Inbraakdetectie- en beveiligingssystemen

Wat werkt?

Wat werkt er op het gebied van inbraakdetectie- en beveiligingssystemen? Het antwoord op deze vraag hangt onder andere af van of men al een inbraakdetectie- en beveiligingssysteem heeft en op zoek is naar uitbreiding of dat het een geheel nieuw te installeren systeem betreft. Ook hangt het af van wat een organisatie wil investeren en of het (nieuwe) systeem aansluit op systemen van andere organisaties.

Een Nederlandse gemeente vroeg LBVD Consultancy B.V. een onderzoek uit te voeren naar de huidige- en de gewenste beveiliging van hun panden en een advies te geven op de eventuele te nemen maatregelen. “Een gemeentehuis is een gedeeltelijk openbaar toegankelijk pand”, vertelt André van Soest, consultant bij LBVD Consultancy. “Dit betekent dat je niet wilt dat het publiek het private deel van de gemeente ongecontroleerd kan betreden. Het private deel is daarom afgesloten met toegangssystemen en alleen toegankelijk voor geautoriseerde medewerkers en haar gasten. In deze gemeente zijn er in het verleden weinig inbreuken geweest op het gebied van fysieke veiligheid, maar de gemeente wil toch een goede, actuele en betrouwbare beveiliging van het pand realiseren. Niet alleen gedurende de openingstijden, maar ook daarbuiten”.

STERK VEROUDERD SYSTEEM

Uit de gesprekken die LBVD Consultancy met de gemeente had, bleek dat het huidige inbraakdetectie- en

beveiligingssysteem al bijna tien jaar oud en ook sterk verouderd was. “De beheerders en betrokkenen ervoeren met regelmaat ongeldige alarmeringen”, vervolgt Van Soest. “Hoofdzakelijk waren er problemen met alarmering en doormelding, verouderde soft-, firm- en hardware en de gebruiksvriendelijkheid van het systeem. Ook losten medewerkers ad hoc de pseudo-ongeregeldheden of gebreken met enige frustratie op.”
Om antwoord te geven op de vraag in hoeverre de gemeente voldoet aan de door haarzelf gestelde eisen én wensen en de geldende wet- en regelgeving omtrent gebouwbeveiliging gemeente stelde LBVD Consultancy een Programma van Eisen (PvE) op. Om tot het PvE te komen moest er een risicoanalyse van het pand en de omgeving plaatsvinden. Dit bestond uit de volgende onderdelen:

- audit van het pand;
- identificeren van de risico’s (dreiging en kwetsbaarheden);
- kwantificeren van de risico’s (Risico = Kans x Effect);
- het toetsen van de risico’s op aanvaardbaarheid.

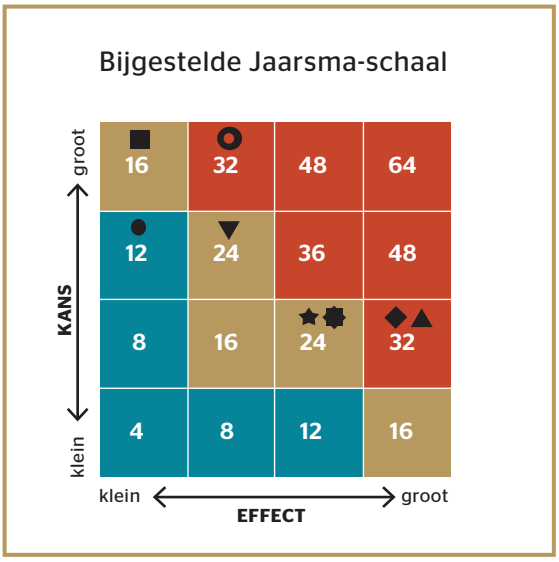
“Vervolgens hebben we met behulp van het PvE een benchmark met andere gemeenten uitgevoerd, waarna de gemeente een leverancierskeuze heeft gemaakt”.

AUDIT VAN HET PAND

Van Soest: “Voor de audit van het pand hebben we in eerste instantie een onderzoek uitgevoerd naar het huidige systeem. Met behulp van plattegronden hebben we de huidige situatie in kaart gebracht en samen met medewerkers gekeken naar welke problemen zij ondervinden met het huidige systeem. Hierbij hebben we onder andere gekeken naar de camera’s en bewegingssensoren, of er overvalknoppen en paniekknoppen op de essentiële plaatsen aanwezig waren, of er toegangsbeveiliging naar het private deel was en of (dak)ramen afdoende beschermd waren. Vervolgens hebben we bepaald wat de potentiële dreigingen en de aanwezige kwetsbaarheden waren.” Uit gesprekken met de gemeente bleek volgens Van Soest ook dat zij blootgesteld waren aan de dreiging van inbraak, overval, fysiek geweld, vandalisme en fraude.

DREIGINGSANALYSE

Risico’s moeten geïdentificeerd worden door dreiging te kwantificeren en kwetsbaarheden te beoordelen.
Van Soest: “Om de dreigingen te kwantificeren is een dreigingsanalyse uitgevoerd. De mogelijke dreigingen voor de gemeentelijke panden zijn geïnventariseerd en vervolgens zijn de dreigingen beoordeeld op ‘kans’ en ‘effect’ (impact). Deze dreigingen hebben we geplaatst in een risicomatrix, de bijgestelde Jaarsma-schaal (afbeelding 1) om inzichtelijk te krijgen welke dreigingen de hoogste prioriteit/zwaarste behandeling dienden te krijgen. Hierbij is gekeken naar de onderwerpen inbraak, overval, fysiek geweld, vandalisme/vernieling en interne fraude/diefstal.”



Afbeelding 1

In de matrix is rekening gehouden met twee factoren: kans en effect. Als je op basis van de dreigingsanalyse prioriteiten gaat stellen kan de indeling als volgt gemaakt worden:

- Blauwe vlakken: de dreigingen zijn dusdanig klein dat ze geen aandacht behoeven.
- Bruine vlakken: de dreigingen behoeven aandacht, hier moeten keuzes worden gemaakt.
- Rode vlakken: de dreigingen zijn dusdanig groot dat ze preventief beschermd moeten worden.

KWETSBAARHEIDSANALYSE

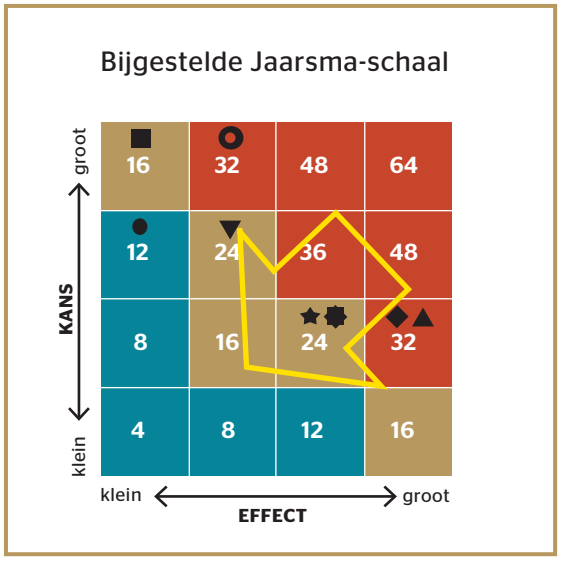
Van Soest: “Nadat we inzichtelijk hadden welke dreigingen de hoogste prioriteit/zwaarste behandeling dienden te krijgen, hebben we een kwetsbaarheidsanalyse uitgevoerd. In de kwetsbaarheidsanalyse zijn de kwetsbare plaatsen in het pand beoordeeld op de mate van beveiliging, bijvoorbeeld goed, redelijk, matig of slecht. Vervolgens hebben we bepaald op welke wijze wij de beveiliging moeten optimaliseren om tot de gewenste situatie te komen, bijvoorbeeld goed.”
Daaropvolgend heeft LBVD Consultancy aangegeven wat de maatregel in de praktijk inhoudt, bijvoorbeeld

→

→

‘IN DE KWETSBAARHEIDSANALYSE ZIJN DE KWETSBARE PLAATSEN IN HET PAND BEOORDEELD OP DE MATE VAN BEVEILIGING’

het plaatsen van extra camera’s binnen en/of buiten, het uitbreiden van het aantal sensor(en), het schrijven van protocollen, et cetera. Kwetsbare plaatsen zijn volgens Van Soest bijvoorbeeld de toegang tot het pand en de publieksruimte, balies, de personeelsingang en kantoor- en werkruimten. Per kwetsbare plaats, zoals de toegang tot het pand en de publieksruimte, zijn vervolgens verbeterpunten benoemd.
“Een voorbeeld hiervan is het plaatsen van een camera op de hoofdingang”, vertelt Van Soest. “Daarna hebben we bepaald in hoeverre deze risico’s geaccepteerd of aangepakt dienden te worden en moesten deze worden vastgelegd in een verklaring van toepasbaarheid (Statement of Applicability). Hierbij zijn tevens de relevante wet- en regelgeving, waarin eisen voor de fysieke beveiliging opgenomen kunnen zijn, meegenomen.”
Voorbeelden hiervan zijn volgens Van Soest de Wet bescherming persoonsgegevens (Wbp), Archiefwet en de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).
“Het resultaat van het nemen van maatregelen heeft invloed op het risico”, zegt Van Soest. “Door inbraakvertragende of afschrikkende maatregelen te nemen neemt de kans dat het risico zich daadwerkelijk voordoet af. Door bijvoorbeeld een goed functionerend inbraakdetectie- en beveiligingssysteem en een adequate opvolging zal de impact van een daadwerkelijke inbraak afnemen.” In afbeelding 2 is grafisch weergegeven dat door het nemen van de juiste maatregelen de dreigingen afnemen.



Afbeelding 2

PROGRAMMA VAN EISEN

“Tenslotte hebben we een PvE opgesteld en aangegeven aan welke eisen het inbraakdetectie- en beveiligingssysteem voor de panden van de gemeente moest voldoen. In het PvE hebben we aandacht besteed aan de algemene eisen voor een inbraakdetectie- en beveiligingssysteem, componentspecificatie en aanvullende eisen. Een voorbeeld van componentenspecificatie voor camerafuncties zijn observatie, identificatie en herkenning. Bij aanvullende eisen kun je bijvoorbeeld denken aan de mogelijkheid tot koppeling aan bestaande systemen, alarmopvolging, alarmverificatie, technisch onderhoud en functioneel beheer”, vervolgt Van Soest.

MARKTVERKENNING

Nadat de selectie van een aantal leveranciers had plaatsgevonden, was de gemeente uiteindelijk zelf verantwoordelijk voor het maken van de uiteindelijke leverancierskeuze en de aanbesteding die daarop volgt. Van Soest: “Tijdens de selectie hebben we rekening gehouden met de Aanbestedingswet en het inkoopbeleid van de gemeente. De eerste beoordeling was dat de leveranciers moesten voldoen aan het PvE. Vervolgens hebben we gekeken naar de vraagprijzen van de leveranciers en de kwaliteit van de verschillende componenten. De uiteindelijke classificatie is gebaseerd op een prijs-(veiligheids)kwaliteitsverhouding. Uiteindelijk hebben we deze gemeente een advies gegeven voor de aanschaf van een inbraakdetectie- en beveiligingssysteem dat past bij haar wensen, en eisen en ook voldoet aan wet- en regelgevingen. ■

André van Soest is consultant bij LBVD Consultancy B.V.