BORG-REGELINGEN EN IT

IN EEN ARTIKEL IN HET TIJDSCHRIFT INFORMATIEBEVEILIGING WORDT ER BIJ DE BRANCHES IT EN BEVEILIGING VOOR GEPLEIT MEER OOG TE KRIJGEN VOOR ELKAARS VAKGEBIED, MEER KENNIS TE HEBBEN VAN ELKAARS HULPMIDDELEN EN MEER SAMEN TE WERKEN. DAT ZAL RESULTEREN IN BETER OP ELKAAR AFGESTEMDE VEILIGHEIDSMAATREGELEN.

In dit artikel leggen Douwe de Jong en Ronald Eygendaal het accent op de pragmatische aanpak: een benadering waarbij een set van beveiligingsmaatregelen geldt die beantwoordt aan een bepaald niveau van veiligheid en betrouwbaarheid. Voor de fysieke beveiliging zijn dat onder meer de BORG-regelingen. Maar wordt daarbij wel voldoende rekening gehouden met IT en de bijbehorende informatie?

Zowel voor informatiebeveiliging als voor fysieke beveiliging geldt dat de bedrijfsprocessen - de te beschermen belangen - centraal staan. Er is een risicoafweging nodig om te komen tot betrouwbaarheids- en veiligheidseisen als opmaat voor de te treffen beveiligingsmaatregelen. Risicoanalyse is een arbeidsintensieve bezigheid maar in veel gevallen kan ook worden volstaan met quick scans.

Voor de fysieke beveiliging is het uitvoeren van quick scans en het toepassen van genormeerde producten gemeengoed; bijvoorbeeld de risicoklassenindeling voor de BORG-regelingen en beveiligingsproducten die voldoen aan SKG-normen (Stichting Kwaliteitsborging Gevelelementen).

Vanaf de introductie van de Code voor Informatiebeveiliging is bij informatiebeveiliging een omslag te zien; de Code wordt steeds vaker als norm gebruikt bij het bepalen van een basisbeveiligingsniveau en TNO geeft Common Criteria (ISO norm) Certificaten uit voor IT-beveiligingsproducten.

Dit artikel verscheen eerder in uitgebreidere vorm in het tijdschrift *Informatiebeveiliging* no. 6, 2002 en maakte daar deel uit van een driedelige serie over fysieke beveiliging en informatiebeveiliging.

BEVEILIGINGSTENDENSEN

De BORG-regelingen zijn een norm voor inbraakbeveiliging voor gebouwen. Een gebouw moet voldoende weerstand bieden om bedrijfsprocessen die zich daarbinnen afspelen te beschermen, inclusief de eventueel aanwezige IT-apparatuur met bijbehorende informatie. De praktijk is echter dat IT-risico's niet altijd even goed worden ingeschat en dat de bescherming achteraf onvoldoende blijkt te zijn geweest.

Normen en regelingen

Voor alle partijen in de beveiligingsbranche neemt het Nationaal Centrum voor Preventie (NCP) een centrale plaats in als het gaat om normering en regelgeving voor fysieke beveiliging. Het heeft diverse producten en certificatieregelingen ontwikkeld en in de markt gezet, waaronder de BORG-regelingen voor woningen, winkels, showrooms, onderwijsinstellingen, (fysieke) beveiligingsbedrijven en particuliere alarm centrales. Daarbij is de bekende risicoklassenindeling ontworpen als norm voor inbraakveiligheid van fysieke omgevingen.

BORG-regeling en IT

Niet iedereen is even gelukkig met de risicoklassenindeling. De attractiviteitstypering komt uit de verzekeringswereld en houdt geen rekening met commerciële risico's als gevolg van diefstal van dossiers of digitaal opgeslagen informatie. De aard van het object kent slechts een driedeling; onder de hoogste klasse vallen productiebedrijven, werkplaatsen, kantoren en instellingen. Als er sprake is van een fysieke IT-locatie zou het onderzoeksobject kunnen worden gesplitst wat leidt tot compartimentering. Dan is de risicoklassenindeling echter niet meer van toepassing op het totale object. De feitelijke oorzaak hiervan moet worden gezocht in de methodiek van assetwaarde. Daarbij wordt uitgaan van de waarde van de geïnstalleerde systemen. Het probleem is dat er geen methodiek is om de waarde van de processen, draaiende op de geïnstalleerde systemen, te berekenen. Het is daarom van belang ook aandacht te schenken aan de IT, in het bijzonder aan de waarde van de informatie.

De waarde van informatie

De waarde van informatie laat zich moeilijk in geld uitdrukken. Een uitgangspunt zou kunnen zijn:
Het waarborgen van de betrouwbaarheid en het minimaliseren van eventuele schade.

Op basis van deze uitgangspunten kunnen kwalitatieve waarderingen worden benoemd. Deze waarderingen kunnen worden uitgedrukt in de factoren:

Tabel 1.

Exclusiviteit, juistheid	**Beschikbaarheid**			
	Laag	*Middel*	*Hoog*	*Zeer hoog*
Laag	0	4	8	12
Normaal	4	4	8	12
Hoog	8	8	8	12

Herstelbaarheid	Misbaarheid; benodigde hersteltijd			
	Kort	*Redelijk*	*Lang*	
	direct	binnen 4 uur	binnen 1 dag	2 dagen of meer
Onmiddellijk vervangbaar	1	2	4	6
Vervangbaar	2	4	6	8
Uniek en wel reproduceerbaar	4	6	8	10
Uniek en niet reproduceerbaar	6	8	10	12

Tabel 2.

- *Betrouwbaarheid*; onder te verdelen in beschikbaarheid, exclusiviteit en integriteit.
- *Misbaarheid en herstelbaarheid*; in relatie tot schadeverwachting.
- *Belangrijkheid*; in relatie tot de attractiviteitswaarde.

Door aan de verschillende waarderingen risicopunten toe te kennen en de som van het puntentotaal in te delen in één van de vier risicoklassen, zou dit kunnen worden gebruikt in de BORG-praktijk.

Uitgaande van de het feit dat men het belang van de informatie kan indelen in een schaalverdeling tussen 1 en 12, resulteert dat bijvoorbeeld in tabel 2.

De risicoklassenindeling

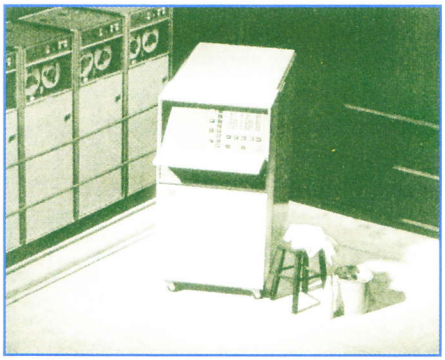
Het totale aantal risicopunten van de drie invalshoeken bepaalt de indeling in één van de vier risicoklassen (zie tabel 4). Deze risicoklassenindeling kan worden bepaald naast de gangbare indeling. De hoogste risicoklasse is bepalend voor de te selecteren beveiligingsmaatregelen.

Wanneer de indeling als gevolg van de waardebepaling van informatie hoger scoort dat de gangbare indeling kunnen ook extra maatregelen voor een IT-compartiment worden overwogen.

BORG voor integrale veiligheid?

In informatiebeveiligingsland bestaat nogal wat weerstand tegen de hier geschetste werkwijze, velen vinden dat de realiteit te complex is om in eenvoudige tabellen weer te geven. Maar de praktijk leert ook dat er vaak geen geld, geen tijd en vooral onvoldoende betrokkenheid is voor een gedegen risicoafweging en zolang er bij fysieke beveiliging nog nauwelijks rekening wordt gehouden met IT, is een pragmatische gulden middenweg aan te bevelen. Het mag niet zo zijn dat een bedrijf als gevolg van een calamiteit failliet gaat omdat bij het bepalen van beveiligingsmaatregelen IT-risico's niet zijn meegenomen.
De invloed van IT op BORG-regelingen verdient dan ook zeker aandacht.

...lees verder op pagina 13



... vervolg van pagina 7

Een werkgroep gaat onderzoeken hoe bij BORG-regelingen rekening kan worden gehouden met informatiebeveiliging om wellicht te komen tot een afzonderlijke BORG-regeling voor IT-bedrijven.

Praktische tips

Ter afsluiting enkele opmerkingen en praktische tips. In alle gevallen is de boodschap dat informatiebeveiliging en fysieke beveiliging niet op zichzelf staan maar overlappende disciplines zijn die steeds meer met elkaar te maken zullen krijgen.

- Let op, toegangsverlenings- en camerasystemen zijn soms aan het IT-netwerk gekoppeld. Bij uitval van het IT-netwerk zullen ook deze systemen niet meer werken.
- Voor iemand die informatie wil stelen kan het wel eens gemakkelijker zijn om een fysieke inbraak te plegen (toegankelijke informatiedragers zoals een cd-rom of een diskette) dan een computerinbraak.
- Laat de BedrijfsHulpVerleningsorganisatie (BHV) onderdeel uitmaken van het disaster recovery plan.

Bij een evacuatie als gevolg van een niet- IT-calamiteit worden wel de IT-aspecten meegenomen.

Belang van informatie	punten
Commerciële informatie	10
Informatie met de classificatie geheim	12
Informatie met de classificatie vertrouwelijk	8
Klant/orderinformatie	8
Koersgevoelige informatie	10
Personeelsinformatie	8
Privacygevoelige informatie	8
Medische informatie	12

Tabel 3.

- Informatiebeveiligingsmaatregelen en compartimentsindeling moeten op elkaar worden afgestemd.
- Beveiligingsactiviteiten die herkenbaar moeten zijn voor de medewerkers op de werkvloer kunnen gezamenlijk worden uitgevoerd. Denk daarbij aan bewustwordingsactiviteiten en veiligheidsprotocollen. Maak voor werk plekken uniforme, op elkaar afgestemde instructies als het gaat om afsluitdiscipline voor ruimten, clear desk policy voor IT-apparatuur en veiligheid in het kader van de Arbo-wet.
- Overweeg een centraal meldpunt voor alle veiligheidsincidenten; het moet voor betrokkenen uitnodigend zijn om incidenten te melden, één aanspreekpunt op een voor iedereen toegankelijke locatie, liefst naast de personeelsingang en beslist niet in een extra beveiligd gebied.

Douwe de Jong is zelfstandig IT-adviseur. Ronald Eygendaal CISMP, CSS is security consultant bij Vizzavi.

Tabel 4.

Risicopunten	Risicoklasse	Beveiligingsmaatregelen	
7 - 14	1	**Bs**	**+0**
15 - 24	2	**Bn** of **Bs** + **Es**	**+0**
25 - 29	3	**Bn** + **En**	**+0**
30 en meer	4	Maatwerk of **Bz** + **En** of **Bn** + **Ez**	**+0**