

Proactief beveiligen



Lesboek

Geschreven door:

Stephan Kapma

Colofon

Copyright

Niets uit deze uitgave mag worden verveelvoudigd en/of openbaar worden gemaakt door middel van druk, fotokopie, microfilm of op welke andere wijze dan ook zonder voorafgaande schriftelijke toestemming van de uitgever.

Samenstellers en uitgever zijn zich volledig bewust van hun taak een zo betrouwbaar mogelijke uitgave te verzorgen. Niettemin kunnen zij geen aansprakelijkheid aanvaarden op onjuistheden die eventueel in deze uitgave voorkomen.

De uitgever meent alle rechten van afbeeldingen te bezitten of daar afspraken over te hebben gemaakt. Indien rechthebbenden toch een opmerking hebben, kunnen zij zich tot de uitgever wenden.

ISBN

9789493252547

Adresgegevens

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

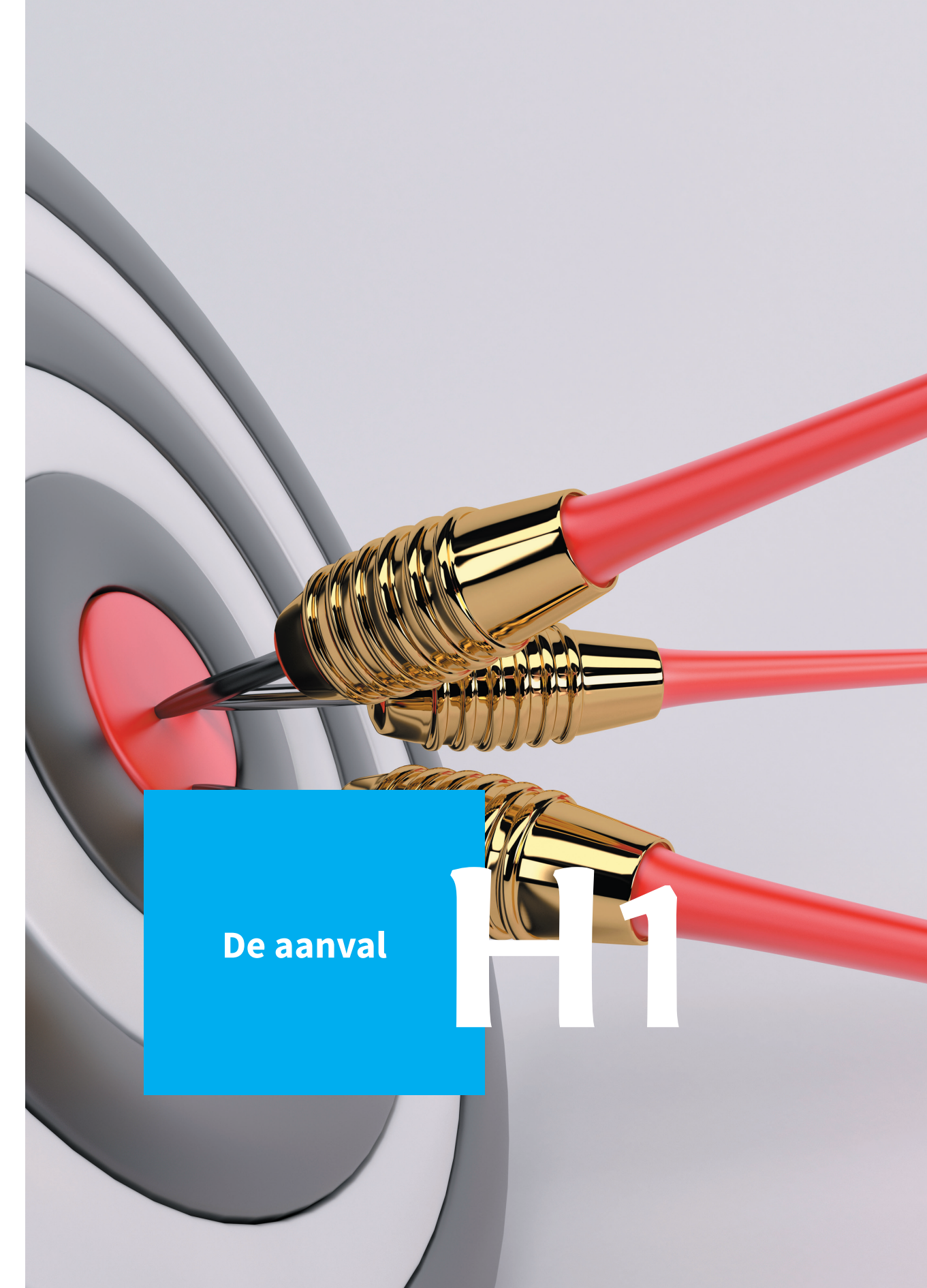
September, 2022



Inhoud

Woord vooraf	6
Algemeen	12
1 De aanval	16
Inleiding	16
1.1 De dadergroepen opgesteld door NAVI	22
1.2 Vier factoren die bijdragen tot een uitvoering	25
1.3 De criminele/terroristische planningscyclus	27
1.4 Social engineering	36
1.5 Coverstory	38
2 De organisatie van de verdediging	42
Inleiding	42
2.1 Wat te beschermen en waartegen?	42
2.2 Proactief beveiligen	44
2.3 Dreiging of risico?	45
2.4 Aanvallers Methode van Operatie (AMO)	49
2.5 Verdachte Indicatoren (VI)	53
2.6 Wat is verdacht gedrag?	54
2.7 Standaard Operationele Procedure (SOP)	59
3 De rol van de proactieve beveiliging	64
Inleiding	64
3.1 Proactief	64
3.2 Voorwaarden en competenties van een proactieve beveiliging	66
3.3 Actieve en passieve preventieve maatregelen	68
3.4 Dreigingsassessment	70

3.5	Classificatie	75
3.6	Security Questioning	76
3.7	Signalen die kunnen duiden op liegen	80
3.8	Open en gesloten vragen	84
4	Red Teaming	90
	Inleiding	90
4.1	Scenario's testen	90
4.2	Interne en externe Red Teaming	92
	Woordenlijst	96

The background of the entire image is a 3D rendering of a target with concentric grey and white rings. In the center, a red bullseye is visible. Three red cables, each with a gold-colored, threaded connector, are plugged into the bullseye. The cables extend from the bottom right towards the center. A blue square is positioned in the lower-left area, partially overlapping the target and the cables.

De aanval

H1

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

Voorbeeld:

Rabo-beveiligers voor de rechter na bankroof

BREDA - Twee beveiligers van het door de Rabobank ingehuurde beveiligingsbedrijf EBN moeten dinsdag voor het eerst voor de rechter verschijnen. De mannen van 43 en 45 jaar uit Etten-Leur en Roosendaal worden verdacht van betrokkenheid bij de miljoenendiefstal uit de kluiselder van de bank in Oudenbosch. Het gaat om een niet-inhoudelijke zitting in de rechtbank in Breda.

De spectaculaire kluisroof werd op 5 maart ontdekt, maar was al enkele dagen eerder gepleegd. Honderden kluisjes werden leeggeroofd. De daders waren meer dan 24 uur in het gebouw en verlieten volgens de politie de bank met miljoenen aan contant geld en sieraden. Op camerabeelden is te zien hoe twee daders met volle vuilniszakken vertrekken.

De twee beveiligers hebben waarschijnlijk de bankrovers geholpen door ze binnen te laten. De dieven zijn nog altijd niet opgespoord. De beveiligers ontkennen dat zij iets met de roof te maken hebben. Hun contract is inmiddels door het beveiligingsbedrijf opgezegd.

De Rabobank had eerder al laten weten alle schade te vergoeden die de gedupeerden van de kluisroof in Oudenbosch kunnen aantonen.

Bron: https://www.telegraaf.nl/nieuws/2368791/rabo-beveiligers-voor-de-rechter-na-bankroof?utm_source=google&utm_medium=organic

1^e veroordeling RABO bankroof: vier jaar cel en 1 miljoen schadevergoeding.