren of hekwerken is wezenlijk anders dan boeven buiten de deur houden door het plaatsen van een *firewall*. De praktijk wijst uit dat beide disciplines niet vanzelfsprekend met elkaar communiceren. Ook de methodische benadering van beide vakgebieden is anders. Het ligt niet voor de hand dat men elkaars werkwijze begrijpt, laat staan dat een vorm van synergie optreedt.
Les: Integratie gaat niet vanzelf en vereist de nodige voorbereiding.

Praktijkvoorbeeld 2

Casus: Een instelling heeft besloten de beveiliging integraal aan te pakken. Een systeembeheerder en een facilitair manager worden gevraagd mee te werken. Men start met een bewustwordingstraject van een jaar. De medewerkers krijgen een gezamenlijke werkruimte vlakbij de personeelsingang en hen is gevraagd zoveel mogelijk de deur open te laten staan en gesprekken aan te gaan met collega's. Er worden opleidingstrajecten opgestart.
Resultaat: Intensieve discussies met collega's, een groeiend beveiligingsbewustzijn en brede acceptatie voor integrale aanpak. Beide beveiligingsmedewerkers krijgen steeds meer affiniteit met elkaars vakgebied.
Reden: De aanpak is eenvoudig en laagdrempelig.
Les: Integratie kan niet zonder acceptatie, zowel bij de specialisten als bij de medewerkers. Synergie-initiatieven ontstaan vanaf de werkvloer.

Executive summary Het etiket integraal zal dan soms oneigenlijk worden gebruikt, er zijn genoeg signalen die wijzen op een werkelijk integrale benadering van het beveiligingsvraagstuk. Integrale beveiliging is een must! Zonder integrale benadering hebben we wel de beveiliging van ons aandachtsgebied op orde, maar verdrinken we in het bluswater van de buren. De bindende factor is de continuïteit van de bedrijfsvoering, gezamenlijke randvoorwaarden zijn wet- en regelgeving. Door samen te werken, worden de maatregelen van de verschillende beveiligingsplannen op elkaar afgestemd. Maar let op: integratie is geen stamppotconcept. Het is een uitdaging om een evenwicht te vinden, de specifieke kenmerken van de verschillende disciplines te koesteren en de raakvlakken uit te buiten.

Noten

1 D.P. de Jong. Informatiebeveiliging én fysieke beveiliging. *Informatiebeveiliging* 2002, nrs. 4, 5 en 6. Academic Service. De drie artikelen zijn op te vragen door te mailen naar douwep@planet.nl.
2 Zie www.platformintegralebeveiliging.org; de site is nog in ontwikkeling en bevat een aantal verwijzingen naar interessante artikelen.
3 Zie *Automatiseringsgids*, juni 2003.
4 Nederlands Normalisatie-Instituut. Toepassing van normen bij integratie van managementsystemen. ISBN 90 5254 08209.
5 Ernst J. Oud. Praktijkgids Code voor informatiebeveiliging. ISBN 90 5261 427x.