Proactief beveiligen

Lesboek

Geschreven door:

Stephan Kapma

Colofon

Copyright

ISBN

978-94-93179-44-8

Adresgegevens

Smart Educational Tools, onderdeel van Stichting eX:plain
Disketteweg 6
Postbus 1230
3800 BE Amersfoort
www.smarteducationaltools.nl

Inhoud

Woord vooraf

Woord vooraf

Dit boek gaat over proactief beveiligen voor een beginnende beroepsbeoefenaar, met andere woorden; het gaat om de beginnende beveiliger. Het boek bereidt u voor op het examen proactief beveiligen dat wordt afgenomen door het SVPB. Het geeft u inzicht in het systeem proactief beveiligen, maar de leerstof is onvoldoende om ook een proactieve beveiliger te zijn. Om dat te worden is specifieke training noodzakelijk. Dat is mede afhankelijk van het soort object waar u uw werkzaamheden gaat verrichten. Het boek geeft u wel veel inzicht waardoor u een betere beveiliger kunt zijn.

U zal ontdekken dat hoe proactief beveiligd wordt afhankelijk is van het object waar u werkzaam bent. Het dreigingsbeeld en de mogelijke manier van een gekozen aanval door een crimineel/terrorist kan door diverse invloeden verschillen. Deze opleiding is dus vooral gericht op het geven van basiskennis over proactief beveiligen.

Het is belangrijk als beveiliger een andere mindset te hebben dan die we vaak in Nederland aantreffen. Het gaat over inperking van dreigingen en dus over het beschermen van levens, goederen en processen. Daarom is het belangrijk dat de beveiliger ook de verantwoordelijkheid neemt als hij een situatie waarneemt waarbij hij bedenkingen heeft. Leg dus niet de focus op waarnemen en rapporteren, maar op zelf nadenken en reageren.

Er wordt van u, de proactieve beveiliger, verwacht dat u de dreigende situatie probeert te weerleggen en daarbij de SOP (Standard Operation Procedures) volgt. Als de beveiliger dat niet doet of niet thuis geeft, dan blijft de directe constante bedreiging aanwezig. Vervolgens is het alleen wachten totdat iemand daar misbruik van maakt, met alle gevolgen van dien. Stel dat de beveiliger niet reageert op een bedenking die hij had bij een aangetroffen situatie of gedrag

en er vallen daardoor doden. Hoe zal de beveiliger daar achteraf op terugkijken?

Er zijn veel voorbeelden van mensen die met een levenslang schuldgevoel achterblijven, omdat als ze gehandeld hadden er wellicht een calamiteit voorkomen had kunnen worden.

Voorbeeld:

Bij de bomaanslag op het vliegtuig dat bij Lockerbie is neergestort is gebruikgemaakt van een *Improvised Explosive Device* (IED) die verstopt zat in de bagage. Degene die dat op het vliegveld had moeten ontdekken was net nieuw en heeft de bom niet gevonden. De persoon heeft na een aantal jaren een eind aan zijn leven gemaakt omdat hij niet kon leven met het idee de dood van zo veel mensen op zijn geweten te hebben.

U kunt in overweging nemen dat hij nieuw was en slecht ingewerkt. Hijzelf zag het anders. Laat staan als een ingewerkte professional zoiets mist.

Als er een aanslag op een vliegtuig plaatsvindt dat bijvoorbeeld van Schiphol is vertrokken, dan is het eerste wat de profiler daar doet is kijken of hij zelf de intake voor deze vlucht heeft gedaan. Beveiliging is dus een taak en een vak met verantwoordelijkheid. Met grote gevolgen als er wat wordt gemist.

De kans om zaken te missen is groter als u ‘gewone’ beveiliger bent dan als u proactief beveiliger bent. U wordt met dezelfde situaties geconfronteerd. Echter, als proactieve beveiliger heeft u geleerd waar u op moet letten, hoe u de verdenking kunt weerleggen en wat u moet doen als u het als een reële dreiging inschat.

Passend daarbij is een uitspraak die ik op LinkedIn tegenkwam van een van de grondleggers van *Predictive Profiling*: '"bedreiging" kent geen niveaus. Het kan niet hoog of laag zijn. Het kan niet groeien of krimpen. Er bestaat een bedreiging of deze bestaat niet. ... *Dus wie bepaalt of er een dreiging bestaat of niet? U!'*

Eigenlijk zou elke beveiliger een proactieve beveiliger moeten zijn, omdat dan de wereld een stuk veiliger wordt. In het land van oorsprong van dit systeem, Israël, is dat allang realiteit.

Elke beveiliger werkt daar volgens deze methode. De organisatie waarvoor hij zijn diensten verleend hebben de bijbehorende procedures vastgelegd en uitgerold.

Opbouw

We starten in hoofdstuk 1 met te kijken naar de aanvaller, de mensen met de kwade bedoelingen. Welke dadergroepen zijn er? We staan stil bij de criminele en terroristische planningscyclus en bij *social engineering*.

In hoofdstuk 2 bekijken we de verdediging vanuit de organisatie. We maken eerst een verschil tussen dreigingen en risico's. Hoe kan een dreiging beperkt worden? Wat is proactief beveiligen? We leggen uit wat AMO's zijn en wat we als Verdachte Indicatoren (VI's) beschouwen. Verder leggen we uit van SOP's zijn en wat ze inhouden.

In hoofdstuk 3 beschrijven we de activiteiten van de proactieve beveiliger, u dus. We staan stil bij de dreigingsassessments, bij coverstory's en *Security Questioning*. Daarnaast kijken we naar de competenties die een proactieve beveiliger moet hebben.

In hoofdstuk 4 sluiten we af met *Red Teaming*.

Waar in dit boek wordt gebruikgemaakt van de hij-vorm, wordt daarmee mensen bedoeld in algemene zin.

Met de term ‘u’ wordt verwezen naar u als proactieve beveiliger. Als de term beveiliger wordt gebruikt, wordt daarmee de proactieve beveiliger bedoeld, tenzij anders aangegeven.

De termen kwaadwillende, agressor, crimineel of terrorist worden in dit boek door elkaar gebruikt. Hiermee wordt steeds de aanvaller bedoeld die het gemunt heeft op het beschermde object waar u dienstdoet.

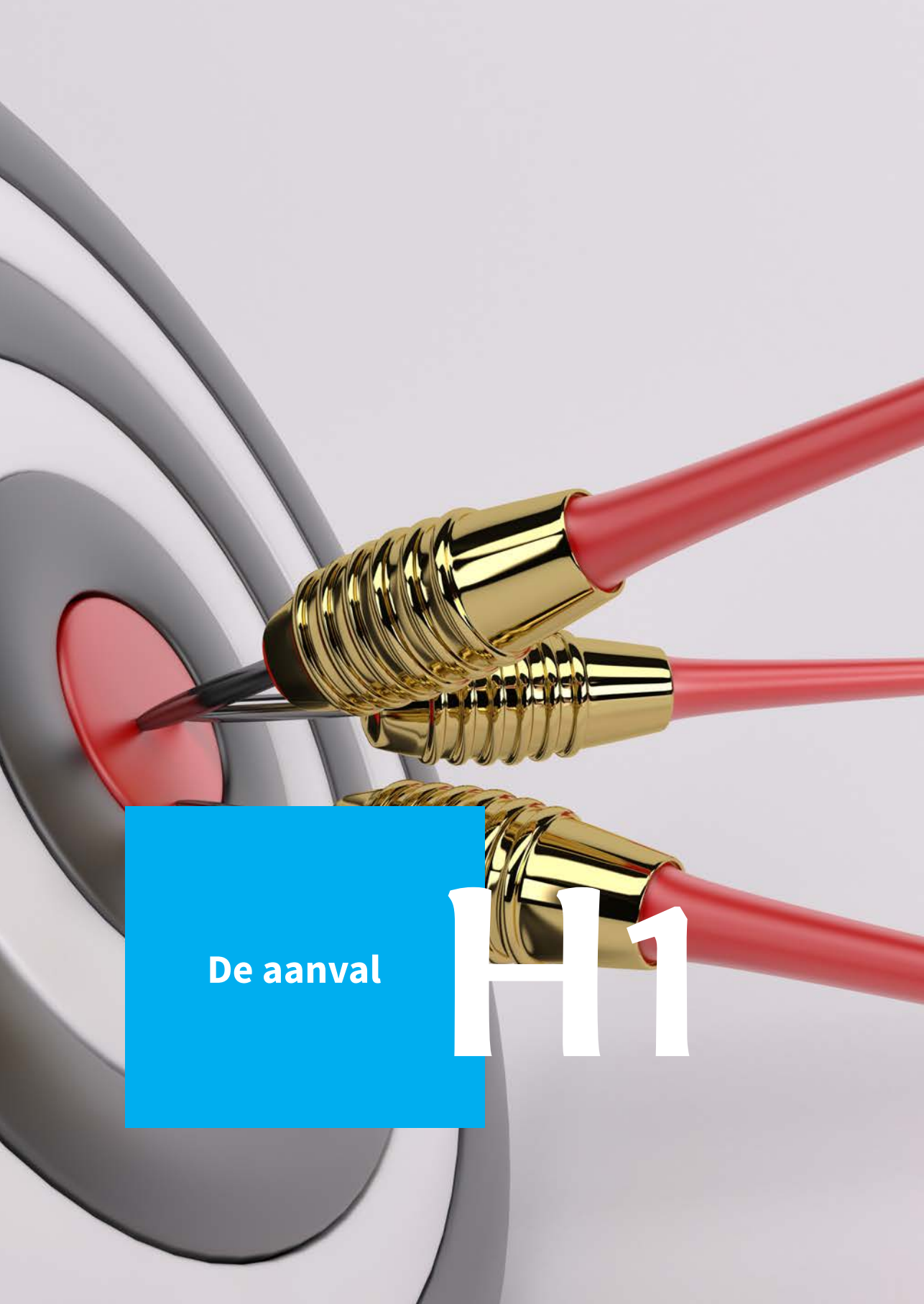
Praktijk

Dit opleidingsboek heeft als doel de beginnende proactieve beveiliger inzicht te geven in het systeem proactief beveiligen. Daarnaast heeft het als doel om u als beveiliger bewuster te maken van hoe belangrijk u bent als schakel in een veiligere wereld, beginnend bij uw eigen object.

De vaardigheid in het doen van een dreigingsassessment en bijbehorende Security Questioning, dient u te ontwikkelen door het te doen, op uw eigen handelen te reflecteren en vervolgens de uitkomsten toe te passen. Een nooit eindigende cirkel van leren.

Veel plezier met lezen, studeren en vooral toepassen.

Stephan Kapma



H1 De aanval

H1 De aanval

Leerdoelen:

- Weten welke dadergroepen de NAVI onderscheidt
- De stappen in de criminele/terroristische planningscyclus kunnen benoemen
- Het begrip *social engineering* kunnen omschrijven
- Weten wat een coverstory inhoudt en uit welke elementen deze bestaat

Inleiding

Elk object wordt constant bedreigd. Welke dreiging dat precies is, is afhankelijk van een aantal omstandigheden en verschilt per object. U weet niet wanneer een dreiging werkelijkheid kan worden en wie de aanvaller is. We bekijken dit onderdeel door de bril van een (mogelijke) dader.

Voorbeeld:

De woninginbraken
De woninginbraken werden goed voorbereid. De verdachten gingen bij de woningen posten en in de buurt hardlopen. Wanneer zij over gingen tot de inbraak, waren de bewoners vaak thuis omdat het alarm dan niet aan stond. De verdachten maakten zoveel mogelijk gebruik van trappen die al aanwezig waren op de locaties waar ze gingen inbreken. Ook hadden ze bij een woninginbraak een trap wit geschilderd omdat het huis waar ze wilden inbreken die kleur had. Het kwam voor dat de bewoners beneden tv keken en de inbrekers boven hun slag sloegen. Zij stonden hierbij ook in de kamers van slapende kinderen, waarbij er één keer een kind wakker werd en rechtop in bed zat.

De verdachten stonden vandaag terecht voor het plegen van tien woninginbraken en voor zes pogingen. Het OM vindt het zeer aannemelijk dat de verdachten veel meer inbraken hebben gepleegd. Zij heeft hier echter alleen aanwijzingen voor en niet het bewijs. Zo is achteraf gebleken dat de auto's waarin de verdachten reden bij meerdere inbraken in de omgeving zijn gezien, maar dat is onvoldoende bewijs om ook die inbraken aan hen toe te schrijven.

Bron: www.om.nl