Leerdoelen

Hoofdstuk 1. **Inleiding in proactieve beveiliging**

- Je weet waarom proactief beveiligen van belang is.
- Je hebt kennis van het ontstaan van de proactieve beveiligingsmethdiek Predictive Profiling in Israël.
- Je hebt kennis van het ontstaan van de proactieve beveiligingsmethodiek OGRI & Predictive Profiling in Nederland.
- Je begrijpt waarom proactieve beveiliging en predictive profiling niets te maken hebben met etnische profilering en criminal profiling.

Hoofdstuk 2. **Beter communiceren**

- Je weet hoe proactief beveiligen wordt uitgevoerd.
- Je kent de begrippen OMA, LSD, ANNA, NIVEA en OEN
- Je weet waarom de begrippen OMA, ANNA, LSD, NIVEA en OEN belangrijk zijn voor een proactieve beveiliger.
- Je begrijpt hoe je beter kunt communiceren

Hoofdstuk 3. **De basisprincipes van proactief beveiligen**

- Je weet waarom proactief beveiligen van belang is.
- Je begrijpt dat het toepassen van enkel reactieve beveiligingsmaatregelen niet effectief is om incidenten vroegtijdig te herkennen en voorkomen.
- Je begrijpt dat als je iets wilt herkennen je moet weten hoe het eruitziet.Je weet hoe proactief beveiligen wordt uitgevoerd.
- Je begrijpt dat je actie moet ondernemen als er mogelijk sprake is van een ongewenste situatie.

Hoofdstuk 4. **Fysieke en technologische beveiligingsmaatregelen**

- Je weet waarom proactieve beveiliging van belang is.
- Je begrijpt dat fysieke en technologische beveiligingsmaatregelen geen intentie kunnen waarnemen.
- Je kent de 3 onderdelen van het driepoortenmodel.
- Je begrijpt het verschil tussen het driepoortenmodel en de OBE-maatregelen.
- Je hebt inzicht in het nut van proactieve beveiligers ten opzichte van de reactieve beveiligingsmaatregelen.

Hoofdstuk 5. **Risico of dreiging? Een nieuwe manier van denken**

- Je begrijpt de voordelen van dreigingsoriëntatie in plaats van risico-oriëntatie.
- Je begrijpt dat risico gaat over kans en waarom dit niet handigis als je incidenten wilt voorkomen.
- Je begrijpt waarom een tweeledige dreigingsbenadering functioneel is voor een proactieve beveiliger.
- Je bent bekend met relevante dreigingsscenario's.
- Je begrijpt het nut van werken met dreigingsscenario's.

Hoofdstuk 6. **Denken vanuit het oogpunt van de tegenstander**

- Je bent bekend met relevante dreigingsscenario's.
- Je kent het verschil tussen een AMO en een scenario en begrijpt dat een scenario uit verschillende AMO's kan bestaan.
- Je begrijpt waarom het kennen van de norm belangrijk is voor je werk als proactieve beveiliger.
- Je kent de stappen van de criminele en terroristische planningscyclus.
- Je begrijpt waarom sommige stappen in de cyclus rood zijn gekleurd.
- Je snapt in welke stap van de cyclus je het best de potentiële tegenstander kunt herkennen.
- Je weet in welke stap jij als proactieve beveiliger de laatste mogelijkheid hebt om vroegtijdig een incident te stoppen.

Hoofdstuk 8. **De mens staat centraal**

- Je begrijpt waarom je een open, neutrale houding moet hebben als je een proactieve interventie pleegt.
- Je werkt met kennis over de begrippen OMA, LSD, ANNA, NIVEA en OEN.
- Je kent de voordelen en het belang van een klantvriendelijke houding in het beveiligingswerk. De zes voordelen van servicegericht werken zijn bekend.
- Je kent het PGO-BD-model en begrijpt de relatie van dit model met hospitality.
- Je begrijpt wat de customer journey is en snapt het verschil met de criminele en terroristische planningscyclus.
- Je begrijpt waarom twee stappen in de cyclus een andere kleur hebben.
- Je kent de LEER-methode en de voordelen van de LEER-methodein professionele gesprekken.
- Je begrijpt waar de afkorting LEER voor staat.

Hoofdstuk 9. **Interventietechnieken**

- Je bent bekend met de theorie over leugendetectie in de praktijk.
- Je kent het begrip ‘prikkelen’ en kunt ‘prikkels’ inzetten ten gunste van je proactieve beveiligingswerk.
- Je begrijpt wat tegenstanders meestal willen verhullen als zij een slechte intentie hebben en je bent bekend met de term ‘coverstory’.
- Je weet hoe een effectief vraaggesprek gevoerd wordt.
- Je hebt kennis van ‘open’ en ‘gesloten’ vragen.
- Je begrijpt hoe het ‘spotlighteffect’ werkt.
- Je hebt kennis van verschillende soorten prikkels en weet hoe je die kunt gebruiken als proactieve beveiliger.
- Je hebt kennis over de methodiek controlled cognitive engagement (CCE) om proactieve vraaggesprekken te kunnen voeren.
- Je weet dat security questioning tot doel heeft om de dreiging te ontkrachten door het verklaren van gedrag.
- Je begrijpt hoe je een indicator kunt verklaren.

Hoofdstuk 10. **Informatiegestuurd werken**

- Je begrijpt waarom informatiegestuurd werken van belang is voor een proactieve beveiliger.
- Je begrijpt waarom het hebben van actuele kennis over de werkwijze van de tegenstander van belang is voor een proactieve beveiliger.
- Je kent minimaal drie relevante cyberdreigingen.
- Je weet hoe je informatiegestuurd kunt werken met behulp van de digitale Applicatie Predictive Profiling (APP).


CARVE IT UP
CALIFORNIA SURF
BEACH
COOL
FLORIDA
ROOTS

Inleiding

Hoofdstuk 1
Inleiding

Hoofdstuk 1

Inleiding

Leerdoelen

- Je weet waarom proactief beveiligen van belang is.
- Je hebt kennis van het ontstaan van de proactieve beveiligingsmethodiek Predictive Profiling in Israël.
- Je hebt kennis van het ontstaan van de proactieve beveiligingsmethodiek OGRI & Predictive Profiling in Nederland.
- Je begrijpt waarom proactieve beveiliging en predictive profiling niets te maken hebben met etnische profilering en criminal profiling.

1.1
Reactief beveiligen

De beveiligingsstructuur binnen een organisatie bestaat altijd uit een combinatie van maatregelen en procedures die gezamenlijk voor een veilige (werk) omgeving moeten zorgen. Veel organisaties beschikken over dikke boekwerken vol veiligheidsprocedures, calamiteitenplannen en bedrijfsnoodplannen. De meeste van deze procedures zijn opgesteld om goed te kunnen handelen nadat een incident heeft plaatsgevonden. Hierdoor wordt geprobeerd om de schade zo veel mogelijk te beperken, of om de reguliere werkprocessen zo snel mogelijk weer op gang te krijgen. Dit zijn zogenoemde reactieve beveiligingsmaatregelen. Dat wil zeggen: maatregelen of procedures die in werking treden nadat er een incident heeft plaatsgevonden.

De meeste organisaties zullen aangeven dat de beveiliging bestaat om ongewenste situaties te voorkomen, maar in de praktijk van de meeste bedrijven is dit niet het geval. Door reactief te beveiligen wordt er slechts gereageerd op ongewenste situaties op het moment dat ze gebeuren. Er bestaan traditioneel weinig tot geen preventieve beveiligingsmiddelen in Nederland, buiten de ‘afschrikkende werking’ van de zichtbare beveiliging. Hoe kunnen beveiligers leren om door hun handelen op het werk bij te dragen aan het voorkómen van incidenten? Hoe kunnen beveiligers proactief beveiligen, en wat betekent dat eigenlijk? Dit leerboek biedt hiervoor de belangrijkste lessen.

1.2
Introductie in proactieve beveiliging

Proactief beveiligen is een redelijk nieuw begrip in Nederland. Google het begrip en je komt al snel uit bij een aantal commerciële bedrijven die een eigen visie op proactief beveiligen hebben. Tot op heden is er nog geen algemeen geaccepteerd leerprogramma proactief beveiligen voor de beveiligers in Nederland. Het leerboek Proactief Beveiligen brengt hier verandering in en creëert daarmee een Nederlandse standaard in de beveiligingsbranche.

In dit leerboek wordt een andere manier van beveiligen aangeleerd. Namelijk proactief beveiligen. Proactief beveiligen houdt in dat je niet reageert op wat er is gebeurd, maar dat je actief bent in je beveiligingswerkzaamheden en met behulp van kennis en aangeleerde vaardigheden je taken en verantwoordelijkheden verricht. Wat voor kennis dat precies is en wat je moet kunnen om proactief te beveiligen wordt in dit leerboek duidelijk gemaakt.

1.3
Wat maakt iemand een proactieve beveiliger?

De vraag wat iemand een proactieve beveiliger maakt, zal direct worden behandeld omdat het laat zien hoe jij actief kunt werken aan de ontwikkeling van een proactieve werkhouding. De kerncompetenties van een proactieve beveiliger zijn in ieder geval dat je 1) nieuwsgierig bent en 2) zelf actie durft te ondernemen. Proactief beveiligen houdt in dat je inzicht hebt in de beveiligingsdoelstellingen van de organisatie en weet wat je wel, en wat je vooral niet moet doen om deze doelstellingen te behalen. Je zult dus zelf actie moeten ondernemen en nieuwsgierig moeten zijn. Dit houdt ook in dat je geïnteresseerd bent in je eigen beveiligingswerkzaamheden en in de dienstverlening van jouw organisatie. Proactief beveiligen vergt niet alleen inzet, het geeft ook een grote mate van verantwoordelijkheid aan de beveiliger. Je bent namelijk zelf verantwoordelijk voor de handelingen die je verricht en de beslissingen die je neemt. In tegenstelling tot veel reactieve beveiligingswerkzaamheden zal je zelf moeten nadenken en zelf moeten beslissen hoe je handelt in bepaalde (bedreigende) situaties.
Proactieve beveiliging houdt in dat je actief op zoek gaat naar jouw tegenstander.

Dit zijn de kwaadwillende bezoekers, gasten, medewerkers of cliënten. Zodra je deze gevonden denkt te hebben, neem je een servicegerichte houding aan en ga je met ze in gesprek. In de gesprekken die je voert probeer je het gedrag te verklaren dat de aanleiding gaf om het gesprek te starten. Als je een sluitende verklaring voor dit vertoonde gedrag vindt, kan het zijn dat de dreiging wordt weggenomen. Je probeert de intentie achter het vertoonde gedrag te ontdekken en moet inschatten of je te maken hebt met een bedreigende situatie of juist niet. Jij hebt dus een belangrijke taak in het beslissen over bedreigende situaties en jij bepaalt hoe je de situatie gaat oplossen.

Je denkt zelf na over de stappen die je gaat zetten en de gevolgen daarvan. Uiteraard hoef je dat niet zelf te bedenken zonder dat je is geleerd hoe je kunt handelen, en vanuit welke beveiligingsvisie je de beveiligingsmaatregelen kunt inzetten. Met dit leerboek helpen we jou om proactief te kunnen handelen. Je wordt 'in de proactieve modus' gezet. Met kennis van de proactieve methodiek kun je straks direct in de praktijk aan de slag.

Goed proactief beveiligen is een proces. Het kost tijd en moeite om vaardigheden te verbeteren. Door training, maar vooral door in de praktijk te oefenen, kun je beter worden in de beveiligingswerkzaamheden. Maar let op: alleen (in de praktijk) ervaren is niet genoeg. Je moet het eigen handelen evalueren met je collega's en bespreken met de teamleiders. Leer dus van je ervaringen, wordt iedere dag een beetje beter in het werk dat je doet en maak de organisatie weer wat veiliger.

1.4
Van reactief naar proactief veiligheidsbeleid

De beveiligingsstructuur in Nederland is van oudsher vooral reactief ingesteld. Dit betekent dat beveiliging over het algemeen gaat over het reageren op incidenten. Als er een inbraakalarm afgaat, volgt de beveiliger een procedure om het probleem op te lossen. Als er een vechtpartij uitbreekt, zorgt de beveiliger ervoor dat de situatie beheersbaar wordt en probeert hij de situatie te de-escaleren. Er wordt in deze twee voorbeelden gehandeld nadat een incident heeft plaatsgevonden. Dit reactieve handelen kan de schade die het incident heeft aangericht alleen zo veel

mogelijk beperken. Als er een vechtpartij uitbreekt, is het bijvoorbeeld mogelijk om het aantal mensen dat bij de vechtpartij betrokken raakt te verkleinen. Ook is het mogelijk dat een beveiliger tussenbeide komt om de schade te beperken. Zoals je misschien al opmerkt, is een groot nadeel van het enkel inzetten van dit soort reactieve beveiligingsmaatregelen dat een beveiliger geen incidenten voorkomt, maar altijd achter de feiten aanloopt.

Om proactief te kunnen beveiligen, moet je onderzoeken waar het gedrag of de situatie die je tegenkomt vandaan komt. Daar is een verandering van je mindset voor nodig. Als je niet nieuwsgierig bent om te onderzoeken, zul je al snel denken 'het zal wel niets zijn'. Maar let op! Deze houding is reactief en dat is niet gewenst als je proactief wilt beveiligen. Om deze reactieve werkhouding zo veel mogelijk te voorkomen, stelt een proactieve beveiliger zichzelf de vragen: Wat gebeurt er? Waarom gebeurt het? En wat zie ik in de omgeving dat mij kan informeren over de afwijkende situatie of het afwijkende gedrag? Je zult je ervan bewust moeten zijn dat er van jou een actie wordt verwacht. De actie die je kunt ondernemen is tevens de enige manier om achter de intentie (het waarom) van het vertoonde gedrag of de situatie te komen. Dit is meteen ook de kerntaak van proactief beveiligen en wordt gezien als het meest uitdagende onderdeel van de proactieve beveiligingsmethodiek.

Tot slot is het belangrijk om te beseffen dat reactief beveiligen niet slecht is, maar je kunt er niet van uitgaan dat een reactief opgeleide beveiliger situaties herkent die mogelijk met criminele activiteiten samenhangen.

Proactief beveiligen geeft een specifieke aanvulling waardoor je incidenten mogelijk vroegtijdig kunt voorkomen.

1.5
Het ontstaan van de proactieve beveiligingsmethodiek in Israël

De proactieve beveiligingsmethodiek Predictive Profiling is in Israël ontstaan nadat er op 20 mei 1972 een terroristische aanslag werd gepleegd op de luchthaven Lod (tegenwoordig Ben-Gurion). Deze eerste grootschalige aanslag