Coördinator beveiliging

Beveiliging van gebouwen

Colofon

Copyright

crebo 25408

ISBN

978-94-93179-24-0

Adresgegevens

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

Juli, 2020

Inhoud

H1

Beveiliging van object als onderdeel van een groter geheel

H1 Beveiliging van object als onderdeel van een groter geheel

Leerdoelen:

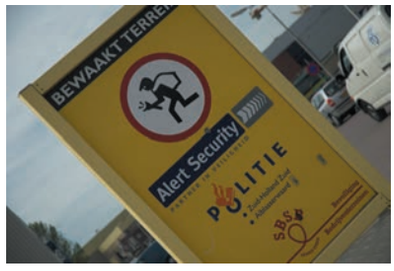
- Kan m.b.t. crisisbeheersing de verschillende begrippen toelichten (zoals Stelsel Bewaken en beveiligen) en de taken van betrokken instanties
- Begrippen uit de circulaire 'Bewaken en Beveiligen' kunnen benoemen
- De rol en taak van een crisis(management)-team kunnen beschrijven
- De vitale infrastructuur in Nederland kunnen beschrijven
- De opschaling bij een calamiteit kunnen beschrijven
- De samenwerking tussen de diverse overheidsinstanties en particuliere beveiligingsorganisaties kunnen beschrijven incl. verantwoordelijkheden

Inleiding

Heel veel particuliere organisaties regelen de beveiliging en veiligheid van hun eigen organisatie. Dit doen ze omdat ze hun processen en mensen willen beschermen tegen inbreuk. Dit gebeurt soms uit eigen wil, maar soms ook door wetgeving zoals de Arbowet en Wetboek van Strafrecht of vanwege eisen die door de verzekering worden gesteld.
Er zijn momenten waarop de particuliere organisaties te maken kunnen krijgen met de publieke veiligheidszorg, die door de overheid wordt geregeld. In dit hoofdstuk geven we meer inzicht in de publieke veiligheidszorg en staan we stil bij de momenten waarop deze zorg de private veiligheidszorg kunnen raken.
We behandelen de diensten die de basis veiligheidszorg in een gemeente verzorgen, we staan stil bij het opschalen binnen het eigen object en kijken naar de mogelijkheden om op te schalen als de basis veiligheidszorg niet meer voldoet en staan we als laatste stil bij rampen. Eerst een toelichting op de veiligheidszorg.

De veiligheidszorg is onder te verdelen in twee gebieden:

- De veiligheidszorg in het publieke domein. Dit noemt men de publieke veiligheidszorg. Met het publieke domein worden bedoeld openbare wegen, openbare gelegenheden en overheidsgebouwen. Deze veiligheidszorg wordt daar voornamelijk geleverd door de overheid. Voorbeelden hiervan zijn politie, buitengewone opsporingsambtenaren (boa's), leger, brandweer, ambulancedienst en inlichtingen- en veiligheidsdiensten.
- De veiligheidszorg in het private domein. Dit noemt men de private veiligheidszorg. Met het private domein worden bedoeld woningen van particulieren, bedrijven en bedrijfsterreinen. Deze veiligheidszorg wordt daar voornamelijk geleverd door particuliere beveiligingsorganisaties.



Het komt regelmatig voor dat taken in het publieke domein door particuliere beveiligingsorganisaties worden overgenomen. Door het overnemen van deze taken kan de publieke veiligheidszorg zich meer richten op hun repressieve taak zoals verbaliserend optreden en aanhouden. Denk hierbij aan een bedrijvengebied waar de politie in samenwerking met een particuliere beveiligingsorganisatie zorgt voor de beveiliging van dat gebied door surveillance.

Een aantal voorbeelden waarbij particuliere beveiligingsorganisaties werkzaam zijn in het publieke domein zijn:
- beveiligers als gevangenisbewaarder of arrestantenverzorger;
- beveiligers als receptionisten bij politiebureaus;
- beveiligers als toezichthouders in bepaalde wijken of winkelcentra;
- beveiligers als begeleiders van demonstraties;
- beveiligers als controleur binnen het openbaar vervoer;
- beveiligers als bewakers van militaire terreinen;
- beveiligers als surveillanten in bedrijfsgebieden onder toezicht van de politie;
- particulier onderzoekers die onderzoeken verrichten voor bedrijven of personen.

Publieke veiligheidsorganisaties

De publieke veiligheidsorganisaties in Nederland zijn politie, boa's, brandweer, GGD en defensie. In het kader van deze opleiding zullen de afzonderlijke taken en functies worden beschreven.

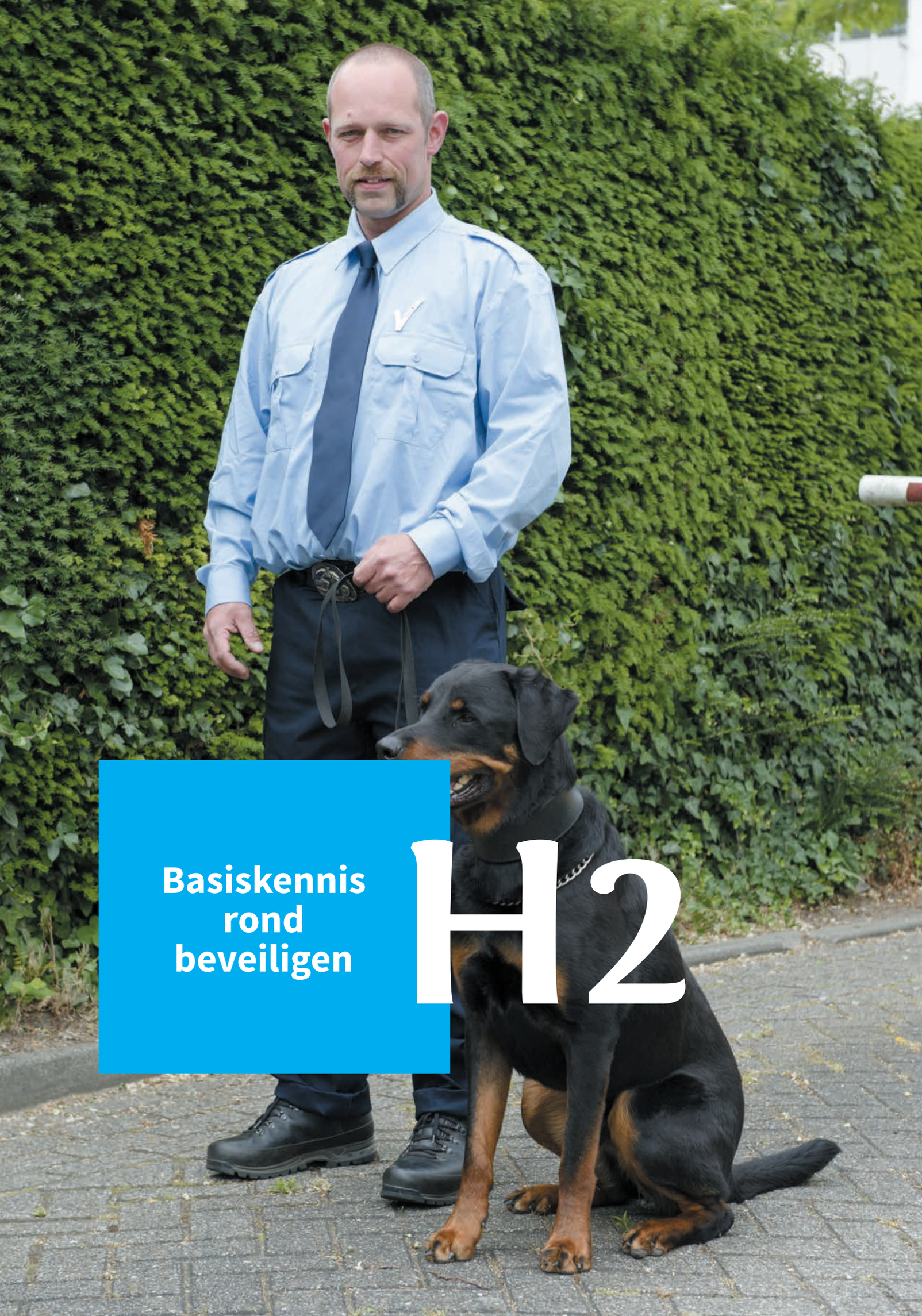
Wanneer de publieke veiligheidszorg en private veiligheidszorg samenwerken aan dezelfde doelen, wordt dat integrale veiligheidszorg genoemd. Dat wil zeggen dat alle neuzen dezelfde kant op staan om een probleem aan te pakken en elkaar daarin ondersteunen. Hoe vaker er gezamenlijke oefeningen worden gehouden, de groter de kans op echte samenwerking.

Samenvatting

De veiligheidszorg in het publieke domein wordt publieke veiligheidszorg genoemd.

De veiligheidszorg in het private domein wordt private veiligheidszorg genoemd.

Wanneer beiden samenwerken noemen wij dat integrale veiligheidszorg.



H2 Basiskennis rond beveiligen

H2 Basiskennis rond beveiligen

Leerdoelen:

- Het doel van beveiligen kunnen beschrijven
- De begrippen primair proces, te beschermen belangen, dreiging en risico's en OBE-maatregelen en informatiebeveiliging kunnen onderscheiden
- De rol van de coördinator m.b.t. de 3 beveiligingstaken kunnen omschrijven
- De competenties van de coördinator kunnen omschrijven
- De doelstelling van proactief beveiligen kunnen uitleggen
- De begrippen afwijkende indicator, normale situatie, sequerity questioning, social engineering en red teaming kunnen onderscheiden
- Risico's kunnen inschatten en van uit perspectief van de kwaadwillende kunnen denken
- De voorwaarden waarop camerabeelden als ondersteunend bewijsmateriaal mag worden overgedragen aan de politie kunnen omschrijven

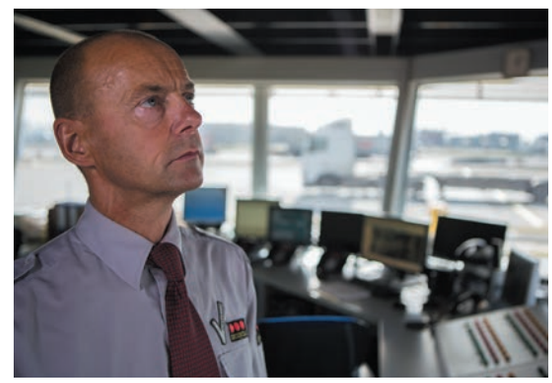
Inleiding

We behandelen in dit hoofdstuk algemene inzichten rond beveiligen. In hoofdstuk 3 staan we meer stil bij het werken met een beveiligingsplan en een veiligheidsplan.

In dit hoofdstuk beschrijven we een aantal basisbegrippen in de beveiliging. We behandelen het doel van het beveiligen; wat we willen beveiligen, waartegen we willen beveiligen en de OBE-maatregelen. Daarna staan we stil bij de rol van de coördinator met betrekking tot de 3 beveiligingstaken en de benodigde competenties van de coördinator. We pakken vervolgens proactief beveiligen op en de afgifte van camerabeelden aan de politie.

2.1 Het doel van beveiligen

Het doel van beveiligen is om een object of onderneming te beschermen tegen interne en externe schadelijke invloeden door het nemen van maatregelen. Als er geen of te weinig maatregelen zouden zijn kan er schade aan het object of bedrijf ontstaan, variërend van een lichte schade (schadecategorie III: van belang), een ernstige schade (schadecategorie II; van zeer groot belang) of kan de schade zelfs catastrofaal zijn en houdt het bedrijf op te bestaan (schadecategorie I; van vitaal belang).



In een risicoanalyse wordt een opsomming gemaakt van welke interne en externe schadelijke invloeden mogelijk een schade effect kunnen veroorzaken met een inschatting over hoe groot die schade zou kunnen zijn.

Hierbij wordt rekening gehouden met welke gedeelten van het object vrij voor publiek toegankelijk zijn (open object), welke gedeelten publiek toegankelijk zijn onder voorwaarden, zoals een kaartje kopen (gedeeltelijk open objecten) en gedeelten die niet voor het publiek toegankelijk zijn (gesloten objecten).

Beveiligen begint met het goed zicht te hebben op wat je wilt beveiligen. Wat is voor het bedrijf zo belangrijk dat men het beschermd wil hebben? Wat zijn de te beschermen belangen? Wat zijn de belangrijke processen?

Primair proces

Met het primaire proces worden die activiteiten bedoeld die rechtstreeks een bijdrage leveren aan het tot stand komen van een product of van een dienst. Daarnaast zijn er ondersteunende processen (secundaire processen) die gedaan worden om bepaalde productiefactoren in stand te houden, zoals informatiesystemen, personeelssystemen en financiële systemen. Het primaire proces is het proces waaraan de organisatie haar bestaansrecht ontleent.

Het onderscheid tussen het primaire proces en het secundaire proces is niet altijd helemaal duidelijk. Soms zijn informatiesystemen juist onderdeel van het primaire proces. Als deze gehackt of versleuteld wordt door vijandige software, komt het bedrijf meteen in grote problemen. Verstoring van het primaire proces kan een bedrijf rechtstreeks platleggen. Een ondernemer wil ondernemen, geld verdienen, zaken doen. Hierbij ziet men dat de ondernemer vooral in mogelijkheden denkt en minder in de risico's. Hierin heeft de coördinator, maar ook de beveiliger een belangrijke rol: het helpen bewust te zijn van de mogelijke gevolgen van een situatie of een gedrag op het primaire proces. Hoe beter voorbereid en geoefend, hoe groter de kans dat een schade wordt afgewend.
Een goede kennis van welke processen voor het betreffende bedrijf cruciaal zijn, op welke wijze verstoringen kunnen optreden en welke maatregelen er zijn genomen om daartegen weerstand te bieden zijn essentieel voor het werk van een beveiliger en zijn coördinator.

Te beschermen belangen

Met te beschermen belangen worden zaken bedoeld die voor de organisatie zeer belangrijk zijn en die bij het confronteren met problemen, of bij de kans dat het belang in de problemen komt, nadelige gevolgen of het risico tot nadelige gevolgen zouden kunnen hebben voor de betrouwbaarheid en continuïteit van de primaire processen.

Belangen of zaken die voor de organisatie belangrijk zijn, dus de te beschermen belangen, gaan over de volgende onderwerpen: de mens, informatie, eigendommen, het imago en de continuïteit.

WETENSCHAP

Radicaal nieuwe supercomputer zoekt naar nuttige toepassing

(Bron: volkskrant.nl)

Interessant voor de concurrentie en andere mogendheden? Te beschermen belangen?

Te beschermen belang: de mens

We kennen de eisen die de Arbowet stelt op gebied van veilig en gezond werken. Deze eisen worden behandeld in het boek Veilig Werken en Dienstplanning. Hierin staat onder andere dat de medewerker beschermd moeten worden tegen agressie en ongewenst gedrag, zoals van eigen collega's en leidinggevende(n).

Onder het te beschermen belang 'de mens' vallen naast personeel ook bezoekers, klanten en contractanten.

Sommige medewerkers zijn cruciaal voor het bedrijf, bijvoorbeeld vanwege hun specifieke kennis, maar soms ook door de toegang die men heeft tot primaire processen. Stel dat een medewerker van het bedrijf iets nieuws heeft uitgevonden, bijvoorbeeld tegen een ziekte. Dan is de kans erg groot dat dit de interesse wekt van concurrenten uit binnen- en buitenland. Als de medewerker ontvoert zou worden of zijn gezin wordt gegijzeld om op deze manier informatie te krijgen, zouden de gevolgen voor een organisatie en uiteraard voor die medewerker, zeer groot kunnen zijn. Inzicht in wie de sleutelfiguren in een organisatie zijn helpt beter te beveiligen. Denk ook aan directieleden, medewerkers van de afdeling Research & Development en medewerkers met een specifieke kennis die een ander in het bedrijf niet heeft.

NIEUWS & ACHTERGROND

Burgemeesterskandidaat Parijs trekt zich terug na seksvideo

(Bron: volkskrant.nl)

Te beschermen belang: Informatie

Welke elektronische en papieren gegevens zijn er binnen het bedrijf? Hoe vervelend zou het voor het bedrijf zijn als deze uitlekt, gestolen of gegijzeld wordt? Met name elektronische informatie is een nieuwe toegangsdeur tot het object.

NIEUWS & ACHTERGROND

Universiteit Maastricht betaalde hackers kwart miljoen euro

(Bron: volkskrant.nl)

Hoe wordt deze informatie aangeboden? Bewaard? In welke vorm? Hoe beveiligd? Wie heeft er toegang tot die informatie?