RisicoRegisseurs B.V.

Weeshuisplein 10
3131CX Vlaardingen
info@risicoregisseurs.nl
www.risicoregisseurs.nl
KVK: 70599335

HET BEVEILIGINGSPROCES GERICHT OP CONTINUÏTEIT

RisicoRegisseurs hanteert haar beveiligingsmodel om organisaties in zeven stappen blijvend baas te laten zijn over de beveiliging van hun organisatie.

Het beveiligingsproces gericht op continuïteit

HET FYSIEKE BEVEILIGINGSPROCES

Er zijn vele definities en beschrijvingen in omloop als het om het begrip fysieke beveiliging gaat. Onder fysieke beveiliging verstaan wij:

- de juiste mix van organisatorische, bouwkundige, elektronische en reactieve maatregelen
- ter preventie, detectie, repressie en correctie van fysieke dreigingen door menselijk handelen
- gericht op bedrijfsprocessen, informatie, materieel en personen
- waarmee een bijdrage wordt geleverd aan de continuïteit van de processen van de organisatie.

Welke definitie je ook hanteert, in onze optiek moet fysieke beveiliging bijdragen aan de continuïteit van de organisatie. Dat kan door beveiliging in te richten als proces waarbij de risico's ten aanzien van de organisatie centraal worden gesteld.

Vanuit RisicoRegisseurs helpen wij organisaties bij het maken van de overstap van een rule-based benadering naar een risk-based benadering en daarmee met het verleggen van een focus op beveiligingsmaatregelen naar een focus op de risico's. Dit doen we aan de hand van het onderstaande proces, waarbij we de risico's van een organisatie als uitgangspunt nemen zodat meer begrip ontstaat voor de realistische risico's die een organisatie loopt en de maatregelen die je hier tegenover kunt stellen om deze risico's beheersbaar te krijgen.

DE RISICO'S VAN EEN ORGANISATIE

Iedere organisatie heeft haar eigen bedrijfsprocessen, informatie, materieel en personen die een bijdrage leveren aan het voortbestaan van de organisatie. De mate waarin een organisatie daarvan afhankelijk is, vormt een belangrijk uitgangspunt voor de wijze waarop beveiliging wordt ingericht. Bij het inrichten van het beveiligingsproces wordt rekening gehouden met het risicogedrag dat past bij de organisatie. Een organisatie kan risicomijdend, risiconeutraal of juist risicodragend zijn. Een organisatie die risicodragend is zal in de praktijk meer risico's accepteren en daarmee minder of minder zware maatregelen treffen dan een organisatie die meer risicomijdend is. Het vinden van de juiste mix aan beveiligingsmaatregelen is daarmee altijd maatwerk voor de organisatie.

Als de risico's niet goed begrepen worden dan is het haast onmogelijk om de juiste beveiligingsmaatregelen te treffen. Dit is de reden dat de risico's van de organisatie het vertrekpunt vormen voor het beveiligingsproces dat wij hanteren.

HET BEVEILIGINGSBELEID

Onder beleid verstaan wij het aanwijzen van de richting en de middelen waarmee de organisatie de gestelde doelen wil realiseren. Passend bij de aard van de organisatie wordt daarom in het beveiligingsbeleid vastgelegd wat de visie is op beveiliging en welke bereidheid er is voor het nemen van risico's. Daarnaast wordt onder meer beschreven hoe de beveiligingsorganisatie is ingericht, wie met welke verantwoordelijkheden betrokken zijn en welke processen van toepassing zijn. Omdat het beleid voor iedereen binnen de organisatie geldend is, wordt tevens aangegeven wat van de medewerkers wordt verwacht.

Bij een risk-based benadering, waarbij de risico's van de organisatie centraal staan, is het van belang het risicobewustzijn van alle medewerkers op peil te krijgen en te houden. Als inzicht wordt gegeven in de risico's die de organisatie loopt, wordt het voor iedereen binnen de organisatie meer duidelijk waarom bepaalde beveiligingsmaatregelen worden genomen en hoe men daar zelf een zo goed mogelijke bijdrage aan kan leveren. Het door de directie vastgestelde beveiligingsbeleid geeft daarmee de kaders weer waarbinnen beveiliging wordt ingericht.

DREIGINGSPROFIEL

"*Hoe weet ik nu welke risico's mijn organisatie loopt?*", is een vraag die we bij veel organisaties tegenkomen. Het eerlijke antwoord daarop is dat je waarschijnlijk nooit alle risico's vooraf zult kennen. Daarom maken we onderscheid in fysieke dreigingen van natuurlijke aard, zoals een aardbeving en fysieke dreigingen als gevolg van menselijk handelen, zoals een inbraak. Tevens maken we onderscheid in realistische en niet-realistische dreigingen voor de organisatie. Datgeen wat logischerwijs denkbaar en voor de organisatie realistisch is, wordt vastgelegd in een zogenaamd dreigingsprofiel.

Het doel van het dreigingsprofiel is om op basis van eenduidige begrippen en definities inzicht te verschaffen in de combinaties van dreigingen, dadertypen en aanvalsmiddelen waarvan beoordeeld wordt dat ze als mogelijke onacceptabele risico's worden gezien en waartegen de organisatie zich wil beveiligen. Hiermee wordt de grens bepaald voor de mate van beveiliging om daarmee te veel of te weinig beveiliging te voorkomen.

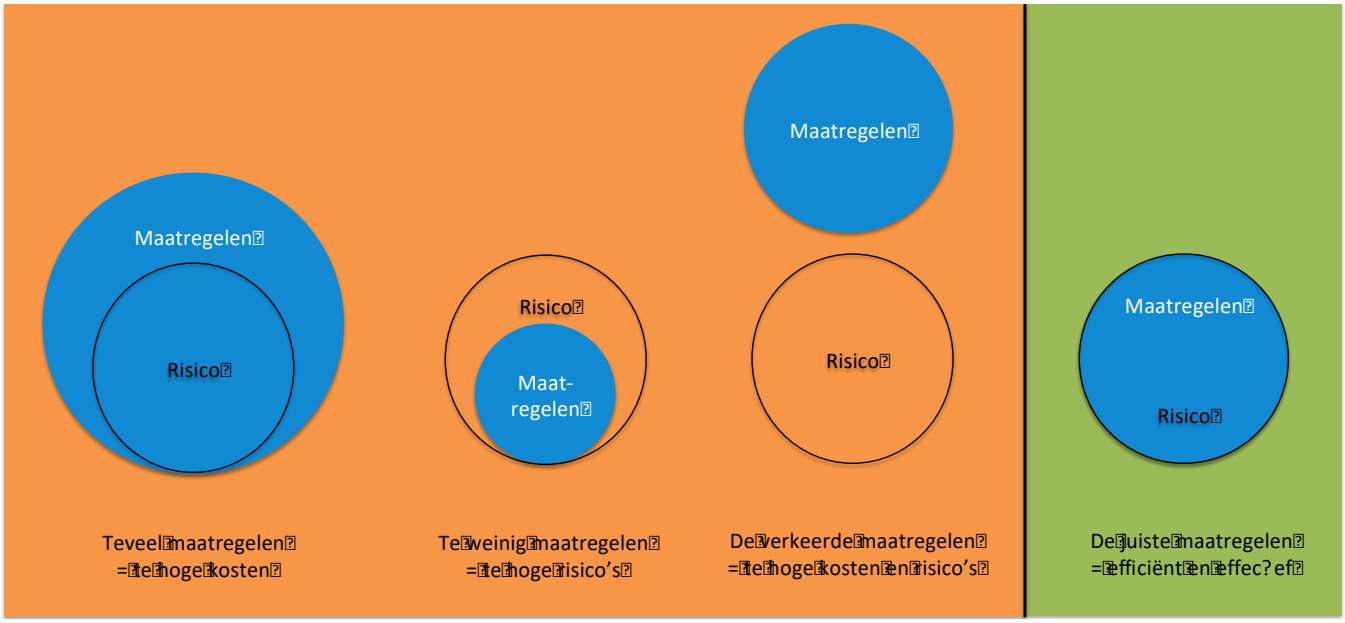
Het dreigingsprofiel wordt actueel gehouden door dreigingen en incidenten die zich binnen en buiten de organisatie voordoen te analyseren en daar waar nodig toe te voegen aan het dreigingsprofiel. Op deze manier wordt voorkomen dat zich nieuwe dreigingen voordoen waar de organisatie onvoldoende op is voorbereid.

PROGRAMMA VAN EISEN

Op basis van wet- en regelgeving, het beveiligingsbeleid en het dreigingsprofiel wordt in het Programma van Eisen beschreven welke beveiligingsmaatregelen genomen worden om de voor de organisatie benoemde risico's beheersbaar te maken. Omdat risico's per type locatie verschillen en omdat locaties in meer of mindere mate van belang zijn voor het voortbestaan van de organisatie, kunnen meerdere Programma's van Eisen relevant zijn. Bijvoorbeeld een Programma van Eisen voor de hoofdkantoren naast een Programma van Eisen voor de verschillende winkelfilialen in het land.

In de Programma's van Eisen worden de organisatorische, bouwkundige, elektronische en reactieve maatregelen beschreven die overwogen kunnen worden om een risico beheersbaar te maken. In onze risk-based benadering kiezen we ervoor om per maatregel onderscheid te maken in de zwaarte van de maatregel. Het voordeel van het werken met gradaties in de zwaarte van maatregelen, is dat je daarmee de meest optimale mix aan beveiligingsmaatregelen kunt treffen. Het best passend bij de hoogte van het risico. Bij een lage risico-inschatting kun je een lichtere maatregel inzetten en daarmee het risico beheersen tegen lagere kosten, terwijl voor hogere risico's juist een zwaardere combinatie van maatregelen gekozen kan worden. Zo kan het bijvoorbeeld voor een locatie, op basis van de risicoanalyse, niet nodig zijn om een camerasysteem te installeren, terwijl voor een andere locatie een lokaal systeem overwogen dient te worden en dat voor weer een andere locatie een uitgebreid camerasysteem met slimme camera's aangesloten op een beveiligingsloge of in combinatie met LiveView nodig is.

Door te veel of te zware maatregelen te nemen wordt de organisatie geconfronteerd met te hoge kosten voor beveiliging. Door te weinig of te lichte maatregelen te nemen loopt de organisatie onacceptabele risico's. En door de verkeerde maatregelen te treffen zijn zowel de kosten als de risico's voor de organisatie te hoog. Het doel is om het optimum te vinden.



KOPPELINGSTABEL

Wat onze aanpak uniek maakt is dat we, voorafgaand aan het uitvoeren van risicoanalyses per locatie, een koppeling leggen tussen alle dreigingen uit het dreigingsprofiel enerzijds en de juiste combinatie van maatregelen uit het Programma van Eisen anderzijds. In de gekozen combinatie van de maatregelen en dreiging worden bovendien de lichtere varianten van de beveiligingsmaatregelen gekoppeld aan de lagere risicoklasse van de dreigingen en andersom. Dit alles wordt vastgelegd in wat we een koppelingstabel noemen.

Het voordeel van het werken met dergelijke vastgelegde koppelingen is dat bij het uitvoeren van de risicoanalyse per locatie gebruik wordt gemaakt van een vast stramien en zo niet meer per locatie hoeft te worden nagedacht, en ook niet achteraf steeds opnieuw hoeft te worden toegelicht en verdedigd, welke combinatie van maatregelen het best passend is. Voor de vastgestelde risicoklasse van alle dreigingen krijg je zo per locatie de beste mix aan maatregelen, die zal bijdragen aan het beheersen van de risico's voor de betreffende locatie. De koppeling tussen de dreigingen vanuit het dreigingsprofiel en de maatregelen vanuit het Programma van Eisen vormen het uitgangspunt voor de risicoanalyse per locatie.

RISICOANALYSE

In de risicoanalyse wordt per dreiging op basis van attractiviteit en het belang de risicoklasse bepaald zodat inzicht ontstaat in de hoogte van het risico. Hierbij onderscheiden we vier risicoklasses, waarbij klasse 1 de laagste en klasse 4 de hoogste risicoklasse is. Dat leidt tot een risicoklasseindeling die er – afhankelijk van de risicostrategie van de organisatie - als volgt uit zou kunnen zien:

Attractiviteit \ Belang	Laag	Midden	Hoog	Zeer hoog
Laag	1	1	2	2
Midden	1	2	3	3
Hoog	2	3	4	4
Zeer hoog	2	4	4	4

In onze aanpak maken we onderscheid in de attractiviteit enerzijds en het belang voor de organisatie anderzijds. Bij de attractiviteit wordt gekeken naar de aantrekkelijkheid van een locatie voor een dader om diens motieven (het doel) van de aanval te kunnen realiseren. Terwijl we bij het belang kijken naar de kritische waarde die een locatie voor de organisatie heeft.

Bij het belang wordt rekening gehouden met de impact van een risico op de continuïteit van de organisatie als dat risico zich manifesteert. Hierbij wordt niet alleen rekening gehouden met directe financiële schade, maar juist ook met de indirecte schade zoals uitval van processen en eventuele gevolgschade zoals bijvoorbeeld imagoschade. Per locatie wordt bij de risicoanalyse gekeken naar de processen die er worden uitgevoerd en wat hiervoor aan informatie, materieel en personen op de locatie aanwezig is. Op grond hiervan wordt bepaald welke dreigingen voor een locatie realistisch zijn, hoe hoog de risico's daarvan zijn, wat de gevolgen daarvan kunnen zijn en welke maatregelen uit het Programma van Eisen wenselijk zijn om die risico's op een aanvaardbaar niveau te houden.

Omdat we in een eerder stadium al een koppeling hebben gelegd tussen de dreigingen en de zwaarte van de beveiligingsmaatregelen, kan de noodzakelijke combinatie van beveiligingsmaatregelen met de juiste zwaarte per maatregel nu eenvoudig en snel bepaald worden. Uiteraard kan, op basis van *professional judgement*, altijd besloten worden dat een andere combinatie van maatregelen beter zou passen. Het gaat immers om het afdekken van de risico's en niet om het nemen van maatregelen.

BEVEILIGINGSPLAN

Voor een locatie is in de risicoanalyse voor iedere dreiging de risicoklasse vastgesteld en aan ieder risico zijn die beveiligingsmaatregelen gekoppeld, die het best passen bij het risicogedrag van de organisatie. Voor risico's die voorkomen moeten worden, kunnen preventieve maatregelen worden getroffen. Voor die risico's die zich toch manifesteren, zijn de juiste detectieve, repressieve en correctieve maatregelen geïmplementeerd zodat incidenten snel ontdekt, beheerst en hersteld kunnen worden. Welk niveau van de maatregel wordt voorgesteld, is afhankelijk van de hoogte van het risico, waaraan de maatregel moet bijdragen. Zo genereer je de meest optimale mix van de best passende beveiligingsmaatregelen. De combinatie van maatregelen en de zwaarte van de te kiezen maatregelen, die volgt uit de risicoanalyse, wordt vastgelegd in het beveiligingsplan.

Door ook inzichtelijk te maken welke maatregelen op locatie reeds gerealiseerd zijn (de zogenaamde IST-situatie) en deze te vergelijken met de maatregelen die nodig zijn om de risico's te beheersen, ontstaat direct inzicht in de restrisico's die er voor de organisatie zijn. Voor deze restrisico's kan gekozen worden ze formeel te accepteren of voor de onacceptabele risico's kan besloten worden dat verbeteringen nodig zijn.

Een beveiligingsproces dat continu gericht is op de continuïteit van de organisatie vraagt uiteraard dat het beveiligingsplan periodiek op actualiteit wordt getoetst. En dat waar er wijzigingen in processen, risico's en/of maatregelen zijn, dat deze in het plan worden verwerkt.

MAATREGELEN

Op basis van de risicoanalyse is inzichtelijk welke risico's aangepakt moeten worden en op basis van het beveiligingsplan is duidelijk welke maatregelen daar dan tegenover moeten staan. De mix aan beveiligingsmaatregelen die getroffen wordt bestaat uit een combinatie van organisatorische, bouwkundige, elektronische en reactieve maatregelen. De maatregelen die wenselijk zijn, worden geïmplementeerd, onderhouden en periodiek gecontroleerd zodat de organisatie erop kan vertrouwen dat de maatregelen naar behoren werken en de risico's daarmee zijn afgedekt.

Daar waar leveranciers betrokken zijn bij de maatregelen vindt afstemming plaats, worden de afspraken in contracten vastgelegd en wordt er periodiek verantwoording afgelegd over de prestaties. De leveranciers wordt uitgelegd welke risico's onderkend worden en welke bijdrage de door hen geleverde producten en diensten daaraan moeten leveren.

RANDVOORWAARDEN

Om het proces goed te laten werken zijn er een aantal randvoorwaarden waarmee rekening dient te worden gehouden. Deze randvoorwaarden dragen eraan bij dat het proces steeds beter wordt en dat de risico's die de organisatie loopt onder controle kunnen worden gehouden. De randvoorwaarden die we onderscheiden zijn:

1. Incidentanalyses
2. Risicoacceptatie
3. Audits

Incidenten

Analyse van de incidenten en bijna incidenten, zowel van binnen als buiten de eigen organisatie, is belangrijk om helder te krijgen of er nieuwe dreigingen relevant zijn geworden en of de gekozen maatregelen (nog) voldoen om de risico's beheersbaar te houden. Door de resultaten van de analyses te verwerken in het dreigingsprofiel wordt ervoor gezorgd dat de beveiliging van de organisatie steeds zo goed mogelijk is afgestemd op de voorstelbare realistische dreigingen die zich voor kunnen doen.

Risicoacceptatie

Een lijnmanager is als eigenaar van de processen verantwoordelijk voor het beheersen van de risico's behorend bij de processen. De beveiligingsrisico's horen hier onderdeel van uit te maken. Daarbij wordt gekeken naar het belang van de processen en de daarbij behorende ondersteunende middelen die nodig zijn om de processen uit te voeren. Binnen de organisatie wordt aan de hand van het risicogedrag bepaald welke risico's men bereid is te lopen en welke met behulp van beveiliging gecontroleerd moeten worden. En dit niet eenmalig, maar continu. In een formeel risicoacceptatieproces wordt een keuze gemaakt tussen het wegnemen van het risico, het accepteren van een risico of een combinatie van deze beiden. De beveiligingsmanager is, als procesbegeleider, aanwezig om het lijnmanagement op een zo goed mogelijke manier te adviseren en te ondersteunen bij het beheersen van risico's. Het is in die zin niet de beveiligingsmanager die bepaalt welke risico's acceptabel zijn, want dat is het lijnmanagement. Voor die risico's die niet acceptabel gevonden worden, is de beveiligingsmanager er wel verantwoordelijk voor de juiste mix aan beveiligingsmaatregelen voor te stellen en te implementeren om het risico tot een acceptabel niveau te reduceren.

Audits

Het doel van beveiliging is om de risico's te beheersen. Is gedaan wat was gepland en zijn de locaties nu voldoende beveiligd? Het uitvoeren van audits geeft zekerheid over de mate waarin de aanpak van beveiliging voldoende is georganiseerd (procesaudit) en de wijze waarop de beveiligingsmaatregelen voldoende in staat zijn om de baas over de beveiliging van de organisatie te zijn (tactisch en operationele audit).

Met het uitvoeren van audits kom je aan het eind van de cyclus van het proces. Maar omdat beveiliging een proces is, waarbij gestreefd wordt naar continue verbetering, wordt de cyclus niet afgesloten. Beveiliging is geen eenmalige activiteit. Om steeds beter grip te krijgen op beveiliging en om steeds beter te kunnen spreken van een manier van beveiligen dat effectief en efficiënt is, wordt fysieke beveiliging als continu proces ingericht.

GRIP OP FYSIEKE BEVEILIGING

Door fysieke beveiliging als continu proces in te richten krijgt de organisatie steeds meer grip op de risico's die van invloed kunnen zijn op de continuïteit. De organisatie krijgt steeds beter begrip van de risico's en weet steeds beter welke mix aan beveiligingsmaatregelen nodig is om die risico's beheersbaar te maken en te houden zodat de organisatie kan aantonen dat ze fysieke beveiliging serieus neemt. Er worden geen beveiligingsmaatregelen genomen omdat er nu eenmaal maatregelen getroffen moeten worden maar er worden maatregelen genomen die daadwerkelijk toegevoegde waarde hebben. Beveiliging is daarmee een bedrijfsproces dat, net als alle andere bedrijfsprocessen, een zo goed mogelijke bijdrage moet leveren aan de continuïteit van de organisatie.

Wil jij weten hoe het met de beveiliging van jouw organisatie zit? Vraag via info@risicoregisseurs.nl direct een beveiligingsconsultatie aan, waarin we:

1. Inzicht verschaffen in de risico's voor de organisatie,
2. aangeven welke beveiligingsmaatregelen daarbij passen,
3. je kunnen laten zien hoe het beveiligingsproces werkt voor jouw organisatie.

Je zult zien dat je na het consult meer inzicht hebt in hoe je de controle over de fysieke beveiliging van jouw organisatie gaat krijgen.