Handreiking Operator Security Plan (OSP)

Een handreiking voor het plannen, implementeren en beheren van operationele beveiligingsmaatregelen

NAVI

Nationaal Adviescentrum **Vitale Infrastructuur**

Augustus 2008
2e druk

Handreiking Operator Security Plan (OSP)

Een handreiking voor het plannen, implementeren en beheren van operationele beveiligingsmaatregelen

Wat is het NAVI

In het Nationaal Adviescentrum Vitale Infrastructuur (NAVI) werken overheid en bedrijfsleven samen aan de verbetering van de fysieke en digitale beveiliging van de vitale infrastructuur in Nederland. Beheerders en eigenaren van de vitale infrastructuur in Nederland kunnen bij het NAVI terecht voor informatie en onafhankelijk advies op het gebied van de beveiliging tegen moedwillige verstoring (security). De vier kerntaken van het NAVI zijn:

Advisering over beveiliging

Het NAVI geeft eigenaren of beheerders van vitale infrastructuur in Nederland advies over beveiliging. Bijvoorbeeld bij het uitvoeren van risicoanalyses of van een second opinion op een bestaand beveiligingsplan. Ook adviseert het NAVI over al genomen of nog te nemen beveiligingsmaatregelen op basis van een risicoanalyse. Hierbij werkt het NAVI vraaggericht.

Delen van kennis en informatie over beveiliging

Het NAVI zorgt ervoor dat betrokken partijen kennis en informatie binnen de vitale sectoren in Nederland kunnen delen. Het NAVI onderhoudt daartoe contacten met overheden en met het bedrijfsleven uit de vitale sectoren en daarnaast met relevante contacten en instellingen in het buitenland. Kennis en informatie worden op verschillende manieren beschikbaar gesteld, ondermeer door het organiseren van bijeenkomsten, via de website en de beschikbaarheid van een kennisbank.

Productontwikkeling

Het NAVI ontwikkelt ook eigen producten. De focus ligt hierbij op producten die voor een hele sector of zelfs meerdere sectoren toepasbaar zijn. Voorbeelden hiervan zijn de verschillende handreikingen die momenteel worden ontwikkeld over beveiligingsonderwerpen. Indien nodig worden de producten op verschillende niveaus van volwassenheid ontwikkeld. Ook spant het NAVI zich in om producten van derden voor de Nederlandse vitale infrastructuur toegankelijk te maken.

Netwerkfunctie

Het NAVI onderhoudt en ontwikkelt een breed netwerk binnen de beveiligingswereld en fungeert als ontmoetingsplek voor de betrokken partijen binnen de vitale infrastructuur. Zowel overheidspartijen, kennisinstellingen in binnen- en buitenland, als bedrijven. Het NAVI brengt partijen bij elkaar, bijvoorbeeld via het organiseren en ondersteunen van kennis- en informatieknooppunten. Hierin komen partijen uit een sector of uit verschillende sectoren op reguliere basis bij elkaar om informatie te delen en over beveiligingsonderwerpen te spreken.

Kijk voor meer informatie op de website: www.navi-online.nl

Inhoudsopgave

1. Inleiding

1.1. Wat is een Operator Security Plan (OSP)

Een Operator Security Plan (OSP) beschrijft de beveiligingsmaatregelen die een organisatie heeft getroffen. De benaming 'Operator' verwijst naar de beheerder van de infrastructuur. Samen met het Security Management Systeem (SMS) en een risicoanalyse sluit het OSP aan op de Europese richtlijn van de European Programme for Critical Infrastructure Protection (EPCIP). De Handreiking Operator Security Plan is geschreven voor bedrijven met vitale infrastructuur. De handreiking is echter ook te gebruiken om beveiligingsmaatregelen te selecteren voor objecten van belang die niet aangewezen zijn als 'vitale infrastructuur'.

Beveiliging moet een integraal onderdeel zijn van het gebruikelijke bedrijfsproces.
Naast risicoanalyses en historische incidenten zijn er ook andere aanleidingen om beveiligingsmaatregelen te treffen. Bijvoorbeeld:

- Wet- en regelgeving;
- Safety, bijvoorbeeld via toegangsregulering voorkomen dat niet gewenste personen een bepaalde locatie betreden;
- Maatschappelijke of management opinie om een bepaalde maatregel te treffen;
- Aantoonbaarheid van beveiliging en wensen ten aanzien van het afleggen van verantwoording;
- Kosteneffectiviteit van maatregelen ten opzichte van andere maatregelen met een vergelijkbaar beveiligingseffect;
- Beheerkosten van maatregelen en keuzen op standaardisatie en architectuur van maatregelen.

Beveiligingsmaatregelen zijn veelomvattend en vaak kostbaar in aanschaf, beheer en uitvoering. Daarom is het van belang duidelijk te maken wat precies het doel is en wat men verwacht van het verminderen van de risico's. Maatregelen werken immers alleen als ze effectief zijn ingevoerd en als zodanig worden gehandhaafd. Als onderdeel van een SMS zorgt het OSP voor een goed beheer van de maatregelenset.

Om effectieve, aantoonbare en in een architectuur geplaatste beveiligingsmaatregelen te beheren, bestaat het OSP uit een beschrijving van of verwijzing naar de volgende hoofdcomponenten:

- De relatie met de omgeving van het OSP (wetgeving, bedrijfsbeleid en –doelstellingen);
- Het beveiligings- en beveiligingsmaatregelenbeleid;
- De belangen en afhankelijkheden van de organisatie;
- De dreigingen, opponenten en incidentscenario's;
- De beveiligingsdoelen en –concepten van de organisatie;
- De risicoafwegingen op operationeel niveau;
- Het invoeren van de maatregelen;
- Het operationeel beheren van de maatregelen;
- De doelstellingen en effectiviteit van de getroffen maatregelen.

In deze handreiking voor het OSP wordt, met behulp van een stappenplan, aangegeven op welke wijze deze hoofdcomponenten kunnen worden ingevuld.

1.2. Waarom deze handreiking

De handreiking Operator Security Plan is een hulpmiddel voor beheerders van de vitale infrastructuur om operationele beveiligingsmaatregelen te selecteren, in te voeren, te beheren en te verbeteren met als doel deze effectief in te zetten op dreigingen tegen de bedrijfsbelangen.

Het aantal beveiligingsmaatregelen en de mogelijke combinaties van maatregelen zijn aanzienlijk. Deze handreiking biedt handvatten om het beveiligingsdoel van een maatregelenset inzichtelijk te maken. Dit kan een controlemiddel zijn om na te gaan of er in de verschillende fasen van het beveiligingsproces de juiste maatregelen zijn getroffen. Het nemen van beveiligingsmaatregelen en het verbeteren van de maatregelenmix is een cyclisch proces.

Deze handreiking geeft een stappenplan om een eerste beeld van de benodigde maatregelen te vormen. Dit 'maatregelenbeleid' moet passen binnen de uitkomsten van de risicoanalyse en met de opvattingen van de bedrijfsleiding op de beveiliging. Vanuit en binnen deze visie kunnen daarna in implementatieprojecten de beveiligingsmaatregelen worden ingevoerd.

Deze handreiking gaat niet in op het selecteren van maatregelen in een specifieke situatie. Het feitelijke handwerk ligt bij de beheerders zelf, waarbij beveiligingskennis beslist nodig is. Als deze in het bedrijf nog onvoldoende aanwezig is, moet dit ontwikkeld en eventueel extern betrokken worden. De handreiking wil bewustwording creëren voor de elementen die van belang zijn in het security plan en kapstokken aanreiken voor de ontwikkeling van dit plan.

1.3. Voor wie is deze handreiking

Deze handreiking is in eerste instantie bestemd voor security managers van bedrijven die tot de vitale sector behoren. Zij kunnen met deze handreiking een Operator Security Plan opstellen, eventueel met hulp van experts op specifieke vakgebieden.

Secundaire doelgroepen zijn:

- Staf- en directieleden van vitale bedrijven die een beeld willen vormen van het beveiligingsproces;
- Beveiligingsadviseurs betrokken bij vitale bedrijven;
- Security managers van bedrijven die niet tot de vitale sector behoren.

1.4. Productpositionering

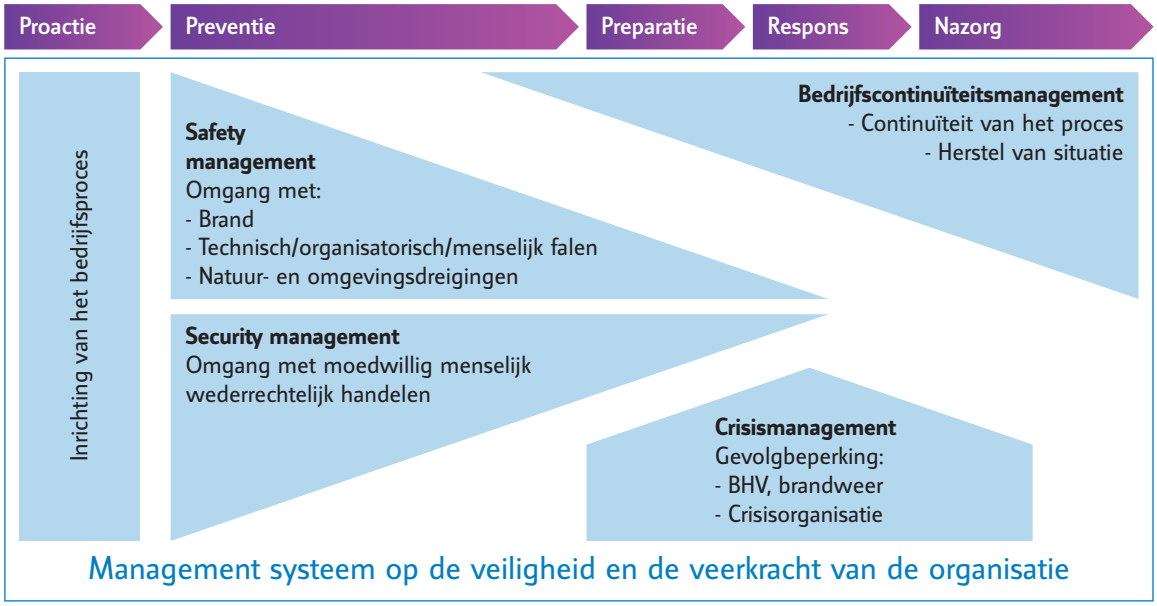
1.4.1. OSP in relatie tot de veiligheidsketen

Bij security gaat het om het (preventief) weerstand bieden aan opzettelijke verstoring. Dit opzettelijke of moedwillige karakter is bepalend voor het onderscheid tussen security en safety. Bij safety gaat het om het (zoveel mogelijk) voorkomen van ongewenste gebeurtenissen als gevolg van natuurlijke anomalieën of rampen, of technisch, organisatorisch of menselijk falen.

Binnen het veiligheidsbeleid en operationeel continuïteitsmanagement van de organisatie richt het OSP zich op het voorkomen en bemoeilijken van dreigingen van moedwillig menselijk handelen. In de veiligheidsketen is het OSP voornamelijk gericht op de preventieve werking.

Op maatregelenniveau is er veel samenhang met de getroffen safety maatregelen. Zowel security als safety hebben een preventieve werking. Zo zijn verschillende toegangbeperkende maatregelen hoofdzakelijk ontworpen om onbedoeld menselijk handelen te voorkomen, bijvoorbeeld het weghouden van ongekwalificeerd personeel uit hoogspanningsruimten. Een ander voorbeeld is een compartimenteringsplan dat bedoeld is om een brand lokaal te houden. Er kunnen ook ogenschijnlijk tegenstrijdige doelstellingen bestaan tussen de verschillende plannen. Vanuit security is het vaak de bedoeling om onbevoegde personen het vluchten te bemoeilijken, terwijl vanuit de Bedrijfshulpverlening (BHV) open vluchtwegen van groot belang zijn. In de uitwerking van de maatregelen moet met beide doelstellingen rekening worden gehouden.

Het security proces bevat ook de interventieactiviteiten om onbevoegde handelingen te stoppen en onbevoegden te corrigeren. De meeste van deze activiteiten kunnen tot de preventieve kolom van de veiligheidsketen gerekend worden, omdat daarmee wordt voorkomen dat de dader het ongewenste effect bereikt. Een snelle en gerichte interventie is één van de kritische succesfactoren van beveiliging. Als een bedrijf dit weet te organiseren, kan de interventie ook gebruikt worden om snel te reageren op detectie van andere typen van onveiligheid en ingezet worden om schade te beperken. Denk bijvoorbeeld aan de rol van beveiligers in de eerste fase van de brandbestrijding en aan het BHV-proces (response activiteiten uit veiligheidsketen).

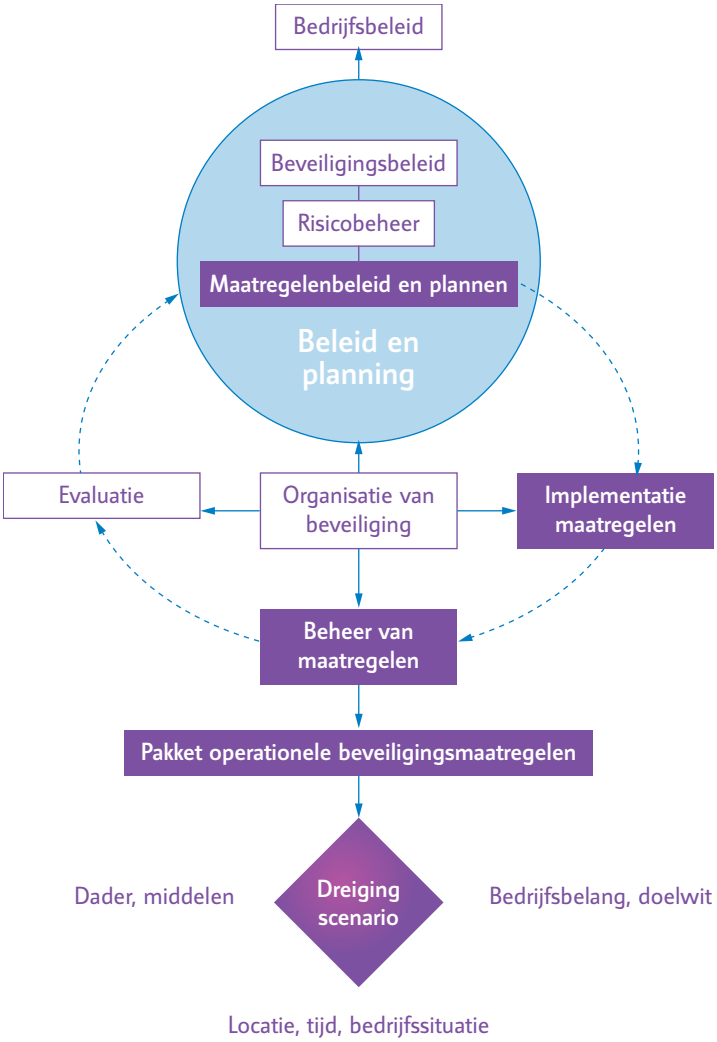


1.4.2. OSP als onderdeel van Security Management Systeem

Beveiligen is een combinatie van verschillende beveiligingsdoelen met daarbij passende beveiligingsmaatregelen. Het geheel aan activiteiten op het gebied van beveiliging binnen een organisatie moet structureel en ordelijk worden georganiseerd in een Security Management Systeem (SMS). Een SMS bestaat uit verschillende fasen, die een cyclisch en iteratief proces vormen. Deze aanpak waarborgt de kwaliteit van het beveiligingsproces.

Deze paragraaf geeft aan op welke wijze het OSP past binnen het Security Management Systeem. De volgende onderdelen van het SMS worden beschreven in het OSP:

- Het maatregelenbeleid en de beveiligingsplannen;
- De implementatie van beveiligingsmaatregelen;
- Het operationele beheer van de maatregelen;
- Het pakket operationele beveiligingsmaatregelen.



De doelstellingen en het plan van aanpak worden in de beleids- en planningsfase vastgesteld. In deze fase worden in onderlinge afhankelijkheid en consistentie de volgende activiteiten uitgevoerd, resulterend in eindproducten per fase:

1. Bedrijfsbeleid
   Beveiligingsplannen dienen consistent te zijn met het bedrijfsbeleid. In dat beleid ligt onder meer vast hoe het bedrijf om wil gaan met klanteisen, branche-eisen en andere regelgeving, maar ook wat afbakeningen zijn van security met bedrijfscontinuïteitsmanagement, Informatie en Communicatietechnologie (ICT), Human Resources Management (HRM), huisvesting en dergelijke.
2. Beveiligingsbeleid
   Het beveiligingsbeleid geeft de noodzaak aan voor beveiliging, de afbakening en de te bereiken beveiligingsdoelstellingen. Als geheel is het beveiligingsbeleid richting- en maatgevend om die doelstellingen te bereiken.
3. Risicobeheer
   Het risicobeheer bestaat uit een risicoanalyse en activiteiten om het risicobeeld actueel te houden. Uit de risicoanalyse wordt duidelijk waar beveiligingsmaatregelen nodig zijn en wat de beveiligingsdoelstellingen zullen zijn.
4. Maatregelenbeleid en plannen (OSP)
   Het maatregelenbeleid vormt de brug tussen beveiligingsdoelen en de concrete beveiligingsmaatregelen. Het heeft als doel om op maatregelenvlak lijn aan te brengen in uitvoering en beheer. De beveiligingsplannen geven aan wat de gewenste maatregelen zijn en hoe deze worden ingevoerd.
5. Implementatie van maatregelen (OSP)
   Dit zijn de activiteiten om maatregelen concreet te implementeren en in beheer te nemen.

6. Operationeel beheren van maatregelen (OSP)
   Activiteiten om maatregelen operationeel te beheren.
7. Pakket operationele beveiligingsmaatregelen (OSP)
   De aanwezigheid van een pakket operationele beveiligingsmaatregelen en de werking hiervan op de beveiliging van bedrijfsbelangen tegen dreigingen.
8. Organisatie van beveiliging
   De manier waarop verantwoordelijkheden, taken, bevoegdheden, verantwoordings- en coördinatiestructuren zijn belegd, alsmede de communicatie, prestatie-indicatoren en budgetten om de beveiliging uit te voeren en continu te verbeteren.
9. Evaluatie
   De evaluatie van maatregelen, organisatie en risicobeheersing.

1.4.3 OSP in relatie tot andere security aanpakken en -verplichtingen

Het OSP heeft overlap met en is een verdieping van verschillende security aanpakken en –verplichtingen waar bedrijven mee te maken kunnen hebben, ondermeer:

- DHM Security Management
- EPCIP (European Programme for Critical Infrastructure Protection)
- PFSP / ISPS (Port Facility Security Plan / International Ship Port Security)
- ISO/PAS 22399 (Incident Preparedness & Operational Continuity Management)
- ISO/PAS 28000 (Security Management System for the supply chain)
- ISO/IEC 27002 (Code of practice for information security management (NEN-ISO/IEC 17799:2002))
- Tabaksblat
- Sarbanes-Oxley
- Basel II

Heeft u vragen over hoe het OSP zich precies verhoudt tot bovenstaande aanpakken, dan kunt u contact opnemen met het NAVI.

1.5. Afbakening

Het aantal beveiligingssituaties, beveiligingsconcepten en beveiligingsmaatregelen is zo omvangrijk dat deze in een handreiking nooit volledig en uitputtend kunnen worden beschreven. In concrete situaties zal gespecialiseerde beveiligingskennis nodig zijn om de meest adequate maatregelen te selecteren.

1.6. Verdere ontwikkeling van de handreiking

De voorliggende handreiking is een eerste versie. Gebruikers uit de praktijk worden van harte uitgenodigd hun ervaringen met de handreiking met het NAVI te delen opdat het product verder met en voor u ontwikkeld kan worden. Op basis daarvan kunnen eventueel gespecialiseerde, toepassingsgerichte handreikingen gerealiseerd worden die directer aansluiten op bepaalde beveiligingssituaties.

Het OSP is een integraal onderdeel van het SMS. De interactie, overlappen en afbakening met het SMS verdient nog enige aandacht. In een volgende versie van het SMS en OSP zal daaraan extra aandacht worden besteed.

1.7. Ondersteuning van het NAVI bij opstellen van een OSP

De Handreiking OSP geeft de gebruiker handvatten om zelfstandig een OSP te kunnen opstellen en implementeren. Heeft u echter na het lezen van handreiking vragen of hulp nodig bij het maken van (onderdelen) van uw OSP, dan kunt u contact opnemen met het NAVI via info@navi-online.nl of (070) 376 59 50.

2. Criteria waaraan een goed OSP moet voldoen

Dit hoofdstuk geeft criteria die bruikbaar zijn om tot een goed resultaat te komen. Deze criteria zijn ook bruikbaar om de kwaliteit van een OSP te kunnen beoordelen. De keuze van beveiligingsmaatregelen is situatiespecifiek, maar er kunnen wel criteria benoemd worden die van belang zijn in (bijna) alle beveiligingssituaties:

2.1. Proces

Werk systematisch volgens het stappenplan

Maak eerst duidelijk wat de beveiligingsdoelstellingen zijn, voordat de beveiligingsmaatregelen bedacht worden. De selectie van passende maatregelen – en ook de managementaandacht hierbij – is dan heel gericht op die doelen. Het resultaat is dat er geen maatregelen ingevoerd en operationeel gehouden worden die niet bijdragen aan de beveiligingsdoelstellingen.

Centrale vragen moeten steeds zijn:

- Wat en waarom is beveiliging nodig?
- Waartegen is beveiliging nodig?

Door vanuit een beveiligingsvisie of maatregelenbeleid te werken, kan het bedrijf sneller en consistenter beveiligingsmaatregelen invoeren en aanpassen.

Creëer draagvlak

Dit lijkt een open deur, maar is wel een essentieel criterium. Het stappenplan en de inbedding hiervan in een Security Management Systeem geeft verschillende momenten en structuren om met de bedrijfsleiding te communiceren over de noodzaak en richting van de security. Breng aan het begin van het traject ook de overige betrokkenen die van belang zijn voor een goede security in kaart. Een goede afstemming met bijvoorbeeld de bedrijfsvoering is essentieel om de beveiligingsmaatregelen goed in te bedden in de fysieke en digitale inrichting van het bedrijfsproces.

Mobiliseer en creëer deskundigheid

Beveiliging is een breed vakgebied. Ga na welke expertise waar in de eigen organisatie aanwezig is. Benoem een beveiligingscoördinator of security manager en zorg dat die adequaat opgeleid is/wordt. Zorg daarna dat ook andere sleutelfiguren in de organisatie een security opleiding krijgen. Gebruik ook deskundigheid die aanwezig is bij collegabedrijven en brancheverenging om te toetsen hoe deze met bepaalde beveiligingssituaties omgaan. Betrek externe beveiligingsadviseurs om de risicoanalyse en de maatregelenselectie te toetsen.

2.2. Keuze van beveiligingsmaatregelen

Classificeer de te beschermen belangen en leg risicoplaatsen vast

Vanuit het OSP moet helder zijn wat de te beschermen belangen zijn en waar die zich kunnen bevinden. Door de mate van vitaliteit voor het bedrijf vast te leggen, wordt het mogelijk een daarbij passend beveiligingsregime te definiëren.

Breng potentiële dreigingen in beeld

In het OSP moet duidelijk zijn wat de mogelijke dreigingen zijn. Maatregelen kunnen alleen goed ingericht worden als helder is tegen welke dreigingen zij moeten functioneren. Gebruik bij het opstellen van een dreigingsanalyse informatie uit alle ter beschikking staande bronnen. Betrouwbare bronnen zijn: wetenschappelijke studies en onderzoeken door gerenommeerde organisaties, publicaties van politie-, inlichtingen- en veiligheidsdiensten (uit binnen- en buitenland) en informatie die door de overheid (onder andere Nationaal Coördinator Terrorismebestrijding (NCTb)), het eigen vakdepartement of een brancheorganisatie ter beschikking wordt gesteld.

Motiveer de keuze van de maatregelen
In het OSP moet worden beschreven wat het beveiligingsdoel is van de maatregelen en wat het verwachte effect is.
Definieer de beveiligingsonderwerpen
Het aantal situaties waarin moedwillig wederrechtelijk gehandeld kan worden tegen het bedrijf is nooit klein.
Het aantal en type van beveiligingsonderwerpen is vanzelfsprekend bedrijfsspecifiek.

Zorg dat de beveiliging niet afhankelijk is van één type beveiligingsmaatregel
Ieder type maatregel heeft slechts een beperkte werking. In het beveiligingsconcept mag geen afhankelijkheid van slechts één type beveiligingsmaatregel zijn. Als een dader één type maatregel weet te ontwijken of te doorbreken, moeten andersoortige maatregelen in werking treden.
In de handreiking en in de Bijlagen worden verschillende kapstokken aangereikt om tot een gevarieerde mix van maatregelen te komen.

Zorg dat de onderwerpen diepgaand zijn beschreven
De diepgang en mate van detaillering van de beschreven onderwerpen moet zodanig zijn dat het op operationeel niveau duidelijk is, wat en hoe de werking van de maatregel is.

Leg de afschermingsmaatregelen en het compartimenteringsconcept vast [1]
Het OSP moet aangeven op welke manieren de belangen worden afgeschermd en wat het toegepaste concept van compartimentering is. Er moeten maatregelen in opgenomen zijn om potentiële daders al in een vroeg stadium te ontmoedigen.

Zorg dat het toegangverleningsconcept zowel effectief is in bedrijfsvoering als in risicobeheersing
De uitvoering van de toegangverlening moet passen bij de bedrijfs- en gebruikslogistiek. Daarnaast moet deze effectief zijn om gewenste gebruikers toegang te verschaffen en ongewenste personen te weren.
Een belangrijk criterium is de beschikbaarheid van een actueel document waarin vastligt welke personen onder welke voorwaarden toegang mogen hebben. Dit geldt niet alleen voor de fysieke toegangsrechten, maar ook voor schakelrechten van inbraakdetectie en toegangsrechten tot ICT.
Het beheer moet ook gericht zijn op het misbruik dat plaatsvindt op de toegangverlening.

Kies detectiemaatregelen op alle benoemde dreigingen
Voor alle benoemde dreigingen moeten ook detectiemaatregelen ingericht zijn. Dit kunnen sociale, organisatorische en technische maatregelen zijn.

Richt een 24x7 uur bereikbaar meldpunt in en leg procedures op de interventie vast
Het bedrijf dient een centraal meldpunt te hebben met betrouwbare communicatiekanalen en –middelen. De procedures over het omgaan met aangegeven dreigingen moeten vastliggen en bekend zijn bij de betrokken personen.
In de procedures moet tot uitdrukking komen wat het verwachte optreden is. Actuele contactlijsten met personen en partijen die een rol spelen in het interventieproces moeten voorhanden zijn.

Sluit de interne beveiligingsprocedures aan op die van externe partijen en publieke veiligheidspartijen
In het OSP moet de aansluiting van de interne beveiligingsprocedures op die van externe partijen als bijvoorbeeld alarmcentrale en beveiligingsbedrijf vastliggen. Er moet zijn beschreven hoe partijen elkaar operationeel oproepen, welke informatie uitgewisseld wordt en wat de taken zijn.
Ook moet het OSP het coördinatiemechanisme bevatten dat er voor zorgt dat de procedures ook op elkaar aangesloten blijven. Dit geldt niet alleen voor private externe partijen maar ook voor de relatie met publieke veiligheidspartijen als politie en brandweer.

---

1 De afschermende, toegangverlenende, detecterende en interveniërende maatregelen gelden zowel in de fysieke beveiliging als in de informatiebeveiliging.

Zorg dat er naast de basisbeveiliging ook dynamische maatregelen bij verhoogde dreiging zijn
Het OSP dient naast een basis beveiligingsniveau ook maatregelen te hebben die kunnen worden ingezet bij verhoogde dreiging. Het dynamische gedeelte van de beveiliging moet overeen komen met de systematiek van het Alerteringssysteem Terrorismebestrijding (ATb) waar de meeste sectoren op zijn aangesloten.

Besteed aandacht aan het levend houden van beveiliging bij personen
In het OSP moeten maatregelen worden beschreven die zijn getroffen op het levend houden van de aandacht voor risicobeheersing bij personen die invloed hebben op de uitvoering van de beveiliging.

2.3. Beheer en organisatie

Besteed aandacht aan beheer, architectuur, standaardisatie en kosten
In de keuze voor maatregelen moet aandacht besteed worden aan de beheeraspecten en aan het kostenniveau van een maatregelenpakket. Als er alternatieven zijn met een vergelijkbaar beveiligingsdoel, maar met een eenvoudiger beheer of een lager kostenniveau, dan moeten die gekozen worden. In grotere en complexere situaties dient het OSP een architectuurvisie te hebben op de maatregelen, systemen en netwerken met keuzen op de te gebruiken standaards.

Richt de operationele organisatie van beveiliging goed in
In het OSP moet vastliggen wat de taken, verantwoordelijkheden en bevoegdheden zijn van de security manager en van de overige betrokkenen in de organisatie van beveiliging. Er moeten afspraken zijn over wie welke prestatie levert, de coördinatie, informatie-uitwisseling en sturing op prestaties. Dit kan bijvoorbeeld gebeuren via Service Level Agreements (SLA's).

Leg de relaties met interne uitvoerende partijen op beveiliging vast
De relaties met interne uitvoerende partijen op security moeten benoemd zijn evenals de wijze waarop deze bewaakt en gestuurd worden. Denk onder meer aan:
- Portier en receptiediensten
- Bedrijfsalarmcentrale, meldkamer
- HRM
- ICT
- Facilitair, 'technische dienst'

Leg de relaties met externe uitvoerende partijen op beveiliging vast
De relaties met externe uitvoerende partijen op security moeten aangegeven zijn evenals de wijze waarop deze bewaakt en gestuurd worden. Denk onder meer aan:
- Particuliere alarmcentrale
- Beveiligers in alarmopvolging
- Beveiligers in surveillance, brand- en sluitronde, toegangbeheer
- Beveiligingsinstallatiebureau
- Particulier recherche of onderzoeksbureau
- Salvage-diensten
- Gecertificeerde chauffeurs, leveranciers

Definieer de relaties met publieke partijen op beveiliging

De relaties met publieke partijen op security moeten aangegeven zijn evenals de wijze waarop deze bewaakt en gestuurd worden. Denk onder meer aan:

- Politie
- Brandweer
- Geneeskundige Hulpverlening bij Ongevallen en Rampen (GHOR)
- Burgemeester (rol in stelsel bewaken en beveiligen)
- Veiligheidsregio

Zie voor dit onderwerp ook de Handreiking Beveiligingsafstemming Vitaal met Overheid (BAVO) van het NAVI. Deze is te downloaden op de website www.navi-online.nl.

Beschrijf verantwoordingsprocessen op beveiliging

In het OSP moet aangeduid zijn welke operationele verantwoordingsprocessen zijn ingericht en wat voor soort rapportages plaatsvinden.

2.4. Structuur OSP-documentatie

Zorg dat OSP-documenten logisch zijn opgebouwd

De opbouw en samenstelling van de OSP-documenten moet aansluiten bij de beveiligingssituaties, organisatie van beveiliging en documentatiemethoden van het bedrijf.

Leg vast hoe OSP-documenten beheerd worden

Het moet duidelijk zijn wie welke onderdelen van het OSP in beheer heeft. Dit kan worden vastgelegd in de wijzigingsprocedure op de documentatie.

Zorg dat de OSP-documentatie, waar nodig, beveiligd is

De vertrouwelijke elementen van de OSP-documentatie moeten geïdentificeerd worden en de documentatiestructuur van het OSP moet met dat vertrouwelijke karakter rekening houden.
Als er bijzondere eisen bestaan op integriteit en beschikbaarheid van onderdelen van de OSP-documentatie, dan moet worden vastgelegd hoe daar rekening mee wordt gehouden.

Zorg ervoor dat de inhoud van het OSP communiceerbaar is

Voor verschillende aspecten van de beveiliging is het wenselijk dat deze eenvoudig te communiceren zijn. De structuur van het OSP moet hier rekening mee houden.

3. Stappenplan

Dit hoofdstuk behandelt het stappenplan dat nodig is om te komen tot een OSP.

De te nemen stappen uit het stappenplan (zie schema op pagina's 22 en 23) hebben de volgende samenhang:

Relatie met Security Management Systeem, beveiligingsbeleid, bedrijfsbeleid

Het OSP is onderdeel van het Security Management Systeem van het bedrijf en moet ook vanuit die kaders gestuurd worden. In veel organisatie zijn beveiligingsbeleid, doelstellingen en randvoorwaarden, die voor het OSP van belang zijn, nog niet expliciet ontwikkeld en vastgelegd. Het expliciet maken van het Security Management Systeem gebeurt dan gelijktijdig met de visievorming op de benodigde maatregelen in de ontwikkeling van OSP (Stap 1-8).

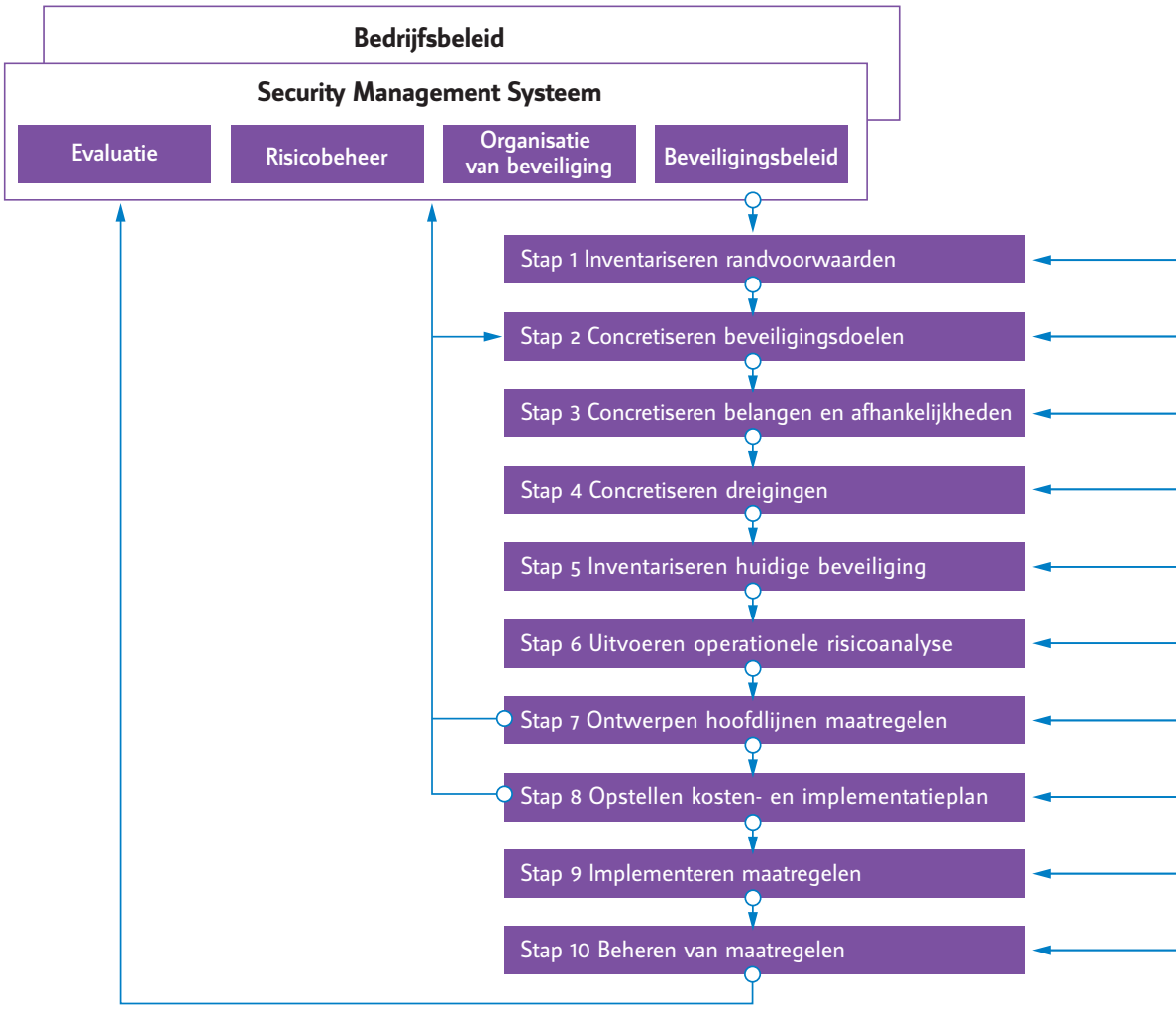
Relatie met risicoanalyse binnen het Security Management Systeem

Een all hazard risicoanalyse wordt uitgevoerd om op bedrijfsniveau vast te stellen wat de risico's zijn voor het bedrijf, voor zowel security als voor andere soorten dreigingen.
Vanuit dit inzicht kan op hoofdlijnen vastgesteld worden waar het OSP zich op moet richten en wat het ambitieniveau moet zijn. In Stap 2 van het OSP worden deze beveiligingsdoelstellingen, samen met mogelijke andere doelstellingen, door de security manager nog eens expliciet gemaakt en teruggekoppeld.
Vanuit de doelstellingen uit Stap 2 wordt op detailniveau een risicoduiding uitgevoerd. Dit gebeurt in de Stappen 3, 4, 5 en 6. Het resultaat is een lijst met alle kwetsbaarheden.

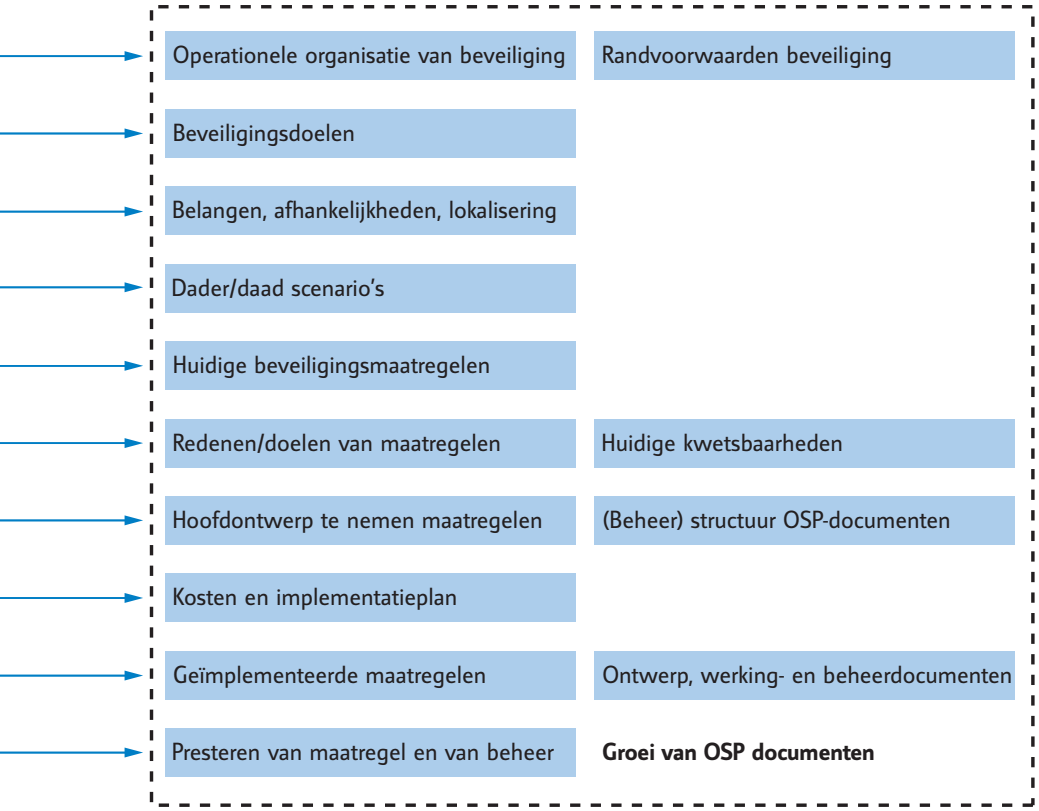
Eerst vormen van overall visie op beveiliging (Stap 1-8) voordat wordt overgegaan op implementeren van maatregelen (Stap 9)

De Stappen 1 tot 8 leiden tot expliciet inzicht in de effectiviteit van de huidige beveiligingsmaatregelen en visie op de gewenste maatregelenmix. De keuzen hierbij, samen met de gerelateerde kosten, moeten door de bedrijfsleiding bekrachtigd worden.
In deze keuze is er altijd een spanningsveld tussen 'tekenen' en 'rekenen'. Ook is het denkbaar dat binnen de gestelde beveiligingsdoelen (Stap 2) en randvoorwaarden (Stap 1) geen goede maatregelenmix te ontwerpen is. Wellicht kunnen de beveiligingsdoelstellingen uit Stap 2 zodanig bijgesteld worden dat deze nog steeds passen binnen het beveiligingsbeleid. Als dat niet mogelijk is, moet op directieniveau opnieuw afgewogen worden hoe met de resultaten van de overall risicoanalyse wordt omgegaan en wat dat betekent voor de doelstellingen op het gebied van security en de randvoorwaarden hierbij.[2]

2 Het resultaat van Stap 8 en 9 kan bijvoorbeeld zijn dat een bepaalde dreiging op een bedrijfsmiddel met beveiliging nauwelijks te verhinderen is of slechts tegen hoge fi nanciële en organisatorische kosten. Vanuit dat inzicht kan besloten worden om de maatregelen in andere fasen in de veiligheidsketen te treffen. Voorbeelden hiervan zijn:
- Het bedrijfsproces zodanig inrichten dat het effect van een dreiging sterk wordt verkleind (pro-actie).
- Maatregelen op het bestrijden van de directe- en gevolgschade (repressie).
- Maatregelen op bedrijfscontinuïteit (rehabilitatie).
Ook kan het voorkomen dat de voorgestelde maatregelenmix botst met de randvoorwaarden op beveiliging. In dat geval zal eerst op directieniveau dit confl ict moeten worden opgelost.


Bedrijfsbeleid
Security Management Systeem
Evaluatie
Risicobeheer
Organisatie van beveiliging
Beveiligingsbeleid
Stap 1 Inventariseren randvoorwaarden
Stap 2 Concretiseren beveiligingsdoelen
Stap 3 Concretiseren belangen en afhankelijkheden
Stap 4 Concretiseren dreigingen
Stap 5 Inventariseren huidige beveiliging
Stap 6 Uitvoeren operationele risicoanalyse
Stap 7 Ontwerpen hoofdlijnen maatregelen
Stap 8 Opstellen kosten- en implementatieplan
Stap 9 Implementeren maatregelen
Stap 10 Beheren van maatregelen

Achter in deze handreiking is dit schema nogmaals opgenomen, om tijdens het lezen van de stappen een duidelijk overzicht te geven. Sla hiervoor de achterflap van deze handreiking open.



Na bekrachtiging door het management van de operationele beveiligingsvisie en de daarbij horende kosten, kan de implementatie van de verschillende maatregelen vanuit een projectmanagement aanpak worden uitgevoerd.

Vormen van OSP-documentatie vanaf Stap 1

De elementen van de OSP-documentatie worden al vanaf Stap 1 verzameld en gevormd. In Stap 7 wordt vastgelegd wat de voor het bedrijf meest praktische vorm is van OSP-documentatie en het beheerproces op het OSP. De eerder verzamelde elementen van de OSP-documentatie kunnen daarna in die structuur gevoegd worden.
Het verbeteren van beveiliging is een continu en cyclisch proces. Nadat de OSP-documentatie in de eerste cyclus gevormd is, kan hier in de volgende cyclus direct gebruik van worden gemaakt. Ook is het mogelijk om het beveiligingsplan per cyclus steeds verder te verfijnen.

3.1. Stap 1: Inventariseren beleid en randvoorwaarden

Doelstellingen van deze stap:
In deze stap wordt beschreven binnen wat voor soort bedrijf de beveiliging moet functioneren, wat het beleid is en wat de randvoorwaarden zijn voor de beveiliging.

Werkwijze

De werkwijze in deze stap is enigszins afhankelijk van het type bedrijf. Als het bedrijf veel gedocumenteerd heeft en haar plannen heeft vastgelegd in beleidsstukken is het vaak voldoende deze documenten te verzamelen, met een verificatie of de documenten nog gelden. In veel situaties zal de informatie ook verzameld moeten worden via interviews.

Denk bij het inventariseren van beleid en randvoorwaarden aan de volgende informatie:

Bedrijfsbeleid, missie

- Missie
- Algemeen bedrijfsbeleid
- Organisatiemodel
- Ontwikkelingen

Security beleid en –organisatie

- Scope van security beleid. Wat valt onder security en wat niet?
- Visie op beveiliging. Wat wil de organisatie bereiken met de beveiliging?
- Draagvlak en committment security beleid bij het management. Hoe belangrijk vindt het management beveiliging?
- Ethische standpunten. Wat is gewenst, wat is acceptabel en wat niet?
- Organisatie van beveiliging. Hoe zijn binnen de organisatie taken, verantwoordelijkheden en bevoegdheden belegd op het gebied van beveiliging?

Externe beleidsrelaties

Wat zijn de externe eisen en aanbevelingen die relevant zijn voor de inrichting van de beveiliging.

- Wat voor eisen stellen klanten?
- Is er wet- en regelgeving van toepassing?
- Wat is het branchebeleid?
- Zijn er voorbeelden vanuit andere organisaties of andere onderdelen van de eigen organisatie (good practices)?
- Wat is de invloed van het beleid van publieke veiligheidsorganisaties, zoals politie, gemeente, brandweer?

Interne beleidsrelaties

Wat zijn interne beleidsrelaties met de beveiliging en wat voor eisen worden gesteld vanuit:

- Bedrijfsvoering
- Bedrijfscontinuïteitsmanagement
- Environment
- Arbo / Occupational Health Safety Assesment Series (OHSAS)
- Informatie- en Communicatietechnologie (ICT)
- Huisvesting
- Facilitair
- Human resource management (HRM)
- Financiën

Vastlegging van te beschermen belangen

Hierbij wordt vastgelegd wat de belangrijkste te beschermen belangen zijn. Bijvoorbeeld:

- Reputatie
- Mensen
- Productiemiddelen
- Voorraden, producten en diensten
- Informatie en informatietechnologische middelen
- Communicatie en communicatiemiddelen
- Gebouwen

Vastlegging van de statische inrichting van het bedrijf

Hierbij gaat het om de statische informatie van de bedrijfsinrichting en mogelijke ontwikkelingen hierin.

Denk hierbij aan:

- Aantal locaties
- Omgeving van de locaties, bijvoorbeeld stedelijk, landelijk of industriegebied
- Infrastructuur naar het bedrijf:
  - Wegen, spoorwegen, waterwegen
  - Nutsvoorzieningen
  - ICT-netwerken
- Omgevingsdreigingen:
  - Lokale criminaliteit
  - Overstroming
  - Bedrijven in buurt met gevaarlijke stoffen
- Bedrijfsterrein, gebouwen en bedrijfsfuncties hierop
- Gebouw, ruimten in gebouw en bedrijfsfuncties hierin

Vastlegging van mens- en processtromen

Vastleggen van de dynamische informatie uit de bedrijfsinrichting en mogelijke ontwikkelingen hierop:

- Goederenstromen naar, van en door de locatie
- Autoverkeer naar, van en door de locatie
- Personenverkeer:
  - Hoeveel personen
  - Waar en wanneer toegang
  - Wat voor personen, bijvoorbeeld medewerkers, contractors, leveranciers of bezoekers
- Informatiestromen

Aan het einde van deze stap zijn de volgende resultaten bereikt:

- De huidige operationele organisatie van beveiliging is in kaart gebracht en gedocumenteerd.
- Relevante gegevens over de bedrijfsinrichting, beleid, doelstellingen en randvoorwaarden op de beveiliging zijn verzameld en gedocumenteerd.

3.2. Stap 2: Concretiseren van beveiligingsdoelen

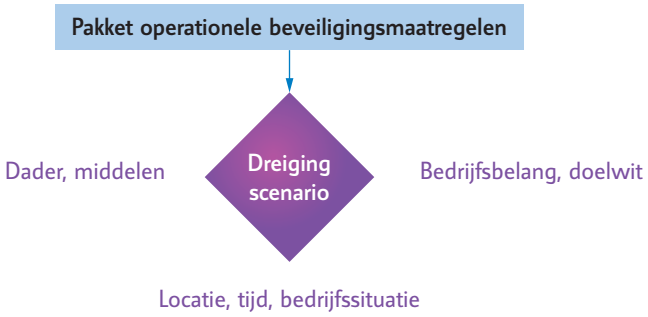
Doelstellingen van deze stap:
In deze stap worden de vaak breed gedefinieerde doelen uit het beveiligingsbeleid en de bedrijfsbrede (security) risicoanalyse geconcretiseerd. Hiermee wordt het mogelijk om in Stap 6 een operationele risicoanalyse in concrete situaties uit te voeren

Werkwijze

De security manager definieert de beveiligingsdoelen uit de risicoanalyse zo concreet mogelijk. Vanuit de risicoanalyse is er bijvoorbeeld een doelstelling geformuleerd over het beveiligen van bepaalde bedrijfsmiddelen tegen gelegenheidscriminaliteit. In de concretiseringsslag wordt dan bepaald dat gelegenheidscriminelen die zich in de buurt van deze assets bevinden, tegengehouden moeten worden.
Naast doelen die een relatie hebben met risicobeheersing zijn er ook andere doelen die concreet gemaakt moeten worden. Als in het beveiligingsbeleid bijvoorbeeld staat dat de beveiliging moet voldoen aan 'wet- en regelgeving', dan kan in deze stap expliciet gemaakt worden om welke wet- en regelgeving het gaat.
Bespreek het resultaat van deze stappen met de bedrijfsleiding om vast te stellen of de geconcretiseerde beveiligingsdoelen nog steeds passen binnen de visie en kaders van het beveiligingsbeleid en bedrijfsbeleid.

Doelen in relatie tot risicobeheersing

Uit de risicoanalyse blijkt welke bedrijfsbelangen bedreigd worden. Om een concrete voorstelling te krijgen van (mogelijke) aanvallen en de beveiliging hierop is het nuttig om de belangrijkste dreigingen vanuit de volgende invalshoeken te beschouwen:



1. Wat zijn doelwitten of bedrijfsbelangen die beschermd moeten worden?
2 Wat zijn de potentiële daders, wat willen zij en wat voor kracht hebben zij?
3. Wat zijn locaties, tijdstippen en omstandigheden waar de dader kan of wil toeslaan? Waar is het doelwit kwetsbaar voor dreigingen?
4. Waaruit bestaat de beveiliging?

De dreigingssituaties en beveiligingsdoelstellingen die in deze stap worden benoemd kunnen in Stap 3 t/m 6 worden gebruikt als input voor een detail operationele risicoduiding.

Voorbeelden van beveiligingsdoelen die kunnen worden nagestreefd:

A Voorkomen dat gevoelige informatie in het publieke domein komt;
B Afschermen van het object en bemoeilijken van verkenningsacties;
C Afschrikken en ontmoedigen van kwaadwillenden;
D Tegenhouden van de dader;
E Detecteren van een (mogelijk) incident;
F Detecteren, vertragen en interventie;
G Consequenties verminderen;
H Registratie van procesuitvoering (safe guarding);

In Bijlage 3 worden de beveiligingsdoelen verder uitgewerkt en zijn voorbeelden opgenomen van maatregelen die passen bij deze doelen. Bij het concretiseren van beveiligingsdoelen kan eventueel ook gebruik worden gemaakt van de terminologie over daders, hulpmiddelen, bedrijfsbelangen en type situaties zoals die zijn opgenomen in Bijlage 1.

Overige doelen

Naast risicobeheersing zijn er ook andere doelen die kunnen gelden voor de beveiliging. Denk ondermeer aan:

- Voldoen aan eisen uit wet- en regelgeving;
- Integratie van verschillende toegangsystemen;
- Doelstellingen en eisen aan beveiligers en beveiligingsmaatregelen in de gevolgenbestrijding van een incident;
- Doelstelling en eisen aan beveiligingsmaatregelen ten behoeve van safety;
- Maatschappelijke of management opinie om een bepaalde maatregel te treffen;
- Aantoonbaar maken van effect van beveiliging en eisen en wensen op het afleggen van verantwoording;
- Kosteneffectiviteit van maatregelen ten opzichte van andere maatregelen met een vergelijkbaar beveiligingseffect inzichtelijk maken;
- Beheerskosten van maatregelen en keuzen op standaardisatie en architectuur van maatregelen inzichtelijk maken.

Aan het einde van deze stap zijn de volgende resultaten bereikt:

- De doelen op de beveiliging zijn zodanig geconcretiseerd dat een operationele risicoanalyse kan worden uitgevoerd.
- De doelen zijn vastgelegd in een document en afgestemd met de bedrijfsleiding.

3.3. Stap 3: Concretiseren belangen en afhankelijkheden

Doelstellingen van deze stap:
In deze stap wordt gedetaileerd inzicht verkregen in de belangen van het bedrijf en waar deze belangen van afhankelijk zijn. Vervolgens wordt de lokalisering van de te beschermen belangen bepaald en wordt het geheel vastgelegd in een document.

Werkwijze

In deze stap wordt detail inzicht opgebouwd in de te beschermen belangen en waar deze belangen van afhankelijk zijn, omdat ook de afhankelijkheden beveiliging nodig kunnen hebben.

Onderzoek op detailniveau de bedrijfsbelangen. Deze komen voort uit de risicoanalyse en zijn vastgesteld door het management van het bedrijf. De detailanalyse bevat aspecten als:

- Waaruit bestaat precies het te beschermen belang? Wat is de begrenzing?
- Wat is de betekenis van dit belang voor het bedrijf?
- Wat is de exacte locatie waar het belang zich bevindt? Kan het belang zich ook verplaatsen naar andere locaties?
- Hoe wordt dit belang gebruikt in de bedrijfsprocessen?
- Wanneer wordt dit belang gebruikt?
- Wie maakt er direct gebruik van? Wie bedient en beheert het belang?
- Is de kwetsbaarheid van het belang hoger in bepaalde bedrijfsituaties?[3]

Leg dit detailinzicht vast in een document.

Onderzoek vervolgens waar het goed functioneren van de belangen van afhankelijk is, bijvoorbeeld elektra en communicatievoorzieningen. Ook deze componenten kunnen beveiliging nodig hebben. Leg daarbij vast wat en hoe de afhankelijkheden zijn, evenals het functioneren en de lokalisering van deze componenten.

3 De belangen kunnen afhankelijk zijn van bedrijfssituaties. Denk aan variabele voorraadgrootten. Een voorraad is kwetsbaarder tijdens de transportfase dan tijdens de opslagfase op de door de operator gecontroleerde locatie.

Aan het einde van deze stap zijn de volgende resultaten bereikt:
- De te beschermen belangen zijn gedefinieerd, inclusief de elementen waarvan de belangen afhankelijk zijn.
- Ook is vastgelegd wat de locaties en bedrijfssituaties zijn waar de bedreigde belangen zich bevinden.

3.4. Stap 4: Concretiseren van dreigingen

Doelstellingen van deze stap:
In deze stap worden de dreigingen verder geconcretiseerd tot aanvalscenario's of dader-daad scenario's.
Deze scenario's zullen in Stap 6 worden gebruikt om vast te stellen of de huidige beveiliging toereikend is voor de in Stap 2 geformuleerde doelen.

Werkwijze

In de dreigingscenario's wordt vanuit daderperspectief de daad beschreven. Zie Bijlage 2 voor een verloop van een incident vanuit daderperspectief.
Ontwikkel voor de belangrijkste dreigingen scenario's. Bij het opstellen daarvan kan onder meer gedacht worden aan onderstaande vragen:
- Wie is de dader?
- Is deze alleen of werkt de dader samen?
- Wat is de motivatie van de dader?
- Wat voor daad wil de dader uitvoeren?
- Wat heeft de dader nodig om na afloop van de daad genot te kunnen hebben. Bijvoorbeeld: helers voor de verkoop van gestolen goed, een communicatieplatform om de motieven van de aanslag of actie te kunnen verspreiden.
- Wat voor hulpmiddelen heeft de dader? Denk aan kennis, toegangsmiddelen, middelen om weg te komen.
- Waar, wanneer en onder welke omstandigheden wil de dader toeslaan?
- Hoe gaat de dader te werk?

Aan het einde van deze stap zijn de volgende resultaten bereikt:
De dader/daad scenario's waar de beveiliging mee rekening moet houden zijn vastgelegd.

3.5. Stap 5: Inventariseren huidige maatregelen

Doelstellingen van deze stap:
In deze stap wordt geïnventariseerd en vastgelegd wat de huidige beveiligingsmaatregelen zijn.

Werkwijze

Voor een OSP is van belang dat alle beveiligingsmaatregelen gedocumenteerd zijn en beheerd worden. Een organisatie die voor het eerst systematisch een OSP opstelt, heeft vaak slechts gedeeltelijk de genomen beveiligingsmaatregelen gedocumenteerd. In deze situatie kan de organisatie ervoor kiezen om een volledige inventarisatie uit te voeren van zowel de gedocumenteerde als de niet gedocumenteerde maatregelen. De organisatie kan er echter ook voor kiezen om de detaildocumentatie van maatregelen in een latere projectstap uit te voeren.

Niet alle maatregelen hoeven per locatie volledig uitgediept te worden. Vaak kunnen Stap 6 (vaststellen effectiviteit van maatregelen) en Stap 7 (ontwerpen gewenst maatregelenmix) uitgevoerd worden wanneer gegevens bekend zijn die gelden voor meerdere type locaties en maatregelen. Slechts indien nodig hoeven deze te zijn uitgewerkt op detailniveau. Als bijvoorbeeld in een detailanalyse geconstateerd wordt dat het compartimenteringsconcept en de bouwkundige maatregelen te wensen overlaten én het duidelijk is dat dit voor alle locaties geldt, dan is die kennis voldoende om conclusies te trekken ten aanzien van de risicobeheersing en het maatregelenbeleid.

Het inventariseren van het huidige pakket van maatregelen gebeurt aan de hand van:

- **Uitvoeren van documentonderzoek**
  Uit dit documentonderzoek wordt duidelijk:
  - Wat de beveiligingsmaatregelen zijn;
  - Wat de kwaliteit van de maatregelen is;
  - Wat de kwaliteit van de vastgelegde documentatie is.

- **Uitvoeren van interviews**
  Deze interviews worden gehouden met zowel personen die verantwoordelijk zijn voor het maatregelenbeleid als met personen die over operationele kennis beschikken. Uit de interviews blijkt:
  - Wat de beveiligingsmaatregelen zijn;
  - Wat achterliggende concepten zijn;
  - Wat de kwaliteit van de maatregelen is;
  - Wat ontwikkelingen zijn in het beheer van de maatregelen;
  - Wat de knelpunten zijn in de omgang met de maatregelen;
  - Wat het kennisniveau is en de opvattingen zijn van de gesprekspartner.

- **Schouwen van de situatie**
  Uit de schouw van de situatie blijkt:
  - Wat de fysieke beveiligingsmaatregelen zijn;
  - Of de gedocumenteerde en/of vertelde maatregelen overeenkomen met de praktische situatie;
  - Wat de kwaliteit van die maatregelen is;
  - Wat kwetsbaarheden zijn in de fysieke maatregelen.

Bij de inventarisatie van maatregelen is het nuttig om onderscheid te maken tussen maatregelen die een generieke werking hebben in de hele organisatie en maatregelen die alleen op een specifieke locatie of bedrijfssituatie werken.

Inventariseren/vastleggen van generieke maatregelen in een organisatie

Voorbeelden van generieke maatregelen:

- Toegangsbeleid
- Centrale meldkamer
- Personele aspecten van security
- Sanctiebeleid
- Trainingsprogramma's en security bewustwording
- Omgang eindgebruikers met risico's en beveiligingsmaatregelen
- Privacy richtlijn
- Contracten met leveranciers en met ketenpartners die van invloed zijn op de security
- Informatiebeveiligingsbeleid

Voorbeelden van ontwerp-, beheer- en organisatiemaatregelen:

- Richtlijnen op te selecteren maatregelen en op het wijzigingsbeheer;
- Organisatie van beveiliging;
- Beheerorganisatie en beheermaatregelen, prestatie-indicatoren van beheer.

Inventariseren/vastleggen van locatiespecifieke maatregelen

De locatiespecifieke maatregelen zijn grofweg te verdelen in fysieke maatregelen, die op een situatieschets afgebeeld kunnen worden en organisatorische maatregelen voor de betreffende locatie.

Situatieschets van bedrijfslocatie

- Omgeving van bedrijf: industrieterrein, landelijke of stedelijke omgeving, toegangsroutes
- Bedrijfsterrein
- Terreingrenzen
- Fysieke barrières op terreingrenzen, zoals hekwerken, grachten, muren
- Compartimentering binnen terrein en fysieke barrières
- Gebouwen op terrein
- Toegangen, vluchtwegen, hulpverleningswegen op terrein
- Toegangsmiddelen op terrein, zoals poorten, slagbomen, intercoms, verlichting
- Parkeervoorzieningen
- Richting/gebod/verbod/waarschuwing borden
- Verlichting op terrein
- Closed-circuit television (CCTV)
- Detectiemiddelen

Situatieschets per gebouw

- Gevels, wandsterkte
- Mechanische beveiligingsmaatregelen op deuren, ramen en andere gevelopeningen
- Toegangen en vluchtwegen van gebouw
- Type toegangsvoorzieningen
- Brand- en inbraakcompartimenten
- Toegangsdeuren en vluchtwegen van compartimenten
- Beveiligingsverlichting
- CCTV

Technische security systemen

- Configuratie elektravoorzieningen voor beveiligingsinstallaties
- Configuratie beveiligingsnetwerk
- Inbraak/toegangsysteem
- CCTV
- Omroep
- Oproep
- Beveiligingsverlichting
- Intercom
- Technisch Security Management Systeem

Organisatie en procedures

- Verantwoordelijkheden en organisatie van beveiliging op locatie
- Beheer van sleutelplan, toegangs- en schakelrechten
- Functioneel beheer van maatregelen
- Technisch beheer van maatregelen
- Omgang eindgebruikers met risico's en beveiligingsmaatregelen
- Beheer van beveiligingscompetenties op locatie
- Bewakingsplan
- Toegangsprocedures op locatie
- Afspraken met externe beveiligingsorganisaties, zoals alarmcentrale en externe beveiligers
- Afspraken met publieke veiligheidsorganisatie, zoals politie en brandweer
- Procedures, onder meer omgang met:
    - Verdachte persoon, verdachte auto
    - Alarmmelding

- Inbraak
- Manipulatie van toegangsysteem
- Brand
- Overval
- Bommelding
- Bombrief

Aan het einde van deze stap zijn de volgende resultaten bereikt:
De huidige beveiligingsmaatregelen zijn geïnventariseerd en gedocumenteerd.

3.6. Stap 6: Uitvoeren van operationele risicoanalyse

Doelstellingen van deze stap:
In deze stap wordt duidelijk wat de motivatie is van het huidige pakket aan beveiligingsmaatregelen en of deze effectief is op de vastgestelde beveiligingsdoelen. Situaties waar de beveiliging niet effectief is, worden vastgelegd in een lijst met kwetsbaarheden. Ook tegenstrijdigheden en maatregelen die geen doel dienen worden gerapporteerd.

Werkwijze

Deze stap bestaat uit de volgende activiteiten:
- Vaststellen reden en doel van de huidige maatregelen;
- Vaststellen effectiviteit van de maatregelen in relatie tot aanvalscenario's;
- Rapporteren van huidige kwetsbaarheden en van overbodige maatregelen.

Vaststellen reden en doel van maatregel

In deze stap worden de redenen voor de huidige beveiligingsmaatregelen vastgesteld.

Vragen die per maatregel moeten worden beantwoord zijn:
- Treedt de maatregel op bij specifiek te beschermen belangen of bij specifieke dader-daad scenario's?
- Wat is het beveiligingsdoel van de maatregel?[4]
- Waarom is er gekozen voor deze maatregel?

Zoals in Stap 2 is aangegeven kunnen naast risicobeheersingsdoelen ook andere redenen bestaan voor beveiligingsmaatregelen.

Plaats maatregelen waarvoor geen enkele reden is te bedenken op een lijst met overbodige maatregelen.
In het implementatietraject (Stap 9) kunnen deze maatregelen worden afgevoerd. Leg ook eventuele tegenstrijdigheden vast.

Vaststellen effectiviteit van maatregelen in relatie tot aanvalscenario's

Redenerend vanuit de dader/daad scenario's, die in Stap 4 zijn opgesteld, kan onderzocht worden hoe effectief de maatregelen zijn in de voorbereidingsfase van een incident, in de uitvoeringsfase (toegang, uitvoering en aftocht) en in de genotsfase van het incident.
In bijna alle scenario's moet de dader zich toegang verschaffen tot het doelwit. Wat zijn de mogelijke toegangspaden en is de beveiliging op de verschillende aanvalspaden consistent?
Stel in deze operationele risicoanalyse vast of de aanwezige mix van beveiligingsmaatregelen effectief werkt voor de in de Stap 2 geformuleerde doelstellingen.

Plaats zwakheden en inconsistenties op een lijst met huidige kwetsbaarheden.

4 Zie Stap 2 in deze handleiding voor voorbeelden van beveiligingsdoelen en Bijlage 3 voor bijpassende maatregelen.

Rapporteren van huidige kwetsbaarheden

De rapportage over de huidige kwetsbaarheden moet worden besproken met de bedrijfsleiding. Ook inconsistenties en nutteloze maatregelen kunnen in dit overleg naar voren komen. Dit overleg vergroot het bewustzijn over de operationele risico's en creëert draagvlak voor de beveiligingsmaatregelen die nodig zijn.

Aan het einde van deze stap zijn de volgende resultaten bereikt:

- Van de huidige beveiligingsmaatregelen is vastgesteld waarom ze er zijn en of ze voldoen aan de beveiligingsdoelen. Maatregelen zonder reden staan op een lijst om te worden afgevoerd.
- Redenerend vanuit de dader/daad scenario's is vastgesteld of de huidige beveiligingsmaatregelen effectief zijn om de beveiligingsdoelen te halen. Zwakke plekken in de beveiliging zijn vastgelegd in een lijst met huidige kwetsbaarheden.
- De bedrijfsleiding is geïnformeerd over de resultaten van deze operationele risicoanalyse met de huidige kwetsbaarheden.

3.7. Stap 7: Ontwerpen hoofdlijnen te nemen maatregelen

Doelstellingen van deze stap:

Met deze stap wordt de vorming van een hoofdontwerp en visie op de gewenste beveiligingsmaatregelen bereikt.

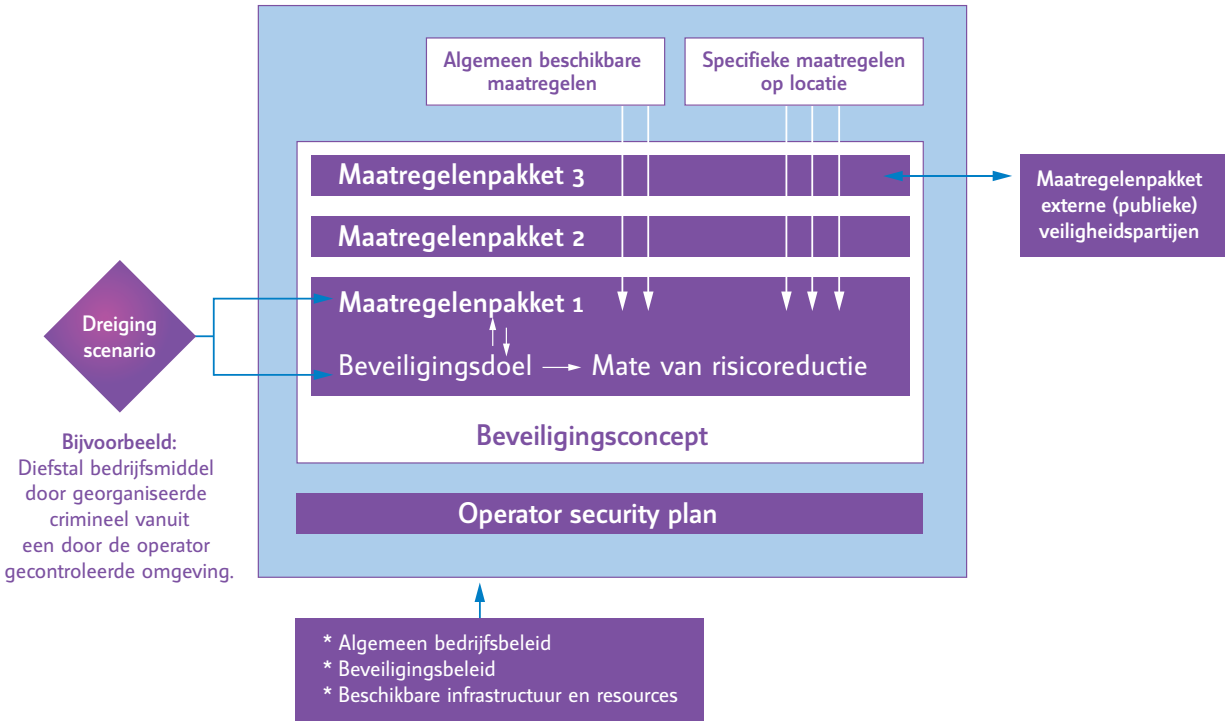
Werkwijze

Deze stap bestaat uit de volgende uit te voeren activiteiten:

- Ontwerpen van maatregelen met als vertrekpunt security scenario's;
- Ontwerpen van maatregelen met als vertrekpunt generieke werking;
- Ontwerpen van maatregelen bij verhoogde dreiging;
- Ontwerpen maatregelen voor andere doelstellingen;
- Ontwerpen van OSP (beheer) structuur;
- Keuzen maken voor maatregelen.

Ontwerpen van maatregelen met als vertrekpunt security scenario's

Het maatregelenontwerp moet antwoord geven op de aanvalsscenario's uit de (operationele) risicoanalyse.



Per aanvalscenario moet het beveiligingsconcept duidelijk zijn. Het beveiligingsconcept kan bestaan uit verschillende maatregelenpakketten, ieder met een eigen doel en een bepaalde risicoreductie. Een maatregelenpakket wordt gevormd door algemeen in de organisatie beschikbare maatregelen (bijvoorbeeld personele maatregelen en beschikbaarheid van de meldkamer) en maatregelen die specifiek voor een locatie aanwezig zijn. Daarnaast kan een maatregelenpakket komen van een externe, publieke veiligheidspartij zoals de politie.[5]
Een beveiligingsconcept bestaat uit enkele maatregelenpakketten. Per maatregelenpakket is vastgelegd:

- Waaruit bestaat de maatregel(groep)?
- Wie zijn betrokkenen bij uitvoering van de maatregel en het beheer van de maatregel?
- Wat is het doel van deze maatregel(groep)?[6]
- Wat is het verwachte effect (risicoreductie) van dit maatregelenpakket?

Met het vastleggen van het beveiligingsconcept wordt helder in welke mate de beveiligingsmaatregelen het risico verminderen.

Dit expliciet vastleggen van het maatregelenbeleid op criminele scenario's vindt in de praktijk alleen bij een beperkt aantal en meest bedreigende scenario's plaats. Bij het opstellen van teveel scenario's of scenariovarianten worden de verschillen in beveiligingsconcept te gering. Dat geldt ook voor de communicatieve waarde daarvan. Het aantal bruikbare scenario's is altijd afhankelijk van de context.

Ontwerpen van maatregelen met als vertrekpunt generieke werking

Veel beveiligingsmaatregelen zijn doeltreffend bij meerdere soorten dreigingen. Deze maatregelen kunnen benoemd worden als generieke beveiligingsmaatregelen. Bijvoorbeeld: de invoering van een compartimenteringsconcept, personele beveiligingsmaatregelen, sleutelbeheer of privacy reglement.
Ook hier moet worden vastgelegd wat de maatregel inhoudt, wie betrokkenen zijn bij de uitvoering en het beheer en wat het doel is.

Ontwerpen van maatregelen bij verhoogde dreiging

Wanneer een bedrijf is aangesloten op het Alerteringssysteem Terrorismebestrijding (ATb) van de Nationaal Coördinator Terrorismebestrijding (NCTb), is het verplicht drie aanvullende maatregelenpakketten voor hogere dreigingsniveaus te hebben. Deze niveaus worden aangeduid met de volgende termen:

- Lichte dreiging
- Matige dreiging
- Hoge dreiging

Het kunnen schakelen tussen de permanent aanwezige maatregelen (op basis beveiligingsniveau) en beveiligingsmaatregelen die zijn aangepast aan een specifiek dreigingsniveau is echter ook aan te bevelen voor bedrijven die niet zijn aangesloten op het ATb. In dat geval zal schakelen naar beveiliging in een hoger dreigingsniveau niet door de NCTb, maar door het bedrijf zelf worden geïnitieerd. Het is hierbij verstandig dezelfde systematiek te hanteren als die van het ATb.

---

5 Enkele voorbeelden van beveiligingsconcepten op de dreiging door een georganiseerde crimineel met inbraak en diefstal van een attractief bedrijfsmiddel in een door de operator gecontroleerde omgeving zijn:
- Voorkomen dat het bedrijf op haar internetsite en in bedrijfsinterviews ruchtbaarheid geeft dat zij over dit bedrijfsmiddel beschikt en nemen van zichtbeperkende maatregelen op dit bedrijfsmiddel. Het beveiligingdoel is het voorkomen dat een potentiële dader kennis opbouwt over de locatie van deze aantrekkelijke buit.
- Inrichten van de omgeving van het bedrijf, waarbij het aantal toegangen (en vluchtwegen!) beperkt is, er een heldere terreinscheiding is, een vrij zicht is op het buitenterrein tot aan de gevels inclusief passende verlichting en een opgeruimd en beheerd terrein en gebouwaanblik. Deze 'security footprint' verhoogt de pakkans perceptie bij de dader en heeft een ontmoedigende werking om verdere verkenningsacties uit te voeren en tot daadwerkelijke inbraak over te gaan.
- Inbraakdetectie in het gebouw en het treffen van bouwkundige en braakwerende maatregelen tot de exacte locatie van het bedrijfsmiddel. De braakwerkendheid moet zodanig zijn dat het de dader meer tijd kost om het doelwit te bereiken, dan de periode dat bijvoorbeeld bedrijfsmedewerkers of beveiligers kunnen ingrijpen. Doel van deze interventie is de dader met lege handen uit het pand te verjagen. Indien alarmverificatie op afstand plaatsvindt, kan in een vroeg stadium de politie worden opgeroepen. Dit vergroot de kans om de daders op heterdaad te pakken.

6 Zie Stap 2 in deze handleiding voor voorbeelden van beveiligingsdoelen en Bijlage 3 voor bijpassende maatregelen.

In het OSP moet vastliggen hoe bij een veranderd dreigingsniveau omgegaan wordt met de volgende zaken:
- Op welke wijze wordt verandering van dreiging geïnitieerd en wie komen bij elkaar en beslissen;
- Coördinatie en informatiedeling met externe veiligheidspartners;
- Coördinatie en informatiedeling binnen het bedrijf zelf.

Alle maatregelen moeten al op basisniveau bestaan of voorbereid en geoefend zijn, waardoor het bedrijf bij verhoogde dreiging in korte tijd het regime kan aanpassen.

De soorten maatregelen per dreigingsniveau zijn maatwerk. Om u te ondersteunen bij het afstemmen van de beveiligingsmaatregelen in verschillende dreigingsniveaus heeft het NAVI de handreiking Beveiligingsafstemming Vitaal en Overheid (BAVO) gemaakt. Hierin wordt beschreven hoe bedrijven uit de vitale sectoren samen met de lokale en regionale overheidspartners afspraken kunnen maken over de afstemming van de (opgeschaalde) beveiligingsmaatregelen en de reactie op incidenten. De handreiking behandelt verschillende soorten dreigingen. U kunt deze handreiking downloaden op de website van het NAVI: www.navi-online.nl

Ontwerpen maatregelen voor andere doelstellingen

Veel ontwikkelingen in het maatregelenbeleid zijn niet direct gekoppeld aan de risicoanalyse, maar eerder aan ontwikkelingen in het beheer van de maatregelen. Hierbij valt te denken aan technische en economische afschrijving van middelen en opvattingen ten aanzien van wenselijke integraties van beveiligingssystemen, -infrastructuren en andere type maatregelen.

Vragen daarbij zijn:
- Wat zijn knelpunten in de maatregelen?
- Wat zijn knelpunten in het beheer van de maatregelen?
- Wat zijn verwachte ontwikkelingen in het beheer van de maatregelen?
- Waar is efficiency te behalen in de maatregelen en het beheer?
- Wat is de opvatting over de huidige architectuur van de maatregelen?

Vanzelfsprekend moet het nieuwe ontwerp niet alleen een beter beheer mogelijk maken, maar ook aan de doelstellingen van de risicobeheersing voldoen.

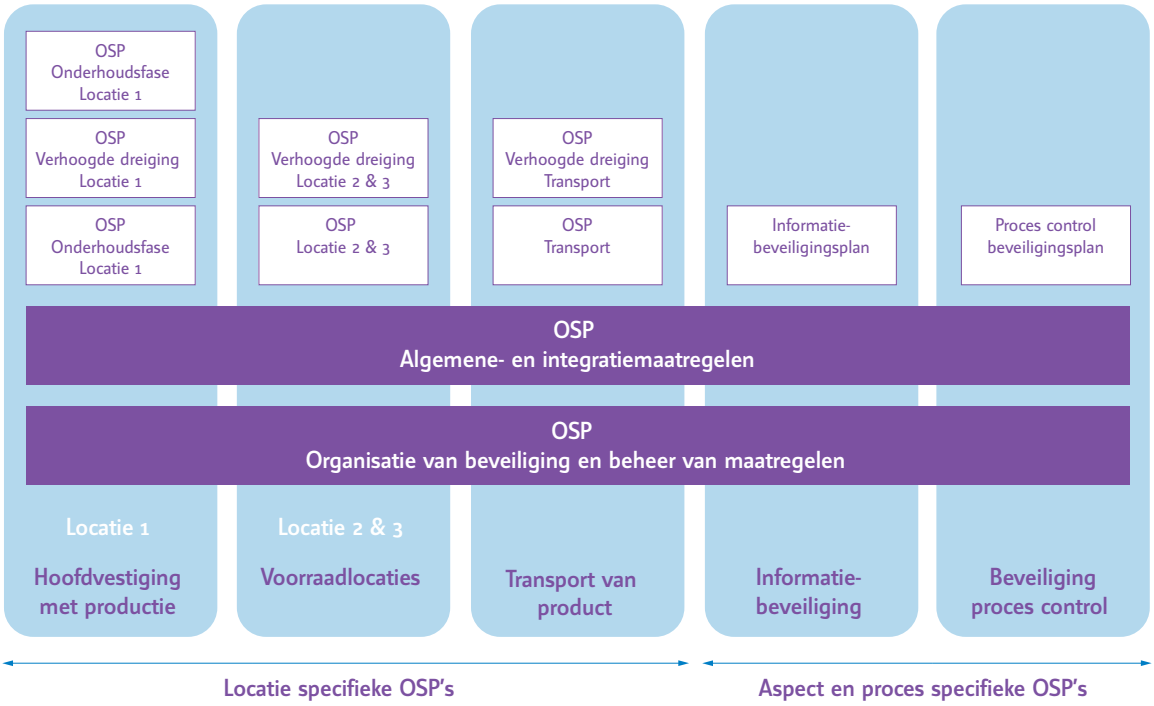
Hierbij moeten de volgende vragen beantwoord worden:
- Waaruit bestaat de maatregel(groep)?
- Wie zijn betrokkenen in het gebruik en het beheer van de maatregel?
- Wat is de doelstelling?
- Wat is het verwachte effect?

Ontwerpen van OSP (beheer) structuur

Bij deze stap wordt vastgesteld wat voor het bedrijf de meest praktische wijze is om het OSP te documenteren en te beheren.

Structuur van OSP's

Alle beveiligingsmaatregelen kunnen in één OSP worden vastgelegd, maar dat hoeft niet. In wat grotere en complexere organisaties kan het nuttig zijn om een structuur van meerdere beveiligingsplannen in te voeren.



In bovenstaand voorbeeld zijn er twee OSP's die voor het hele bedrijf van toepassing zijn:

- OSP voor de organisatie van de beveiliging en het beheer van de maatregelen.
- OSP met algemene en integratiemaatregelen. Bijvoorbeeld integriteitsmaatregelen voor personeel, toegangsbeleid, CCTV-richtljin, centrale meldkamer.

In het voorbeeld heeft het bedrijf een hoofdlocatie waar de productie plaatsvindt en twee vergelijkbare voorraadlocaties. Daarnaast vindt er transport van het product plaats.

Voor de hoofdlocatie is er een OSP, een supplement beveiligingsplan dat in werking treedt bij verhoogde dreiging en een plan dat van toepassing is in de onderhoudsfase van de productie, waarbij vele buitenstaanders activiteiten op het terrein uitvoeren.

Voor de voorraadlocaties en voor het transport zijn er aparte beveiligingsplannen. Daarbij kunnen er aspect- en/of proces specifieke OSP's worden gemaakt. In het voorbeeld heeft het bedrijf een informatiebeveiligingsplan en een plan op de beveiliging van de proces control.

Beheer van documentatie

In het OSP moet vastliggen wie welke onderdelen van het OSP in beheer heeft. Ook moet vastliggen wat het wijzigingsproces is op de documentatie.

Welke elementen documenteren
In het OSP moet zijn opgenomen welke elementen gedocumenteerd moeten zijn. Wat zijn de belangrijkste maatregelen en principes die in ieder geval gedocumenteerd moeten worden en op welke wijze moet dat gebeuren? Toegangsrechten liggen al vast in het operationele toegangbeheersysteem. Zij moeten echter ook in een aparte documentatieomgeving worden vastgelegd om ongewenste effecten van analyseactiviteiten op de operationele toegangsomgeving te voorkomen.

Bekendheid van maatregelen en kennis van zaken
De invulling van de documentatiestructuur is afhankelijk van de communicatiewensen om eindgebruikers en beheerders bekend te maken met de beveiliging. Ook de kennis van zaken van beheerders ten aanzien van beveiliging speelt daarbij een rol.

Vertrouwelijkheid
Een bijzonder aspect in de documentatiestructuur is het waarborgen van de vertrouwelijkheid van onderdelen van het OSP. De documentatie- en beheerstructuur moet hier rekening mee te houden.

Keuzen maken voor maatregelen
Nadat alle afwegingen uit de vorige paragrafen zijn gemaakt moeten er keuzen worden gemaakt voor de samenstelling van de maatregelenpakketten. In Bijlage 5 worden verschillende maatregelen verder uitgewerkt.

Het samenstellen van een maatregelenmix en het maken van een hoofdontwerp van beveiligingsmaatregelen vraagt nauwe afstemming met partijen en randvoorwaarden die in Stap 1 zijn verwoord. Ook hierin moeten keuzen worden gemaakt. Het afstemmings- en keuzeproces heeft bovendien een relatie met de bewustwording en het creëren van draagvlak voor de in te voeren maatregelen. Hoe deze afstemming plaatsvindt, is afhankelijk van de organisatie en de context daarvan.

In deze afstemming en besluitvorming kan naar voren komen dat er geen acceptabel pakket aan beveiligingsmaatregelen te ontwerpen is voor de beveiligingsdoelstellingen (Stap 2) en binnen de randvoorwaarden (Stap 1). Kijk dan of de doelstellingen in Stap 2 aan te passen zijn binnen de strekking van het beveiligingsbeleid. Lukt dat niet, ga dan na op het niveau van het beveiligingsbeleid of op bedrijfsbeleid welke aanpassingen van de doelstellingen en randvoorwaarden voor de beveiliging nodig zijn.

Wanneer ook het kosten- en implementatieplan is opgesteld, kan de bedrijfsleiding in Stap 8 formeel akkoord gaan met de invoering van de maatregelen.

Aan het einde van deze stap zijn de volgende resultaten behaald en in documenten vastgelegd:
- Hoofdontwerp op de te nemen beveiligingsmaatregelen.
- Ontwerp op de OSP-documentatie en het beheer hierop.
- Keuzen op de maatregelenmix en afstemming hiervan met betrokken partijen.

3.8. Stap 8: Opstellen van kosten- en implementatieplan

Doelstelling van deze stap:
Met deze stap worden de kosten van de voorgestelde maatregelen en de wijze van implementatie inzichtelijk gemaakt zodat vervolgens besluitvorming mogelijk is.

Werkwijze
Inzicht krijgen in de kosten en het opzetten van een implementatieplan is voor elke organisatie anders en wordt bepaald door de personen die de besluiten nemen over de security.

Deze stap bestaat uit drie onderdelen:

Opstellen kostenplan
In het kostenplan zijn in ieder geval de eenmalige kosten en de exploitatiekosten opgenomen. Mogelijk dient het kostenplan in de vorm van een business case gepresenteerd te worden.

Opstellen implementatieplan
Het implementatieplan is een projectenplan dat per project (maatregelgroep) aangeeft:
- Wie zijn betrokken bij ontwerp, bouw en implementatie;
- Wat zijn de kosten;
- Wat is de doorlooptijd;
- Wat zijn de afhankelijkheden van andere projecten.

Komen tot besluitvorming
De bedrijfsleiding moet de plannen formeel accorderen, voordat tot uitvoering wordt overgegaan. Als de plannen te kostbaar zijn, moet onderzocht worden op welke wijze de beveiligingsdoelen (Stap 2) of het beveiligingsbeleid (in security management systeem) kunnen worden aangepast.

Aan het einde van deze stap zijn de volgende resultaten behaald:
- Kosten- en implementatieplannen voor de te implementeren maatregelen zijn opgesteld.
- Bedrijfsleiding heeft de plannen goedgekeurd.

3.9. Stap 9: Implementeren maatregelen

Doelstellingen van deze stap:
In deze stap wordt een geplande beveiligingsmaatregel of groep van maatregelen gebouwd en ingevoerd in de organisatie. Dit gebeurt binnen de visie en het ontwerp op het totaal van huidige en gewenste beveiligingsmaatregelen (Stap 8).

Werkwijze
Het implementeren van de maatregelen wordt gefaseerd en projectmatig uitgevoerd.
Volg daarbij per project onderstaande stappen:

1. Maatregelenselectie.
   Op basis van de beveiligingsredenen, het maatregelenbeleid en hoofdontwerp (Stap 5) worden de maatregelen op detailniveau geselecteerd voor een bepaalde situatie.
2. Ontwerp.
   Het ontwerpproces ligt in het verlengde van de maatregelenselectie. In sommige situaties kan een standaardnorm worden geselecteerd die binnen het maatregelenbeleid aanwezig is. In andere situaties zijn de maatregelenselectie en het ontwerp maatwerk.
3. Vergunningaanvraag.
   Bij bouwkundige aanpassingen is vaak een vergunning nodig. Soms is toestemming van de ondernemingsraad vereist. Een aandachtspunt hierin is het bewaken van de vertrouwelijkheid van het beveiligingsplan.
4. Aanbesteding.
   Selecteren van de leverancier en aanbesteden. Er zijn niet alleen externe leveranciers, maar ook interne leveranciers die beveiligingsdiensten leveren. Denk bijvoorbeeld aan HRM, ICT en Facilitair. Naast diensten worden ook beveiligingsproducten aanbesteed. De omgang met vertrouwelijkheid is ook in de aanbesteding van belang.
5. Bouw maatregelen en begeleiding van bouwproces.
   De leverancier gaat de maatregelen (technisch, organisatorisch) verder ontwerpen en bouwen. De opdrachtgever heeft daarbij een begeleidende rol.

6. Samenstellen van maatregelen tot werkend geheel. Het samenstellen van de verschillende onderdelen tot een beveiligingsoplossing. Een oplossing kan bestaan uit een bouwkundige component, integratie in een elektronisch beveiligingssysteem en het opstellen van procedures.
7. Opleiden en testen.
   Opleiden van beheerders en eindgebruikers. Testen van maatregelen.
8. Communiceren en invoeren.
   Communiceren over het nieuwe gebruik van maatregelen en maatregelen invoeren.
9. Bijwerken van documentatie.
   Opleveren van documentatieset op werking en beheer van maatregelen en het bijwerken van het OSP.
10. Accepteren en in beheer nemen.
    Accepteren door de opdrachtgever en het in beheer nemen van de maatregel door een beheerder.
11. Audit en afstemmen van maatregelen.
    Het verhelpen van kinderziekten en het afstemmen van de maatregelen op de praktische gang van zaken. Kort na het in gebruik nemen wordt een audit uitgevoerd op de maatregelen om te beoordelen of deze in de praktijk correct worden toegepast en functioneren.

In complexere organisaties is het raadzaam in het OSP ook vast te leggen wat de kwaliteiteisen zijn van het wijzigingsproces en hoe dit proces moet worden uitgevoerd.

Aan het einde van deze stap zijn via verschillende deelprojecten:
- Maatregelengroepen ingevoerd in de organisatie.
- Actuele ontwerp-, werking- en beheerdocumenten van die maatregelen toegevoegd aan de OSP-documentatie.

3.10. Stap 10: Operationeel beheren van maatregelen

Doelstellingen van deze stap:
Met deze stap wordt bereikt dat de ingevoerde maatregelen de beoogde werking hebben in de beveiliging.
Het beheer van de maatregel wordt geregeld en dit beheer wordt bewaakt.

Werkwijze

Het pakket aan operationele beveiligingsmaatregelen moet voortdurend beschikbaar zijn om ingezet te worden in beveiligingssituaties. Het beheer op deze maatregelen is een continu proces.

Onderscheid in routinematige en niet-routinematige maatregelen

Om het gebruik en het beheer van de maatregel goed in de organisatie in te bedden, is het raadzaam binnen het OSP een duidelijk onderscheid te maken in maatregelen die gebruikt worden in routinematige situaties en niet-routinematige situaties.

De meeste security maatregelen bestaan uit routinematige handelingen die de security in stand houden en onder normale omstandigheden laten functioneren. Deze maatregelen worden uitgevoerd volgens ingeslepen procedures. Typische routinematige maatregelen zijn:
- Toegangbeheer
- Routinematig toezicht
- Alarmafhandeling van veel voorkomende incidenten
- Opleiden, trainen
- Technisch en functioneel beheren van de maatregelen

Er zijn echter ook situaties die niet routinematig zijn en waar de incidenten een veel groter effect kunnen hebben. Hierbij zal tijdens het incident snel opgeschaald worden naar hogere beslissingsniveaus en krachtiger optreden. Niet-routinematige omstandigheden zijn onder meer:

- Chantage, brand, geweld en andere incidenten die weinig voorkomen, maar grote impact hebben;
- Bijzondere bedrijfsomstandigheden, zoals verhuizen, bijzondere voorraden, VIP-bezoek;
- Wijzigen naar andere dreigings- en beveiligingsniveaus.

Operationeel beheren van de maatregelen

Het OSP moet aangeven wie het operationele beheer van de verschillende beveiligingsmaatregelen uitvoert. Het beheer kan bij huisvesting, HRM, ICT en andere afdelingen liggen. Leg in deelbeheerplannen vast waaraan dit beheer moet voldoen en hoe dat georganiseerd moet worden.

Voor bijvoorbeeld de elektronische beveiligingsmaatregelen is een contract met een gecertificeerd installatiebedrijf gewenst. Hierin worden afspraken opgenomen over bijvoorbeeld:

- Uitvoeren van regulier technisch onderhoud.
- Uitvoeren van het verhelpen van storingen. Wat is de reactietijd van het installatiebedrijf?
- Op welke wijze vindt opdrachtverstrekking aan het installatiebedrijf plaats?
- Wie van het installatiebedrijf voert de werkzaamheden uit? Is deze persoon gescreend?
- Welke informatie wordt aan het installatiebedrijf verstrekt en over welke informatie voert het installatiebedrijf het beheer? Op welke wijze wordt de vertrouwelijkheid, integriteit en beschikbaarheid van deze informatie gewaarborgd?
- Op welke wijze is de fysieke en digitale toegang geregeld voor het installatiebedrijf?

Stel in het OSP ook vast wat belangrijke kenmerken zijn van het beheer. Voor bijvoorbeeld de elektrische beveiligingsmaatregelen:

- Aantal storingen, niet functionerende componenten.
- Wat voor type storingen? Welk type storingen kunnen wijzen op een security incident (voorbereidingsfase, uitvoeringsfase, plaatsgevonden incident) en wat moet dan de reactie zijn?
- Tijdsduur van storingsoplossing.
- Wijze van inspectie van maatregelen op het bestaan en de werking en de rapportage hierover.

Operationeel monitoren van maatregelenbeheer en incidenten en het bijsturen hiervan

In het OSP moet vastliggen op welke wijze een rapportageproces is ingericht. Dit maakt het mogelijk de werking van de beveiligingsmaatregelen te monitoren en na te gaan hoe de operationele verbetering van maatregelen plaatsvindt. Bronnen waaruit de informatie komt zijn:

- De beheeractiviteiten op maatregelen;
- De omgang met routinematige situaties;
- De omgang met niet-routinematige situaties.

Op basis van elektronische, schriftelijke en mondelinge rapportages kan de security manager bijsturen. Dat kan in verschillende situaties nodig zijn:

- Verbeteren van het beheer en de uitvoering van de maatregelen. De geïmplementeerde maatregelen zijn in principe goed, maar ze worden niet goed toegepast.
- Kiezen van effectievere maatregelen binnen het maatregelenbeleid. Het maatregelenbeleid is in principe goed, maar op uitwerkingsniveau zijn verbeteringen gewenst.
- Aansturen op aanpassing van het beleid. Er hebben zich dreigingen voorgedaan die nog niet in de risicoanalyse benoemd zijn of het maatregelenbeleid blijkt in de praktijk onvoldoende effectief te zijn. Ook kan overwogen worden om de doelstellingen en randvoorwaarden aan te passen. Bijvoorbeeld: binnen een bedrijf waar het management zeer terughoudend is in de toepassing van screening, blijken regelmatig incidenten plaats te vinden met niet-integer personeel. Kan er alsnog meer van screening gebruik gemaakt worden of moeten met verdere compartimentering, technopreventie en controles de beveiligingsdoelstellingen bereikt worden?

Wijzigingsbeheer

Het OSP moet een procedure bevatten op het wijzigen van de maatregelen.

Aan het einde van deze stap zijn de volgende resultaten bereikt en vastgelegd in documenten:

- Het beheren van de operationele beveiligingsmaatregelen is een continu proces.
- In dit beheer wordt duidelijk gemaakt welke maatregelen door wie en hoe beheerd worden.
- Om het beheer van alle maatregelen te kunnen overzien heeft de security manager een rapportagefunctie ingericht voor het beheer en de operationele incidenten.

Bijlage 1: Belangen, daders, daden en omstandigheden

Bedrijfsbelang en/of doelwit

Wat zijn de bedrijfsbelangen en/of doelwitten waarop de dader het gemunt kan hebben? Een voorbeeld voor een indeling:

- Fysieke producten
- Fysieke diensten
- Informatie producten
- Productiemiddelen
- Besturingsystemen
- Gebouwen en terreinen
- Medewerkers, bezoekers en executives
- Informatie en IT-middelen
- Communicatie en communicatiemiddelen
- Imago

Doelwit vanuit daderperspectief

Het is nuttig om het te beschermen bedrijfsbelang te beschrijven vanuit de optiek van de dader en wat de dader er mee kan doen:

- Contanten
- Financiële middelen
- Verhandelbare goederen
- Vervoerbare goederen
- Aantrekkelijke goederen
- Goodwill
- Status
- Kennis

Dader

Er zijn verschillende mogelijkheden om dadertypen te onderscheiden. Bijvoorbeeld:

- Gelegenheidscrimineel
- Lichte crimineel
- Zware crimineel
- Verwarde persoon
- (ex-)Personeel
- Gewelddadige activist
- Inlichtingendienst
- Terrorist
- Script-kiddie
- Hacker
- Hactivist
- Activist

Daad

En wat is de onbevoegde daad? Bijvoorbeeld:

- Afluisteren
- Beschieten
- Bezetten en/of blokkeren
- Bom
- Brandstichting
- Carjacking
- Chantage
- Compromitteren (in opspraak brengen)
- Corruptie
- Denial of service aanval
- Diefstal
- Gijzeling en ontvoering
- Hacking
- Inbraak
- Infiltratie
- Insluiping
- Insluiting
- Manipulatie
- Molest aan bedrijfsmiddelen
- Molest aan gebouwen
- Nucleaire -, biologische - of chemische aanval
- Overval
- Sabotage van communicatiemiddelen
- Sabotage van processen
- Virussen

Dader hulpmiddelen

Een dader heeft ook hulpmiddelen:

- Kennis
- Geld
- Samenwerking
- Hulpmiddelen op de toegangsverschaffing
- Hulpmiddelen voor de vlucht
- Hulpmiddelen om genot te krijgen van de actie, zoals de helingmarkt voor gestolen goederen en een communicatiekanaal voor actievoerders

De dreigingen kunnen ook gegroepeerd worden op:

- Fysieke aanvallen: zoals diefstal al dan niet met braak, brandstichting, bomaanslag en/of sabotage
- Ordeverstoringen: zoals demonstratie, actie, arbeidsonlust en/of blokkade van bedrijf of transport
- ICT-aanvallen: zoals hacken, sabotage, virussen, Distributed Denial of Service (DDoS)

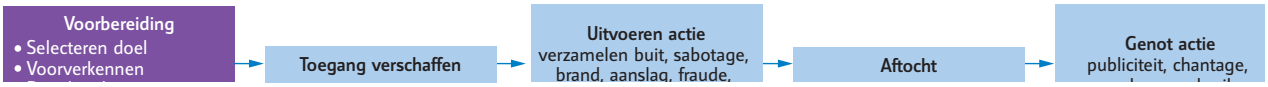
Plaats delict, omstandigheden van onbevoegde handeling

De plaats delict geeft de locatie, het tijdstip en de omstandigheden aan waar de potentiële dader kan of wil toeslaan en waar het doelwit kwetsbaar is. Een voorbeeld voor een indeling:

- Door operator gecontroleerde en bemande locatie
- Door operator gecontroleerde maar onbemande locatie
- Locatie van de leverancier, klant en/of service provider
- (semi-) Openbaar gebied
- Transport
- Gedurende werktijd
- Buiten werktijd
- Na een incident
- Gedurende een incident in de omgeving van het bedrijf
- Tijdens een onderhoud
- Tijdens de opstart en shutdown fase
- Tijdens een verhuizing
- Tijdens een staking

Bijlage 2: Incidentverloop vanuit daderperspectief

Bij de selectie van maatregelen is het van belang het door de dader gewenste verloop van het incident inzichtelijk te hebben. Vanuit de dader gezien kunnen de meeste incidenten in de hieronder genoemde fasen worden onderverdeeld. Het feitelijk getoonde gedrag van de dader is in elke fase sterk afhankelijk van het type dader, zijn doelstellingen, motivatie en hulpmiddelen, het doelwit en de omstandigheden waarbij het doelwit bereikbaar is.



Voorbereidingsfase

Bij een gelegenheidscrimineel of verwarde persoon kan de voorbereidingsfase zeer kort en een enkele maal ook ondoordacht zijn. De voorbereiding kan ook een langere periode zijn waarin de criminele actie doordacht wordt voorbereid. Een meer planmatige dader voert in meer of mindere mate de volgende activiteiten uit:

Selecteren van doelen

Op basis van algemeen beschikbare informatie, onder meer via het internet, selecteert de dader enkele potentiële doelen.

Voorverkennen potentiële doelen

In een algemene voorverkenning bouwt de dader een beeld op van de locatie en het niveau van de beveiliging. Op basis hiervan beslist de dader op welk specifiek doelwit hij zijn voorbereidende activiteiten richt.

Detail verkennen van doel

In deze fase wordt detailkennis opgedaan van het doelwit, de locatie en de beveiliging. Activiteiten kunnen zijn:

- Observatie van het doel vanaf de openbare weg of bereikbare locaties dichterbij het doelwit;
- Via social engineering toegangsprocedures omzeilen en daarmee het doelwit verder naderen of op een andere wijze informatie verzamelen over het doelwit en de beveiligingsmaatregelen;
- Via human engineering andere personen aanzetten om activiteiten uit te voeren die tot meer informatie leiden;
- In dienst treden bij het bedrijf om eenvoudiger toegang te krijgen tot het doelwit;
- Uitvoeren van een proefinbraak om de beveiligingsreactie van het bedrijf te testen.

Plannen van uitvoering

In deze subfase wordt de uitvoering operationeel voorbereid:

- Verzamelen van noodzakelijke hulpmiddelen;
- Verzamelen van identiteits- en toegangsmiddelen;
- Verzamelen van voertuigen om toegang tot het object te krijgen en/of te vluchten;
- Onklaar maken van beveiligingsmaatregelen. Dit gebeurt eventueel met handlangers binnen het bedrijf.

Als de dader van mening is voldoende voorbereid te zijn om toe te slaan, zal deze een moment en locatie kiezen om dat te doen.

Toegang verschaffen tot doelwit

De toegangsverschaffing markeert het operationele startpunt van de onbevoegde handeling. De dader breekt in deze fase door de toegangs- en beveiligingsschillen en komt bij het doelwit uit. Als er bouwkundige barrières zijn (target hardening) dan kost dat enige tijd om die te doorbreken[7]. Als de dader over efficiënte toegangsmiddelen beschikt, is de duur van de toegangsverschaffing fase aanzienlijk korter.

Uitvoeren van actie

In deze fase bevindt de dader zich bij het doelwit en zal hij zijn actie uitvoeren. Dat kan bijvoorbeeld het meenemen van de buit zijn, maar ook het saboteren en manipuleren van het doelwit. Deze fase duurt zo kort mogelijk voor de dader.

Enkele dadertypen zullen in deze fase brand stichten om de sporen te vernietigen. De bedrijfsbrand kan aanmerkelijk grotere gevolgen hebben dan de schade uit de directe actie van de dader (bijvoorbeeld diefstal van LCD-schermen). Er zijn ook dadertypen die op andere wijze de sporen van de actie maskeren om de actie, bijvoorbeeld fraude, herhaaldelijk uit te kunnen voeren of om te pakkans te verkleinen. ICT-aanvallers zullen mogelijkerwijs gebeurtenislogboeken aanpassen of zelfs hele computersystemen vernietigen om sporen te wissen.

Aftocht

Het merendeel van de daders heeft baat bij een veilige aftocht. Doordat er al een vrije weg is, kan de aftocht meestal nog sneller plaatsvinden dan de toegangsverschaffing. Soms heeft de dader voertuigen nodig om de buit af te voeren. Ook bij aanvallen via ICT-systemen, waarbij informatie wordt gestolen of gemanipuleerd, zal de buit op een bepaalde manier onopgemerkt bij de dader moeten aankomen, wil deze hiervan gebruik maken.

Genot van actie

In deze fase is de dader veilig weggekomen van de plaats van delict en kan hij genieten van de actie door bijvoorbeeld de buit door te verkopen aan een criminele handelspartner. Bij een actie/terroristische groep zal het veelal eerder gaan om het genieten van de publiciteit die ontstaat over de actiegroep en het bedrijf.

---

7 Het passeren van een standaard hekwerk kost 1 minuut. Het passeren van SKG** hang- en sluitwerk kost 3 minuten en het passeren van SKG*** hang- en sluitwerk kost 5 minuten. Voor ICT-systemen is het passeren van de toegangfunctie die over tokens of biometrie beschikt vele male malen moeilijker dan een toegang die alleen met een wachtwoord is afgeschermd.

Bijlage 3: Type maatregelen bij beveiligingsdoelen

Deze bijlage bevat voorbeelden van maatregelen die passen bij beveiligingsdoelen.

A Voorkomen dat gevoelige informatie in het publieke domein komt

Deze maatregelen hebben als doel te voorkomen dat een potentiële dader informatie over een doelwit of over beveiligingsmaatregelen via het publieke domein kan inwinnen. Zolang een potentiële dader niet weet dat er een doelwit is en waar dat doelwit zich bevindt, komt er ook geen aanval.

Typische maatregelen zijn:

- Niet publiceren van gevoelige informatie op websites, in jaarverslagen, interviews en artikelen;
- Geen vertrouwelijke zaken bespreken in een omgeving waar meegeluisterd kan worden;
- Niet laten rondslingeren van documenten en andere informatiedragers (bijvoorbeeld een USB-stick);
- Clean desk, clear screen;
- Zichtbeperkende maatregelen op gevoelige objecten;

Deze maatregelen hebben alleen effect bij potentiële daders die zich buiten de organisatie bevinden. Voor veel van deze maatregelen is een hoge mate van bewustzijn van het personeel ten aanzien van security noodzakelijk.

B Afschermen object en bemoeilijken verkenningsacties

Deze maatregelen hebben als doel de potentiële dader uit de buurt van het doelwit te houden en verkenningsacties te bemoeilijken.

Typische maatregelen zijn:

- Compartimentering, beperking van toegang tot de ruimte waar het object zich bevindt en het houden van toegangscontroles;
- Duidelijke functieaanduiding van ruimten en maatregelen die voorkomen dat een 'dwaalgedrag excuus' kan worden gebruikt;
- Toezicht en detectie van personen die bijzondere belangstelling voor het object ten toon spreiden en het aanspreken van deze personen met afwijkend gedrag;

Deze maatregelen kunnen ook nuttig zijn bij potentiële daders uit de eigen organisatie, tenminste als deze uit een organisatieonderdeel komen waarbij toegang tot de omgeving van het doelwit niet per se noodzakelijk is.

C Afschrikken en ontmoedigen van kwaadwillenden

Deze maatregelen hebben als doel de perceptie van de pakkans bij potentiële daders zodanig te vergroten dat zij afzien van uitvoering van de actie.

Typische maatregelen zijn:

- Inzichtelijk maken wat de beveiligingsmaatregelen zijn, een overzichtelijke omgeving, weghalen van verstopplaatsen, beperken van aantal vluchtwegen. Dit tonen van beheer en beveiliging wordt ook wel de security footprint genoemd;
- Toezicht houden op en detecteren van personen die bijzondere belangstelling voor het object hebben;
- Actief aanspreken van onbekende personen;
- Registratie door CCTV en toegangsverleningssystemen, die de traceerbaarheid vergroten van onbestemde aanwezigheid van eigen personeel;
- Schrikverlichting;
- Voorlichting geven aan medewerkers en op gevolgen van onbevoegd handelen wijzen;
- Opvragen van referenties bij nieuwe personeelsleden;
- (Disciplinaire) maatregelen ten aanzien van daders en verantwoordelijken voor een incident.

D Tegenhouden van de dader

Deze maatregelen hebben als doel een dader tegen te houden. Denk aan:

- Hekwerken en grachten;
- Voertuigwerende objecten zoals rampalen;
- Muren, deuren en gevelelementen;
- Kasten en kluizen;
- Afschermende voorzieningen tegen beschietingen;
- Firewalls, encryptie, autorisatieschema's en virusscanners;

De dader kan deze maatregelen doorbreken, maar zijn tijd en hulpmiddelen voor nodig.

E Detecteren van een (mogelijk) incident

Deze maatregelen hebben als doel om op het spoor van een mogelijk incident te komen, zodat een onderzoek kan worden opgestart en gecorrumpeerde beveiligingsmaatregelen kunnen worden hersteld.

Typische maatregelen zijn:

- Sociaal toezicht;
- Business assurance, toezicht op ordentelijk procesverloop en het controleren van de inventaris;
- Georganiseerd toezicht, inspecties, brand- en sluitronden en CCTV-toezicht;
- Digitale inspecties op gebruik en misbruik van toegang- en inbraaksystemen;
- Toegang- en inbraak systemen;
- Intrusion detection systemen in de ICT-configuratie;
- Audits.

F Detecteren, vertragen en interventie

Deze maatregelen hebben als doel een dader op tijd tegen te houden. Het is een samenhangend proces en beslaat de hieronder genoemde onderdelen.

1. Detecteren van een incident. Dit gebeurt door middel van elektronische beveiligingsmaatregelen of sociale oplettendheid.
2. Alarmmelding en organiseren van interventie. Het alarmsignaal moet bij een centraal meldpunt[8] binnenkomen, waar de melding beoordeeld kan worden en waar vandaan de interventie opgeroepen kan worden. Hiervoor zijn elektronische beveiligings- en communicatiemaatregelen en een afgestemde organisatie nodig.
3. Dader vertragen in het bereiken van zijn doel. Dit gebeurt onder meer door bouwkundige barrières.
4. Interventie plegen op de locatie en tegenhouden van dader. Dit gebeurt door medewerkers van het bedrijf, een beveiligingsbedrijf of de politie. De aard van de inzet is sterk afhankelijk van de informatiepositie die de meldkamer heeft over het incident.

De samenstelling van deze beveiligingsmaatregelen kan in een tijdspad worden geplaatst samen met die van het bedreigende incident. Dit maakt duidelijk op welk moment de interventie bij de dader kan zijn en of dit nog op tijd is. In sommige situaties is de beveiliging namelijk alleen effectief als de interventie plaatsvindt vóórdat de dader de plaats van het doelwit heeft bereikt. In andere situaties kan het nog effectief zijn als de interventie plaatsvindt in de periode dat de dader met de uitvoering van de daad actief is of vertrekt. De grootste preventieve werking heeft de beveiliging natuurlijk in die situatie dat de voorbereiding wordt opgemerkt en de dader wordt weerhouden om te starten met de uitvoering.

---

8 In de praktijk zal het bedrijf meestal meerdere 'centrale punten' inrichten die met elkaar verbonden zijn. Op fysieke meldingen kan dat een bedrijfsalarmcentrale of particuliere alarmcentrale zijn. Het meldpunt voor inbreuken op de informatievoorziening wordt ook wel security operations center genoemd. De interventie kan worden uitgevoerd door medewerkers van het bedrijf, beveiligers of politie. De interventie op digitale aanvallen kan door computer emergency response team worden uitgevoerd.

G Consequenties verminderen

Het lukt niet altijd de actie van de dader te voorkomen. In dat geval moeten maatregelen genomen worden om de gevolgen van die moedwillige acties te verkleinen. Het is enigszins een definitiekwestie of dit echte security maatregelen zijn. De aard van de maatregelen vraagt vaak om direct handelen tijdens het incident. Daarbij hebben personen uit de organisatie van beveiliging op dat moment een actieve rol.

Maatregelen zijn onder meer:

- Verminderen van de waarde van de buit na het incident, bijvoorbeeld vervoer van geld in een plofverfkoffer;
- Ontruiming van een gebouw bij brand;
- Eerste brandbestrijding, gebruik van kleine blusmiddelen;
- Waarschuwen van de proces-control van de onderneming met goede informatie over het incident, zodat het bedrijfsproces kan worden bijgestuurd;
- ICT-systemen (tijdelijk) offline zetten.

H Registratie van procesuitvoering (safe guarding)

Het vastleggen van de procesuitvoering heeft als doel de juistheid van de uitvoering van het proces aan te tonen en onregelmatigheden te kunnen onderzoeken. Daarmee wordt achteraf:

- Aantoonbaar gemaakt dat een procedure op integere wijze is uitgevoerd;
- Aantoonbaar gemaakt waar een procedure gefaald heeft;
- Duidelijk gemaakt wanneer en waar een dader in de fout is gegaan en tevens wordt bewijslast verzameld;
- Inzicht in de werkelijke uitvoering van het proces opgebouwd dat bruikbaar is om een chantagedreiging te beoordelen.

Maatregelen zijn onder meer:

- Registratie (bijvoorbeeld met CCTV) van belangrijke processtappen en overdrachtsmomenten;
- Registratie van toegangverlening;
- Registratie van telefoongesprekken met de meldkamer;
- Registratie van computernetwerkverkeer en gebeurtenissen op ICT-systemen.

Bijlage 4: Beveiligingssituaties

Naast generieke beveiligingsprincipes en –maatregelen zijn er ook beveiligingsprincipes die voornamelijk bruikbaar zijn in bepaalde bedrijfssituaties. Bij het ontwikkelen van een OSP is het daarom zaak vast te stellen wat voor type situaties voorkomen. Omdat het maatregelenpakket en sturing op beveiliging verschillen, zal dit vaak ook terugkomen in de opbouw van het OSP of OSP's. Enkele beveiligingssituaties die relevant kunnen zijn voor een operator:

Beveiliging van een door de operator gecontroleerde fysieke locatie
In deze situatie heeft de operator zelf de compartimentering en toegangsregulering in de hand.

Locatiebeveiliging binnen een (semi-) openbaar gebied
Het beschermen van bedrijfsmiddelen en -processen in (semi-) publiek toegankelijk gebied heeft een eigen dynamiek. In deze situaties dient de beveiliging ook elementen te bevatten uit een gebiedsaanpak op beveiliging, waarbij wordt samengewerkt met de andere gebruikers van de ruimte, de politie en de gemeente.

Beveiliging van het bedrijfsproces
Een bedrijfsproces is een gestructureerde stroom van activiteiten. De activiteiten zelf en de bedrijfsmiddelen die daarvoor nodig zijn, worden vaak uitgevoerd op fysieke locaties die de operator met locatiebeveiliging kan beschermen. De producten- en dienstenstroom verplaatst zich van locatie naar locatie. Bedrijfsprocesbeveiliging stuurt vooral op de processtroom en overdrachtsmomenten in het proces.
Met een afhankelijkheidsanalyse kan worden onderzocht in welke mate het primaire bedrijfsproces afhankelijk is van secundaire bedrijfsprocessen en externe input. Ook deze processen verdienen beveiligingszorg.

Beveiliging van de supply chain
Sturing en beveiliging van de supply chain zijn vergelijkbaar met die van het bedrijfsproces. Groot verschil is de verscheidenheid van externe partijen in de stroom. Bovendien wordt de sturing op de supply chain meestal niet door de operator zelf uitgevoerd.

Beveiliging van vervoersstromen
Bij vervoersstromen gaat het om dynamische objecten die zich op ongecontroleerd en potentieel onveilig gebied kunnen bevinden. In veel situaties wordt het vervoer uitgevoerd door andere parijen dan de operator.

Beveiliging van informatie, communicatie, ICT-middelen en bedrijfsvoeringsystemen
Informatie, communicatie en ICT-middelen vormen essentiële beschermingswaardige bedrijfsmiddelen. Enkele verschijningsvormen zijn:
- Fysieke documenten;
- Digitale documenten zoals een website of een lichtkrant;
- Gegevensdragers, applicaties en ICT-middelen;
- Gesprekken, lezingen, presentaties en conferenties;
- Communicatiemiddelen en communicatiekanalen en –dragers;
- Bedrijfsvoeringsystemen, databases, email en ERP;
- Proces control systemen (SCADA).

Beveiliging van personen
Het beveiligen van personen kan in verschillende situaties noodzakelijk zijn. Deze personen kunnen op een bepaalde locatie gestationeerd zijn of juist mobiel zijn.

Dynamische beveiligingsniveaus bij verhoogde dreiging

Het is een goed gebruik om naast een vast beveiligingsniveau ook tijdelijke zwaardere beveiligingsniveaus te kunnen inzetten bij hogere dreiging. Het Alerteringssysteem Terrorismebestrijding (ATb) gebruikt ook deze aanpak en hanteert drie hogere beveiligingsniveaus ten opzichte van een basisniveau.

0. Basisniveau
1. Lichte dreiging
2. Matige dreiging
3. Hoge dreiging

Het OSP bevat de systematiek van deze vier beveiligingsniveaus. Ook voor bedrijven en sectoren die niet zijn aangesloten op het ATb is het raadzaam om deze systematiek in te voeren, zodat bij verhoogde dreiging eenduidiger met publieke veiligheidpartijen gecommuniceerd kan worden.

Het bepalen van de verschillende soorten maatregelen per dreigingsniveau is maatwerk. Ter ondersteuning bij het afstemmen van de beveiligingsmaatregelen in verschillende dreigingsniveaus heeft het NAVI de handreiking Beveiligingsafstemming Vitaal en Overheid (BAVO) opgesteld. Hierin wordt beschreven hoe bedrijven uit de vitale sectoren samen met de lokale en regionale overheidspartners afspraken kunnen maken over de afstemming van de (opgeschaalde) beveiligingsmaatregelen en de reactie op incidenten. De handreiking behandelt verschillende soorten dreigingen. U kunt deze handreiking downloaden op de website van het NAVI: www.navi-online.nl

Beveiliging tijdens en na een calamiteit

In het OSP kunnen ook de beveiligingssituaties benoemd worden die van toepassing zijn tijdens en na een calamiteit bij het bedrijf. Denk hierbij aan:

- Begeleidings- en toegangverlening van hulpdiensten tijdens een calamiteit;
- Beveiliging van terrein en goederen als beveiligingsvoorzieningen niet meer functioneren. Bijvoorbeeld:
    - Niet meer functionerende toegangsschil;
    - Uitval van elektriciteit;
    - Uitval of corruptie van communicatiemiddelen;
    - Uitval van security systemen;
    - Uitval van bewakers.
- De situatie als gevolg van incident of ramp in de omgeving van het bedrijf met bijvoorbeeld rookontwikkeling of een wegblokkade;
- Het beveiligen van het bedrijf na evacuatie van gebied door bijvoorbeeld brand in de omgeving of een potentiele dijkdoorbraak;
- Beveiliging tegen fysieke media-aandacht van crisiscentrum en/of de mediaruimte, eventueel de woning van de directeur;
- Beveiliging van de uitwijklocatie van de bedrijfsvoering.

Beveiliging van bijzondere bedrijfsvoering situaties

Het OSP kan ook ingaan op de noodzakelijke maatregelen bij bijzondere Bedrijfsvoeringsituaties. Bijvoorbeeld:

- Opstart en shutdown van bepaalde bedrijfsprocessen;
- Onderhoudsfase (veel personen op het terrein);
- Verhuizingen;
- Stakingen;
- Open dagen en andere evenementen waarbij veel personen op het terrein aanwezig zijn.

Bijlage 5: Beveiligingsmaatregelen

In deze bijlage worden enkele beveiligingsmaatregelen benoemd. Het is niet mogelijk volledig te zijn in het beschrijven van alle maatregelen. Hiervoor is het aantal verschillende maatregelen te groot en dit aantal stijgt exponentieel als maatregelen ook in combinaties worden beschouwd. In het stappenplan wordt zo'n combinatie een maatregelenpakket genoemd, dat beveiligingsdoelen heeft en zorgt voor een bepaalde mate van risicovermindering. De meeste maatregelen zijn afhankelijk van de context, van het te beschermen belang, van het type bedreigingen, locaties en bedrijfsvoeringsituaties die voorkomen.

Er bestaat tal van indelingen op maatregelen. Bekende indelingen zijn ondermeer:

- Naar de aard van de maatregel:
  - Organisatorisch, fysiek, ICT, personeel
  - Organisatorisch, bouwkundig, elektronisch (OBE)
- Naar het type dreiging:
  - Inbraakbeveiliging
  - Antiterrorisme
  - Contraspionage
  - Brandbeveiliging
  - Fraudebestrijding
  - Anti-virus beveiliging
  - Vandalisme bestendig
- Naar het te beveiligen belang of object:
  - Beveiliging van supply chain
  - Beveiliging van informatie
  - Beveiliging van personen
  - Beveiliging van de vitale infrastructuur
- Naar de positie in de veiligheidsketen
  - Pro-actie
  - Preventie
  - Preparatie
  - Repressie
  - Nazorg en herstel
- Naar niveau van beveiliging gerelateerd aan het ATb
  - Basisniveau
  - Lichte dreiging
  - Matige dreiging
  - Hoge dreiging
- Naar routinematig optreden van security en niet-routinematig optreden
- Naar wie de maatregelen uitvoert of beheert:
  - Verschillende functiegebieden/afdelingen binnen de eigen organisatie (HRM, ICT)
  - Externe partijen (externe beveiligers, leveranciers)
  - Publieke veiligheidspartijen (politie, brandweer)

Het gebruik van één of meerdere indelingen is geen op zichzelf staand doel, maar kan nuttig zijn in de communicatie met de verschillende doelgroepen in de beveiliging. In deze bijlage worden maatregelen in de volgende groepen geplaatst:

1. Afschermende maatregelen
2. Toegangverlenende maatregelen
3. Maatregelen op zichtbaarheid, toezicht en detectie
4. Maatregelen op alarmbehandeling en interventie
5. Maatregelen op personen

1. Afschermende maatregelen

Afschermende maatregelen hebben als doel de te beschermen belangen in enige mate af te schermen tegen potentiële dreigingen. Hier kan ondermeer het volgende type maatregelen onder worden verstaan:

- Compartimentering/zonering concept
- Gebruiksgebonden/organisatorische zonering
- Terreingebonden compartiment begrenzing
- Gebouwgebonden compartiment begrenzing
- Bemoeilijken van beschieten
- Meeneem beperkende maatregelen
- Weghalen van criminele hulpmiddelen
- Zichtbeperkende maatregelen
- Meeluister beperkende maatregelen

Compartimentering (zonering) en dieptebeveiliging

Compartimenteren is een van de belangrijkste beveiligingsmaatregelen. Een andere benaming is zoneren. Met compartimenteren worden bedrijfsfuncties met gelijke gewenste gebruikers geografisch gegroepeerd en afgeschermd van ongewenste gebruikers van de ruimte. De compartimentbegrenzing kan verschillende vormen hebben.

Relatie met toegangverlening en gebruikslogistiek

Aan compartimentering is altijd een vorm van toegangscontrole verbonden om toegang te verlenen aan de gewenste gebruikers en toegang te weigeren aan de ongewenste gebruikers. Deze toegangverlening is sterk gekoppeld aan de gebruikslogistiek van de ruimte. Het is daarom van belang om in een zo vroeg mogelijk stadium in het ontwerp van een locatie de gebruikslogistiek en de toegangslogistiek op elkaar af te stemmen.

Buitenschil beveiliging

In talrijke situaties komt alleen buitenschil beveiliging voor. Kwaadwillende personen, die als gewenste gebruiker tot het compartiment zijn toegelaten of op een andere wijze de toegangscontrole hebben omzeild, hebben daarna vrije toegang tot alle locaties binnen deze buitenschil. Om dit te voorkomen kan het wenselijk zijn ook compartimenten binnen de buitenschil te definiëren.

Dieptebeveiliging en toegangverlening

Met dieptebeveiliging liggen de compartimenten binnen elkaar. Iedere compartimentbegrenzing en toegangscontrole zorgt ervoor dat bepaalde type ongewenste gebruikers van de ruimte buiten worden gehouden en een kleinere groep van gewenste gebruikers toegang krijgt.

Een voorbeeld van een zonering- en toegangconcept is:

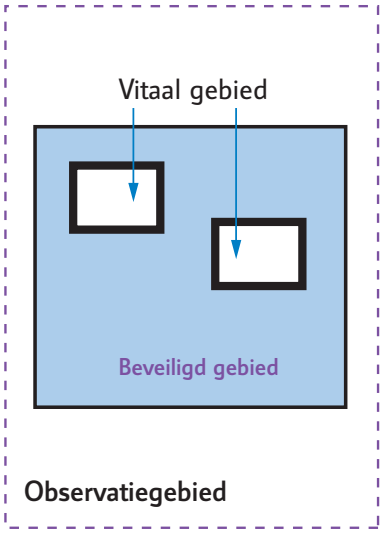
Zone	**Gewenste gebruikers**	**Maatregelen**
Omliggend industrieterrein	Bezoekers, medewerkers, leveranciers van bedrijven op industrieterrein	– Beperking aantal toegangen tot industrieterrein – CCTV-toezicht op toegang en tactische knooppunten – Overzichtelijke indeling – Snelle interventie door beveiligingsbedrijf die verdachte personen aanspreekt
Parkeerterrein bedrijf	Alle medewerkers en bezoekers van bedrijf	– Overzichtelijke indeling – Heldere borden met gebod/verbod/bewegwijzering – Toezicht vanuit bedrijf, eventueel via CCTV en handelend optreden bij verdachte personen en ongewenst gedrag
Ontvangstgedeelte bezoekers Spreekkamers om bezoekers te ontvangen	Alle medewerkers, bezoekers	– Toegangscontrole bezoekers door portier – Toegangscontrole medewerkers via toegangspas
Algemene gedeelten van het bedrijf (restaurant, verkeersruimte)	Alle medewerkers, beperkte groep van bezoekers	– Toegangscontrole medewerkers via toegangspas – Toegangscontrole bezoekers door portier. Daarna begeleiding door gastheer/medewerker.
Afdelingen	Medewerkers van de betreffende afdeling, beperkte groep van bezoekers	– Toegangscontrole medewerkers via toegangspas – Bezoekers via begeleiding door gastheer/medewerker
Vitale locaties (bijvoorbeeld control room)	Beperkte groep van medewerkers van de betreffende afdeling	– Toegangscontrole medewerkers via toegangspas. Eventueel verificatie van toegangsgebruik via CCTV.

Dieptebeveiliging, braakwerendheid en detectie

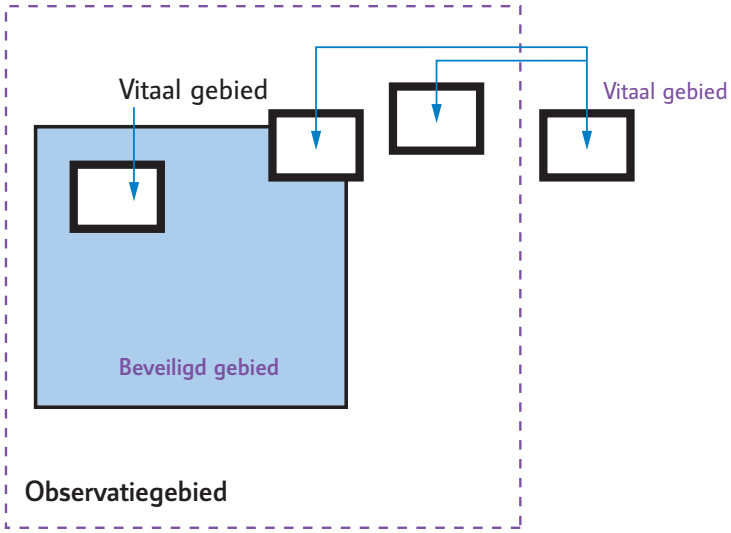
Wanneer een kwaadwillende persoon niet via de reguliere toegangsmogelijkheden toegang krijgt tot de locatie van zijn doelwit, zal deze de compartimentbegrenzingen op andere plekken doorbreken. De compartimentgrens heeft een bepaalde mate van braakwerendheid. Afhankelijk van de hulpmiddelen van de kwaadwillende zal de compartimentgrens enige tijd weerstand bieden voordat deze doorbroken is. Indien dieptebeveiliging wordt toegepast, zal daarna de dader op een volgende barrière stuiten. Wanneer de indringer vroegtijdig wordt gedetecteerd kan de interventie op tijd aanwezig zijn voordat de dader de vitale locatie bereikt.

Door het hanteren van een dieptebeveiligingsconcept wordt bereikt dat:

- indringers zo vroeg mogelijk worden gedetecteerd en interventie kan worden georganiseerd, terwijl opeenvolgende compartimentschillen de indringer tegenhouden;
- de vitale compartimenten zo klein mogelijk worden gehouden;
- de meest kostenefficiënte inzet van kostbare bouwkundige- en elektronische beveiligingsmaatregelen ontstaat. Alleen voor de meest vitale bedrijfsbelangen worden de meest kostbare maatregelen ingezet.



Vitale gebieden binnen concept van dieptebeveiliging geplaatst



In praktijk wordt dieptebeveiliging niet altijd toegepast

Gebruiksgebonden en organisatorische compartiment begrenzing

Ook met organisatorische maatregelen en 'aanwijzingen' vanuit de bebouwde omgeving is het mogelijk om compartimenten te definiëren en te begrenzen zonder gebruik te maken van moeilijk doordringbare grenzen. Doel van deze maatregelen is om het gewenste gedrag van de gebruikers van de ruimte te sturen en kwaadwillenden geen excuus te geven om te verdwalen. Indien een kwaadwillende persoon zich van de maatregelen niets aantrekt, valt dat op en kan interventie worden gepleegd door deze hierop aan te spreken.

Type maatregelen zijn:

- Duidelijke afspraken
- Verboden toegang borden
- Gebod borden
- Heldere toegangsroutes en richtingborden
- Bestrating, verlichting, kleurgebruik om gewenst ruimtegebruik aan te geven
- Lage hekken, muurtjes en heggen om grenzen aan te geven
- Beperken van toegangen
- Goed zicht op de locatie vanuit omliggende ruimtes
- Sociaal toezicht door gebruikers van de ruimte. Deze gebruikers dienen zich 'eigenaar' van de ruimte te voelen en ongewenste gebruikers van de ruimte aan te spreken

Harde terreingebonden compartiment begrenzing

Voor gesloten terreincompartimenten zijn verschillende mogelijkheden, onder meer:

- Hekwerken
- Muren
- Grachten
- Wallen
- Plantenbakken
- Palen

Sommige maatregelen hebben als doel om personen buiten een gebied te houden. Andere barrières zijn gericht om ramvoertuigen en voertuigen met explosieven uit de buurt van gevels te houden. Daarnaast kunnen er maatregelen in de periferie worden genomen om het afvoeren van de buit met een voertuig te bemoeilijken.

Gebouwgebonden compartiment begrenzing

Harde grenzen van gebouwcompartimenten worden onder meer gedefinieerd door:

- Muren
- Gevelopeningen
  - Vensters, luiken
  - Glas
  - Kozijnen, hang- en sluitwerk
  - Deuren
  - Rolluiken, tralies
- Opbergmiddelen
- Kluizen (braakwerend, brandwerend)

Ook hier zal vastgesteld moeten worden wat de weerstand moet zijn op bijvoorbeeld braak, rammen, beschieten, explosieven en het binnendringen van water, gassen en brandbare vloeistoffen.

Bemoeilijken van beschieten

Het bemoeilijken van beschieten kan onder meer bereikt worden door:

- Het plaatsen van vitale functies aan gebouwzijde waar geen zicht en schietlijn is vanaf semi-openbaar gebied;
- Het aanbrengen van andere maatregelen die het zicht ontnemen, bijvoorbeeld gordijnen;
- Barrières om beschietingen op het doelwit te bemoeilijken (wallen, muren, begroeiing);
- Locaties die zicht en schietlijn hebben op doelwit alleen bestemmen voor bedrijfsfuncties met een gecontroleerde toegang.

Meeneem beperkende maatregelen op artikelen

Voorbeelden van meeneem beperkende maatregelen:

- Vastzetten cq. verankeren van een artikel;
- Ophijsen, buiten bereik plaatsen van een artikel;
- Toepassen van elektronische detectie op een artikel die reageert wanneer het artikel wordt bewogen of buiten een ruimte wordt gebracht;
- Verminderen van de buit voor de dader (bijvoorbeeld door de plofkoffer in het geldtransport of bij het merken van het artikel).

Weghalen van criminele hulpmiddelen

Weghalen en/of vastzetten van mogelijke hulpmiddelen die de dader kan gebruiken bij de uitvoering van zijn actie, onder meer:

- Overklimmogelijkheden bij hekwerken (o.m. bomen en takken, stapels pallets en andere objecten die tegen het hekwerk geplaatst zijn);
- Ladders, waarmee hoger gelegen en minder zwaar beveiligde gebouwgedeelten kunnen worden bereikt;
- Bootjes, waarmee water kan worden overgestoken;

- Voertuigen, die als crimineel object kunnen worden gebruikt;
- Kranen en andere bedrijfsobjecten, waarmee schade kan worden veroorzaakt;
- Stoelen, tafels, computers en andere losse voorwerpen in een ruimte die bij agressie kunnen worden gebruikt.

Zichtbeperkende maatregelen

Zichtbeperkende maatregelen bemoeilijken het de dader om informatie te krijgen over het object. Maatregelen zijn onder meer:

- Het plaatsen van kritische functies aan de gebouwzijde waar geen zicht is vanaf de openbare weg;
- Een fotografeerverbod;
- Geen borden plaatsen waar de functie van de ruimte op wordt verduidelijkt;
- Voorkomen dat via afvalstroom (bv. verpakkingsdozen met opdruk) duidelijk wordt dat attractieve goederen aanwezig zijn;
- Het bevestigen van gordijnen;
- De manier van de inrichting van de ruimte. Geen zicht op beeldschermen en op wandplaten waar mogelijk vertrouwelijke informatie op staat;
- Een Clean desk;
- Een Clear screen;

Meeluisterbeperkende maatregelen

Meeluisterbeperkende maatregelen zijn onder meer:

- Speciale ruimtes waar in vertrouwelijkheid gesproken kan worden;
- Bewustzijn bij medewerkers om alleen in besloten kring over vertrouwelijke zaken te spreken;
- Eventueel specifieke en gecontroleerde omgeving ten behoeve van het voeren van vertrouwelijke gesprekken. Deze omgeving regelmatig controleren op aanwezigheid van meeluisterende voorzieningen (sweepen). Opname apparatuur (mobiele telefoons e.d.) weren uit deze ruimte.

2. Toegangverlenende maatregelen

De toegangverlenende maatregelen hebben als doel om in het bedrijfsproces gewenste gebruikers toegang te verlenen en ongewenste personen de toegang te weigeren. De regels en de organisatie hiervan worden in een toegangsplan en toegangsbeleid vastgelegd, vastgesteld en bewaakt.

Bij het opstellen van toegangverlenende maatregelen gelden de volgende principes:

- Beperken van het aantal toegangen vergroot de effectiviteit van toegangscontrole en verkleint de vluchtmogelijkheden voor daders;
- Bij de toegangverlening tot compartimenten van eenzelfde type dient dezelfde toegangscontrole te worden gebruikt. Als gekozen wordt voor elektronische en traceerbare toegangverlening, dan moet dat plaatsvinden op alle toegangen tot dit compartiment.;
- Naast toegangsroutes en toegangsdeuren voor normaal gebruik kunnen er ten behoeve van calamiteiten ook specifieke vluchtroutes, vluchtdeuren, hulpverleningsroutes en hulpverleningstoegangen zijn gedefinieerd. Deze vluchtroutes en vluchtdeuren moeten ook als zodanig herkenbaar zijn. Wanneer deze niet dezelfde zijn als de toegangsdeuren moeten maatregelen getroffen worden om oneigenlijk gebruik te voorkomen;
- Het gebruik van sterke toegangsrechten en -middelen moet worden beperkt. Een sterk toegangsmiddel is onder meer een generale hoofdsleutel, een toegangspas met rechten tot alle ruimtes of een digitaal toegangsrecht tot alle ICT-middelen, applicaties en bestanden. Naast beperking van het aantal personen dat dit recht heeft, kan ook worden gedacht aan mechanismen die het gebruik traceerbaar maken en verantwoording afleggen voor dit gebruik;
- De toegangsmiddelen moeten zijn afgestemd op het type te reguleren toegang bijvoorbeeld door middel van een poort, deur, tourniquet, slagboom, sluis of een roadblocker.

Toegangscontrole via mechanische middelen (sleutel)
De toegangscontrole kan plaatsvinden via een slot met mechanische sleutel. In het sleutelplan is vastgelegd wat de sleutelrechten zijn ten opzichte van de ruimtes. In het sleutelbeheer ligt vast welke personen sleutels hebben.

Toegangscontrole via toegangapplicatie en toegangspas
De toegangscontrole kan ook via een toegangapplicatie plaatsvinden. De identificatie van de gebruiker vindt dan plaats via een toegangspas met kaartlezer en mogelijk biometrische kenmerken. In deze applicatie kunnen regels worden gedefinieerd wie waar en wanneer toegangsrechten heeft. Het gebruik van de toegangspas kan worden geregistreerd waardoor een grotere traceerbaarheid ontstaat. Dit verkleint de kans op 'dwalen' van een persoon die op zichzelf toegangsrechten heeft, maar op dat moment niets te zoeken heeft op een locatie.
Het gebruik van software biedt ook mogelijkheden om andere regels te definiëren op rechten die personen hebben. Denk aan:
- Rechten om de inbraakdetectie in- of uit te schakelen;
- Toegangsrechten tot een ICT-applicatie met voorwaarde dat de persoon zich ook in die ruimte moet bevinden;
- Toegangsrecht tot een ruimte of apparaat dat alleen bestaat in gezamenlijkheid met een andere persoon.

Toegangscontrole via toegangspersoneel
De toegangverlening en –controle kan ook door receptiemedewerkers of bewakingspersoneel worden uitgevoerd. Eventueel kan dit ook op afstand plaatsvinden, waarbij dan ook middelen als intercom, CCTV, verlichting en poortbediening aanwezig moeten zijn.
Bij de inzet van toegangspersoneel moeten ook procedures bestaan op het vooraankondigen van het bezoek, ID-verificatie, bezoekersregistratie en het oproepen van de gastheer.

Toegangscontrole via sociale maatregelen
Het aansturen op sociale controle is in veel situaties een krachtig middel. Daarbij wordt verwacht dat legitieme gebruikers van de ruimte personen aanspreken die niet in die ruimte verwacht worden. Een hulpmiddel hierbij kan de badgeplicht zijn, waarbij via de badge zichtbaar is wat de status is van een persoon (bijvoorbeeld vaste medewerker, tijdelijke medewerker, leverancier of bezoeker etcetera). Dit zal overigens alleen werken als het management een voorbeeldfunctie heeft.
Andere sociale regels zijn:
- Niet binnenlaten of mee laten lopen van personen waarvan het onduidelijk is of deze toegangrechten hebben;
- Gesloten houden van toegangsdeuren en vluchtdeuren;
- Begeleiden van bezoekers (ophalen, wegbrengen).

Screening van voertuigen, bagage, artikelen
Naast toegangscontrole voor personen kan het ook wenseliik zijn toegangscontrole toe te passen voor voertuigen, bagage en artikelen. Afhankelijk van het doel dient de controle op ongeoorloofde zaken bij binnenkomst dan wel bij vertrek plaats te vinden.
De hulpmiddelen voor de controle zijn afhankelijk van het type onderzoek, bijvoorbeeld wapendetectie. Als er kans bestaat op ploffen of biochemische uitspattingen dan moet de screening aan de buitenrand van het complex plaatsvinden. Overige bedrijfsprocessen worden dan niet gefrustreerd bij een incident. Dit principe is onder meer van belang voor de lokalisering van de postkamer.

Toepassing toegangsregels buiten het fysieke domein
De toegangsregels gelden niet alleen voor fysieke toegang, maar ook op de toegang tot ICT-devices, applicaties en gegevens en kunnen ook gelden voor de toegangsrechten op voertuigen, vaartuigen en andere bijzondere bedrijfsvoeringapparatuur.

Actuele vastlegging van rechten

Het moet altijd helder zijn wie waar rechten toe heeft. Deze rechten dienen systematisch te worden vastgelegd en zowel voor gebruiker als controlerende partij helder te zijn.

Toegangsbeleid

Het geheel aan uitgangspunten, procedures en organisatie kan worden vastgelegd in een toegangsbeleid.

3. Zichtbaarheid, toezicht en detectie

Wanneer in bedrijven te weinig aandacht wordt besteed aan toezicht en detectie kunnen in de praktijk de volgende ongewenste situaties voorkomen:

- Het incident wordt niet geconstateerd en het is voor de dader mogelijk om herhaaldelijk het incident te veroorzaken;
- Het incident wordt pas achteraf geconstateerd, nadat de dader zijn activiteit volledig heeft uitgevoerd en is vertrokken;
- Het incident wordt wel geconstateerd, maar er wordt geen alarmmelding gemaakt;
- Het incident wordt wel geconstateerd, maar de reactie duurt te lang om de dader te keren en te voorkomen dat de schade wordt aangebracht.

In deze paragraaf worden enkele type maatregelen benoemd om het detecterende vermogen te vergroten.

Overzicht en zichtbaarheid

Het creëren van overzicht en zichtbaarheid heeft verschillende doelen:

- Visueel zicht krijgen op de activiteiten;
- Potentiële dader uit de anonimiteit halen en daarmee afschrikken;
- Gewenste gebruiker een veilig gevoel geven.

Overzicht en zichtbaarheid wordt bereikt door:

- Overzichtelijk terrein, zonder verstopplaatsen;
- Zicht vanaf openbare weg tot aan gevels;
- Verlichting zoals permanente verlichting, veiligheidsverlichting, schrikverlichting, geleide verlichting (verlichting om interventie te geleiden naar locatie van alarmmelding);
- Bewegwijzering;
- Tonen van beveiligingsmaatregelen (camera's);
- Zichtbaar (beveiligings)personeel dat toezicht houdt;
- Werknemers in bedrijfskleding;
- Badges.

Detectiesystemen

Er zijn vele soorten detectiesystemen voor toepassingen op ondermeer de periferie, gebouw, artikel, ICT en procesniveau. Sommige detecties zullen direct een actieve interventie moeten opstarten op de dreiging. Andere detecties zijn een reden om een onderzoek te starten. Een voorbeeld van dit laatste is het ontdekken dat herhaaldelijk een onbevoegde toegangspas aan een kaartlezer wordt aangeboden.

Volg- en vastleggingsystemen (safeguarding)

Met safeguarding wordt hier verstaan het digitaal vastleggen van de procesvoering of uitvoering van de beveiliging om achteraf aantoonbaar te hebben dat de procesgang correct is verlopen, dan wel inzicht te krijgen in een afwijkend verloop van de procesgang. Hieronder kan ondermeer worden verstaan:

- Track & trace: het volgen van de positie van een artikel/voertuig/persoon en mogelijk in actie komen wanneer deze zich buiten het gewenste gebied gaat bevinden;
- Vastleggen van belangrijke transacties en overdrachten, waardoor het helder is tot waar de procesgang correct is verlopen;
- Vastleggen van camera beelden, waardoor het helder is tot waar de situatie normaal is verlopen en wat er daarna is gebeurd;
- Vastleggen van communicatie van en/of naar meldkamer waardoor het achteraf duidelijk is hoe de alarmbehandeling is uitgevoerd.

Sociaal toezicht

Bewustwording bij gebruikers van de ruimte om op ongewone zaken te letten en bij detectie een meldpunt te alarmeren. Gebruikers kunnen zijn:

- Medewerkers
- Andere gebruikers van de ruimte
- Buren

Als van sociaal toezicht gebruik gemaakt wordt is het belangrijk om betrokkenheid met deze personen te creëren, een meldpunt te communiceren en eventueel uitleg te geven waarop gelet kan worden.

Georganiseerd toezicht

Er zijn verschillende vormen waarin georganiseerd toezicht kan voorkomen. Denk aan:

- Toezichthouders/beveiligers;
- Toezicht op afstand via CCTV;
- Brand en sluitronden;
- Inspectie ronden;
- Ook in toezicht vanuit andere meldpunten zoals 'Beheer toegangsrechten', 'ICT-helpdesk', 'Facilitair meldpunt' of 'Gebouw, terrein en installatiebeheer' kunnen onregelmatigheden naar boven komen. In deze meldpunten moet het helder zijn wat aanwijzingen zijn voor een mogelijk security incident.

Kwaliteitscontrole, verlies preventie en business assurance

Het helder organiseren van de bedrijfsprocessen en het aantoonbaar toezien dat deze volgens plan worden uitgevoerd, heeft als neveneffect dat in een vroeg stadium signalen ontstaan op mogelijk ontvreemde dan wel gemanipuleerde producten of diensten.

Door regelmatige controles uit te voeren op de inventaris, wordt inzicht verkregen of materialen worden ontvreemd of worden gebruikt voor andere doeleinden. Voorwaarde hiervoor is dat de goederen en inventaris geregistreerd zijn. Ook het periodiek controleren van de kwaliteit van de producten kan aan het licht brengen of deze producten gemanipuleerd worden. Vermissing van een product en/of aantasting van de kwaliteit kan een teken zijn van een beveiligingsincident en zal hierop onderzocht moeten worden.

4. Alarmering en interventie

Het alarmering- en interventieproces bestaat in grote lijnen uit de volgende onderdelen:

- Detectie en alarmoproep;
- Alarmontvangst, -beoordeling en opstarten interventie;
- Interventie zelf die kan bestaan uit:
  - Tegenhouden van dader;
  - Bestrijden van de gevolgen van de daad en beperken van schade;
  - Onderzoek.

De uitvoering hiervan is afhankelijk van de beschikbaarheid van:
- Communicatiemiddelen
- Procedures
- Nazorgactiviteiten

Detectie en alarmoproep

De detectie van een ongewenste situatie en de alarmoproep kan plaatsvinden vanuit verschillende bronnen. Deze moeten gedefinieerd worden met de passende procedures en communicatiemiddelen.

1. Alarmoproep door personen
   Medewerkers, partners en buitenstaanders kunnen een ongewenste situatie ontdekken en een alarmoproep doen. Dit kan gebeuren via de telefoon, andere communicatienetwerken of een noodknop.
2. Alarmoproep door systemen
   Beveiligingsystemen kunnen een afwijkende situatie detecteren en een alarmoproep doen.
3. Alarmoproep door andere beheerprocessen
   Beheerprocessen zoals 'Beheer toegangsrechten', 'Facilitair meldpunt', 'ICT-helpdesk', 'Gebouw-, terrein- en installatiebeheer' en 'Personeelzaken' kunnen een mogelijk beveiligingsincident detecteren en melden.

Alarmontvangst, -beoordeling en opstarten van interventie

Voor de alarmontvangst, -beoordeling en het opstarten van de interventie, moet een meldpunt worden ingericht. Dit kan een bedrijfsalarmcentrale zijn, een particuliere alarmcentrale of een ander type meldkamer. Dit meldpunt kan zodanig zijn ingericht, dat het alleen een doorgeefluik is van de meldingen naar een persoon die beslist welke interventie wordt uitgevoerd. Het meldpunt kan ook zelf een veel grotere regievoerende rol hebben als het meldpunt beschikt over kennis van de organisatie en een goede informatiepositie heeft over het incident. Deze informatiepositie is van cruciaal belang om snel de juiste interventie te kunnen plegen en te schalen in de bestrijding.
Bij onvoldoende informatie over het incident moet eerst verificatie worden uitgevoerd door een beveiligingsbedrijf of een medewerker van het bedrijf. Andere mogelijkheden om het alarmbericht te verifiëren en een beter beeld te krijgen van het incidentverloop zijn ooggetuigenberichten, cameratoezicht op het incident en combinaties van verschillende detecties.
Voor de inrichting van het meldpunt is het van belang dat de alarmcentrale:
- 24 uur per dag bereikbaar is;
- Communicatievoorzieningen en informatiefuncties zijn ingericht;
- De bemensing, zowel qua competenties als in kwantiteit toereikend is;
- Instructies helder zijn;
- Inrichting van het meldpunt, inclusief de beveiliging van het meldpunt adequaat is.

Sommige organisaties kiezen ervoor om door dit 24-uurs meldpunt ook andere diensten uit te laten voeren. Denk hierbij aan toegangverlening of toezicht op afstand.

Interventie

Interventie kan bestaan uit:

1. Tegenhouden van de dader
   Hiermee wordt bereikt dat het security incident geen effecten heeft voor de bedrijfsvoering.
2. Bestrijden van de gevolgen van de daad en beperken van schade
   Als de dader niet op tijd is tegengehouden, zal de security-aanval waarschijnlijk effect hebben op de bedrijfsvoering. Denk aan brand, een bommelding of een geslaagde sabotage. De handelswijze in de bestrijding en gevolgschade beperking liggen vast in het noodplan. Security heeft hierin een ondersteunende functie.
3. Doen van onderzoek
   Er zijn verschillende momenten dat een vorm van onderzoek plaats moet vinden. Denk bijvoorbeeld aan een verificatie van een alarmmelding, een onderzoek naar de oorzaak en modus operandi bij constatering van een reeds plaatsgevonden aanval of een onderzoek bij constatering van een vermoedelijke voorbereiding van een aanval.

Communicatiekanalen en -middelen

In het OSP moet worden aangegeven:

- Wat de verschillende communicatiemiddelen en –kanalen zijn om alarmmelding door te geven naar het centrale meldpunt;
- Wat de communicatiemiddelen en –kanalen zijn die het centrale meldpunt heeft om interventie op te roepen en om met de gebruikers van het pand te communiceren. Denk aan communicatie met 112-centrale, oproepsystemen, omroepsystemen en dergelijke;
- Wat de communicatiemiddelen en –kanalen zijn van de personen die een interventierol hebben.

Hierbij moet ook helder zijn wat de noodzakelijke betrouwbaarheid moet zijn in de zin van beschikbaarheid, vertrouwelijkheid en integriteit van de communicatie en op welke wijze hierin wordt voorzien.

Interventie procedures

Binnen het OSP moet vastliggen op welke wijze incidenten geregistreerd worden, wat de stappen zijn in de levencyclus van een incident en wie 'incident manager' is. Het OSP moet operationele procedures bevatten voor het type dreigingen waartegen beveiliging moet plaatsvinden. Denk bijvoorbeeld aan:

- Inbraak, insluiping
- Brand
- Bezetting
- Blokkade
- Bommelding
- NBCR-incident
- Verdachte zending
- Verdacht voertuig
- Verdacht persoon
- Verdachte activiteit
- Chantage

Nazorg activiteiten

Nazorg activiteiten zijn onder meer:

- Continuïteitsmaatregelen en herstelmaatregelen op de bedrijfsprocessen. Deze liggen vast in het business continuïteit plan en vormen geen onderdeel van het OSP;
- Herstellen van gefrustreerde beveiligingsmaatregelen. De schade kan bewust veroorzaakt zijn in een security aanval, maar de maatregelen kunnen ook ontregeld zijn door menselijk falen, technisch falen en door omgevingsomstandigheden. Meestal gaan beveiligingsmaatregelen defect buiten de normale werktijden. De tijdsduur van de tijdelijke verzwakking van de beveiliging dient zo beperkt mogelijk te zijn. Daarom moeten er beslisregels en procedures bestaan op:
    - Welke beveiligingsmaatregelen direct hersteld dienen te worden (noodherstel) en welke beveiligingsmaatregelen hersteld kunnen worden op de eerste normale werkdag;
    - Of een tijdelijke verzwakking van de beveiliging geaccepteerd wordt tot het moment van (nood)herstel of dat er additionele maatregelen getroffen moeten worden. Daarbij moet aangegeven zijn wat die additionele maatregelen zijn;
    - Wie beslist of een tijdelijke verzwakking van de beveiliging acceptabel is;
    - Op welke wijze het noodherstel georganiseerd is;
    - Op welke wijze het definitieve herstel georganiseerd is.

- Maatregelen naar slachtoffers. Dit kan ARBO-achtige slachtofferhulp zijn. Echter vanuit security kunnen ook maatregelen worden getroffen opdat de security situatie rond het slachtoffer en de afdeling (of de beleving hiervan) weer genormaliseerd wordt;
- Maatregelen naar daders. Naar de veroorzaker van het incident dienen maatregelen getroffen te worden, bijvoorbeeld opvoedkundig, disciplinair, verhalen schade of juridisch;
- Evaluatie.
  In het OSP moet vastliggen hoe het incident geregistreerd wordt, wie de beheerder is van het incident, hoe de evaluatie plaatsvindt van het incident - bijvoorbeeld rapportage naar security platform - en op welke wijze het incident wordt afgesloten.

5. Maatregelen op personen

De mens neemt in het beveiligingsproces een centrale plaats in. De mens kan dader/veroorzaker zijn van een beveiligingsincident en kan ook het slachtoffer/doelwit zijn van het incident. Daarnaast is de mens ook een belangrijk instrument om beveiligingsincidenten te signaleren en beheersbaar te maken.
Deze paragraaf geeft enkele type maatregelen om de factor mens in de beveiliging te versterken.

Consistent maken van type maatregelen voor de verschillende personengroepen

De type maatregelen voor de verschillende personengroepen die de organisatie kent moeten consistent zijn.
Denk aan de volgende personengroepen:
- Vast personeel, eventueel in type functies;
- Tijdelijk personeel;
- Extern personeel, contractors, leveranciers;
- Bezoekers.

Bovenstaande houdt niet in dat de eisen en maatregelen voor de verschillende groepen gelijk zijn, maar wel dat er consistentie is.

Inrichting van de organisatie

Bij de inrichting van de organisatie moet vastliggen:
- Wat de functie-eisen zijn;
- Wat de integriteiteisen zijn van de functie;
- Over welke security- en safety-kennis personen moeten beschikken.

Instroom maatregelen

Instroom maatregelen in de organisatie zijn onder meer:
- Werving, selectie en aanname procedure;
- Zwarte lijst;
- Controleren CV, getuigschriften, referenties;
- Antecedenten onderzoek;
- Verklaring omtrent gedrag, eigen verklaring omtrent gedrag;
- Integriteittest, drugstest;
- Geheimhoudingverklaring;
- Security / safety opleiding en test.

Employment maatregelen

Maatregelen gedurende het dienstverband zijn bijvoorbeeld:
- Beveiligingsopleidingen / bewustzijn;
- Integriteitopleidingen, bewustzijn;
- Gedragscode, integriteitbeleid;
- Functionerings- en beoordelingsgesprekken;
- Belonings- en sanctiebeleid;
- Screening of VOG op periodieke basis en/of bij doorstroom naar andere functie.

Exit maatregelen

Maatregelen bij beëindigen van dienstverband zijn onder meer:

- Intrekken autorisaties;
- Inleveren pasjes, sleutels, telefoon e.d.;
- Checklist laatste dag;
- Exitgesprek met leidinggevenden;
- Ontslag op staande voeten procedure;
- Monitoren gedrag na vertrek.

Integriteitbeleid

Het integriteitbeleid kan van belang zijn om expliciet vast te leggen wat de organisatie verstaat onder integer handelen en hoe dit bereikt moet worden.

Sancties

Sancties zijn nodig tegen veroorzakers van security incidenten en kunnen ook een afschrikkende werking hebben.

Beheren van beveiligingscompetenties

Effectieve omgang met risicosituaties is sterk afhankelijk van de menselijke factor. In welke mate worden risicosituaties gezien, voorzien en doorzien en wat is de kennis en het gedrag om de persoonlijke rol in de risicobeheersing optimaal uit te voeren.

Het operationeel beheren van de benodigde competenties in de organisatie is een belangrijke taak. Onder competenties worden in ieder geval kennis, gedrag en cultuuraspecten verstaan. Daarnaast is het van belang om zoveel mogelijk te sturen op kennis- en gedragsaspecten op individueel niveau. Daarmee kan op langere termijn ook de beveiligingscultuur in een organisatie beïnvloed worden.

Vanuit bovenstaande optiek is het zinloos om een losse security bewustwordingsactiviteit - bijvoorbeeld postercampagne - uit te voeren, omdat deze niet past in een lange termijn visie, aanpak en volhardendheid en concrete doelstellingen. Ook is het niet effectief om bewustwording los te zien van andere kennis- en gedragssturende activiteiten als training en oefening.

Definiëren van benodigde competenties

Start met het definiëren van concrete benodigde kenniscompetenties, zoals:

- Weet waar incidenten gemeld moeten worden;
- Weet hoe vertrouwelijke informatie herkend wordt.

Hierbij dienen ook doelstellingen te worden vastgelegd. Bijvoorbeeld 90% van afdeling moet weten waar de incidenten moeten worden gemeld.

Vanzelfsprekend kunnen de doelstellingen ook in de loop van de tijd worden aangepast:

- In jaar 1 moet 70% van personeel weten waar incidenten gemeld moeten worden;
- In jaar 2 moet 90% van personeel en 70% van leveranciers weten waar incidenten gemeld moeten worden;
- In jaar 3 moet 95% van personeel en 90% van leveranciers weten waar incidenten gemeld moeten worden.

Uitvoeren van metingen

Een nulmeting legt de startpositie vast en geeft inzicht in waar de grootste probleemgebieden zijn en dus waar de meeste winst te behalen is. Deze input kan gebruikt worden bij het vaststellen van de benodigde doelstellingen op competenties.

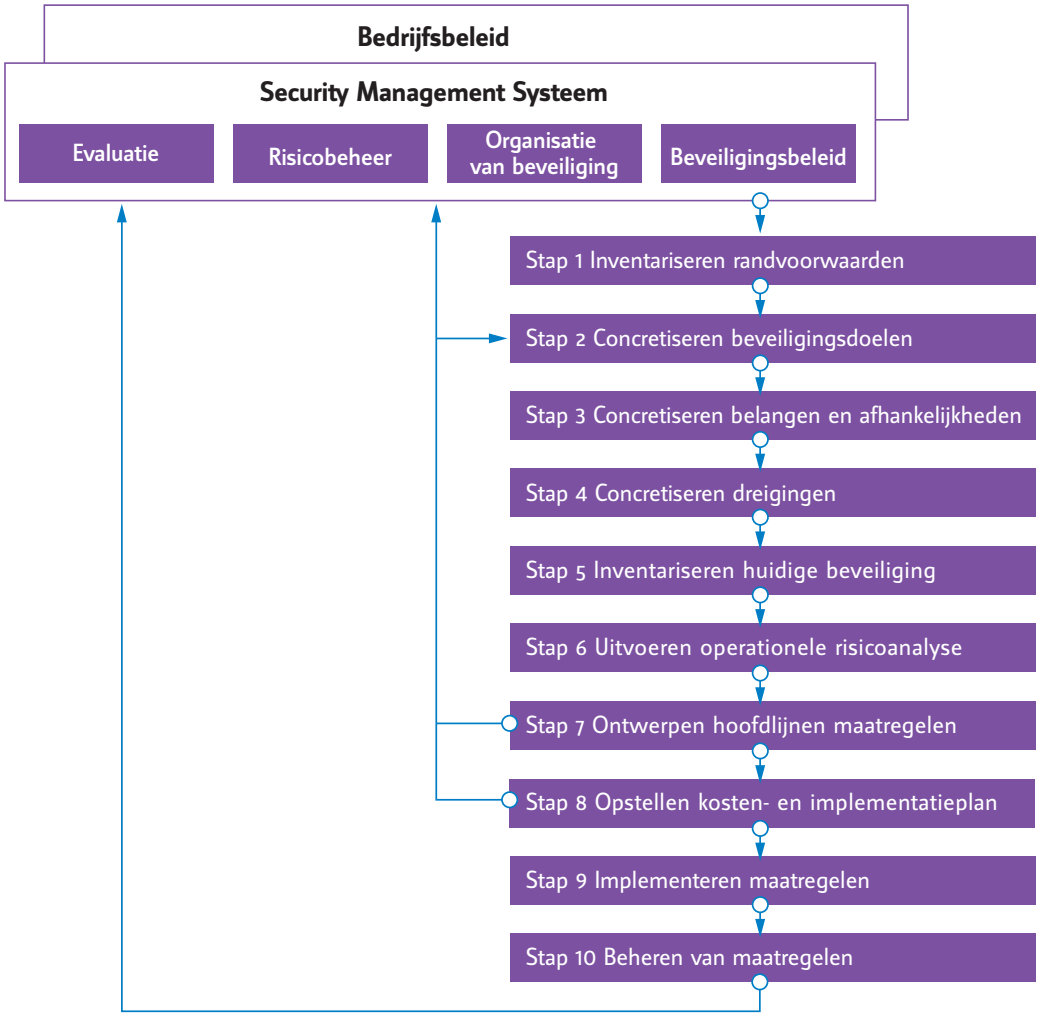
Door daarna periodiek de kennis te meten wordt inzichtelijk in welke mate de doelstellingen worden gehaald. Met de verkregen gegevens kan op individueel of groepsniveau bijgestuurd worden met activiteiten om de doelstellingen te halen. Daarnaast kan het vertoonde gedrag gemeten worden. Dit gebeurt vanuit de incidentevaluatie en de evaluatie van oefeningen.

Uitvoeren van competentie beïnvloedende activiteiten

Competentie beïnvloedende activiteiten zijn onder meer:

- Posters
- Artikelen in personeelsblad
- Filmpjes
- Bericht direct na afloop van beveiligingsincident
- Security kennisplein op intranet
- Werkoverleg
- Trainingen bij indiensttreding
- Directiespeech bij indiensttreding
- Communicatie naar bezoekers
- Algemene security trainingen
- Gespecialiseerde security trainingen
- E-learning trainingen
- Oefeningen

Stappenplan
Operator Security Plan



Producten van het NAVI

In de reeks NAVI-producten zijn de volgende publicaties beschikbaar:

- Handreiking Risicoanalyse. Deze handreiking stelt een beheerder van de vitale infrastructuur in staat om en een goede risicoanalyse m.b.t. risico's, dreigingen en kwetsbaarheden te maken.
- Handreiking Beveiligingsafstemming Vitaal en Overheid (BAVO). Deze handreiking beschrijft hoe in het operationele pakket van beveiligingsmaatregelen de afstemming tussen het vitale bedrijf en de overheid geregeld kan worden.

In de reeks producten van derden zijn de volgende publicaties beschikbaar:

- Handreiking Security Management Systeem (SMS) voor de olie- en chemiesector. Deze handreiking biedt handvatten aan een beheerder van installaties binnen de olie- en chemiesector om een security management systeem in te richten. De handreiking is opgesteld door het ministerie van VROM in samenwerking met het NAVI.
- US-CCU Checklist voor cybersecurity. Deze checklist is opgesteld door de onafhankelijke U.S. Cyber Consequences Unit in de Verenigde Staten en biedt praktische handvatten voor informatiebeveiliging. De checklist heeft een brede internationale verspreiding en is in samenwerking met de US-CCU vertaald door het NAVI voor de Nederlandse markt.
- Pre-employment screening in Groot-Brittannië. Een handreiking van The Centre for the Protection of National Infrastructure (CPNI).

Nationaal Adviescentrum
Vitale Infrastructuur

T (070) 376 59 50
E info@navi-online.nl
www.navi-online.nl

Lange Voorhout 13
2514 EA Den Haag
Postbus 20011
2500 EA Den Haag