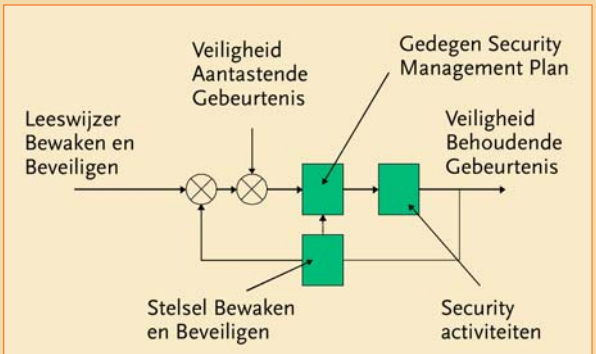
Procesbeheersing Corporate Security Nederland

Beveiliging (security) vindt veelal niet op een systematische of gestructureerde wijze plaats, terwijl security als proces vanuit de cybernetica eenvoudig kan worden weergeven. De in zo'n proces van belang zijnde en te regelen grootheden zijn:

- het gewenste resultaat: de Veiligheid Behoudende Gebeurtenis;
- de verstorende factor: de Veiligheid Aantastende Gebeurtenis;
- een referentiekader, in casu de Leeswijzer Bewaken en Beveiligen (LWBB);
- de security activiteiten van de onderneming/instelling op basis van een gedegen security management plan (opgesteld door een erkend security expert);
- een terugkoppeling in casu het stelsel Bewaken en Beveiligen.

Daarmee is het blokschema Corporate Security Nederland een feit.



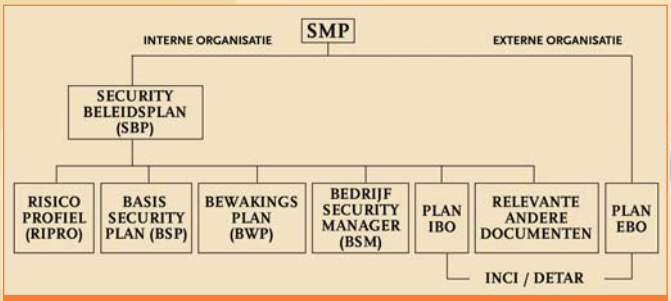
Blokschema Corporate Security Nederland

Corporate Security Nederland omvat in hoofdlijnen:

1. Een onderneming/instelling beschikt over een gedegen security management plan, opgesteld door een erkend security expert;
2. Het Beveiligingsvoorschrift tegengaan onbevoegde beïnvloeding (BEVOB)®; grondslag voor het op te zetten security management;
3. Kwaliteitsborging: evaluatie van de uitvoering van het beleid;
4. Omstandigheden creëren die samenwerking dicteren (LWBB);
5. Kwalificatiestructuur Security Branche Opleidingen (KSBO);
6. Onderwijs geven: voor de praktijk door de praktijk;
7. Goed voorbeeld doet goed volgen (project Vitale Infrastructuur).

1 Gedegen Security Management

Gedegen security management wil volgens mij zeggen: security van beleid tot en met uitvoering inclusief kwaliteitsborging. Alle essentiële onderdelen moeten worden gedocumenteerd in een security management plan (SMP). Onderstaand een compleet overzicht van het security management plan zoals dat inmiddels door vele bedrijven en instellingen wordt gehanteerd.



Security Management Plan

Het topdocument bevat het beleid inzake het tegengaan van onbevoegde beïnvloeding en wordt het Security Beleidsplan (SBP) genoemd. Om het SBP een integraal onderdeel uit te laten maken van het beleid van de onderneming c.q. overheidsinstelling moet het uiteraard geautoriseerd zijn door het (top)management.
Het Security Beleidsplan omvat:

- Het Risico Profiel (RIPRO) specificeert de incidenten waartegen security maatregelen moeten worden getroffen.
- Het Basis Security Plan (BSP) bevat een inventarisatie van de getroffen beveiligingsmaatregelen per risicoplaats en hun status. Deze maatregelen zijn onderverdeeld in Organisatorische, Bouwkundige en Elektronische (OBE) beveiligingsmaatregelen.
- Het Bewakingsplan (BWP) bevat relevante informatie met betrekking tot personeel en materieel dat is ingezet voor bewakingsdoeleinden.
- Het document inzake de Bedrijf Security Manager (BSM) geeft een overzicht van de taken, eisen van vakbekwaamheid (erkend security expert) en bevoegdheden van de security manager.
- Het plan Interne Beveiligings Organisatie (IBO) bevat een overzicht van de te ondernemen interne actie ingeval van een dreiging of een daadwerkelijk incident.
- Het plan Externe Beveiligings Organisatie (EBO) geeft een overzicht van de acties van politie en/of andere response forces in geval een incident of dreiging

daarvan.
- De naadloze aansluiting van het plan IBO op het plan EBO laat zich eenvoudig vaststellen met behulp van de, bij erkende security experts bekende, tijdpadanalyse INCI/DETAR®.

2 BEVOB

Met het door de erkende security expert opgestelde en door het management ondertekende Beveiligings-voorschrift tegengaan Onbevoegde Beïnvloeding (BEVOB) legt het bedrijf c.q. de instelling, met de Leeswijzer Bewaken en Beveiligen als uitgangspunt, zich de verplichting op om maatregelen te treffen tegen onbevoegde beïnvloeding risico's. BEVOB en SBP vormen dus het fundament voor het Corporate Security Management.

3 Kwaliteitsborging: evaluatie van de uitvoering van het beleid

De uitvoering van een security kwaliteitsprogramma kan zeer kostbaar zijn. Elke erkende security expert bezit de gebruikerslicentie om een aanzienlijk goedkoper security kwaliteitsprogramma uit te voeren, te weten de Interne Security Audit (ISA).
De ISA maakt gebruik van de elementen uit het Security Management Plan.
Door het uitvoeren van een Interne Security Audit (ISA) wordt aantoonbaar gemaakt dat:
- corporate security management plaatsvindt op basis van een helder security beleid;
- de relevante documenten voor het corporate security management conform SBP en BEVOB aanwezig zijn;
- vastgesteld is welk beheersbaarheidniveau bereikt moet worden;
- de beheersbaarheid van elk potentieel incident per risicoplaats deugdelijk is geanalyseerd, zodat de conclusie getrokken kan worden dat de beveiliging voldoende of onvoldoende is en verbeteringen nodig zijn.

4 Omstandigheden creëren die samenwerking dicteren: LWBB

De door de Nationaal Coordinator Terrorismebestrijding op 24 januari 2005 gestuurde brief aan de Tweede Kamer bevat de volgende zinsnede: "bewaken en beveiligen in Nederland bevat een woud aan regels". De stichting Security Expert Register Nederland (SERN) werd hierdoor geënthousiasmeerd en heeft de *Leeswijzer Bewaken en Beveiligen: Corporate Security Nederland* tot stand gebracht. Het betreft een (nog niet eerder) gestructureerd overzicht van overheidsdocumenten terzake. Voor de volledige Leeswijzer zie http://www.sern.nl

5 Kwalificatiestructuur Security Branche Opleidingen (KSBO)

De eisen van het ministerie van OCenW inzake de Erkenning van elders Verworven Competenties (EVC) zijn geprojecteerd op de actoren in de security branche. Dit heeft geleid tot de door SERN opgestelde KSBO. Hieruit is ondermeer een overbruggingscursus tot stand gekomen die tot doorstroming leidt naar cursussen op hbo-niveau en de mogelijkheid om de status van erkend security expert te verkrijgen.

6 Onderwijs geven: voor de praktijk door de praktijk

Inmiddels deelt een aantal erkende security experts hun kennis met anderen door middel van het geven van onderwijs in de vorm van cursussen op post hbo-niveau. Dergelijke cursussen zijn in de afgelopen jaren door vele honderden geïnteresseerden gevolgd en hebben bijgedragen tot een verdere professionalisering van Corporate Security Nederland.

7 Goed voorbeeld doet goed volgen (project Vitale Infrastructuur)

Vanuit het project Vitale Infrastructuur heeft de VROM-Inspectie het initiatief genomen om de van EZ overgedragen nucleaire security expertise breder in te zetten. De daarbij gehanteerde bekende methodiek wordt door erkende security experts ook toegepast bij rijksgebouwen (rechtbanken, justitiële inrichtingen, ministeries), drinkwaterbedrijven, militaire objecten en chemische bedrijven.

Nederland is klein, denk groot. Ga voor eenheidstaal, stel een norm

Rest voor de zeer nabije toekomst nog de volgende wens. Als een onderneming of instelling, welke deel uitmaakt van de vitale infrastructuur, beschikt over een Security Management Plan, en aantoonbaar maakt middels een recent Intern Security Audit rapport dat het, voor wat bewaking en beveiliging datgene gedaan heeft wat redelijkerwijs noodzakelijk kan worden geacht,
dan ware door:
het Inspectoraat-Generaal van het ministerie waaronder de onderneming of instelling ressorteert een Conformiteitsverklaring Beveiligde Onderneming/ Overheidsinstelling (CVBO?) af te geven;
en
dan zou die onderneming c.q. instelling recht moeten hebben op een door de lokale driehoek vastgesteld plan EBO dat naadloos aansluit op het plan IBO van de betreffende onderneming c.q. instelling. Wanneer die situatie bereikt wordt dan is, naar mijn mening, voor wat betreft de vitale infrastructuur sprake van een professioneel opgezette bewaking en beveiliging.

Bert Duijndam,
Register Security Expert

Dit artikel is op persoonlijke titel geschreven