Fysieke beveiliging en Baseline Informatiebeveiliging Nederlandse Gemeenten

Alle gemeenten hebben toegezegd om voor eind januari 2017 te voldoen aan de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG). Maar wat is dat: de BIG? De Baseline is een uitwerking informatiebeveiligingsbeleid en omvat maatregelen met betrekking tot inrichting, beheer en onderhoud van informatiesystemen binnen gemeenten. De Baseline is door 95% van Nederlandse gemeenten geaccepteerd. Op deze baseline is 'verplichte zelfregulering' van toepassing. Wie denkt dat de baseline alleen over informatiebeveiliging gaat heeft het mis. Hoofdstuk 9 van de baseline gaat over fysieke beveiliging en beveiliging van de omgeving.

Hoofdstuk 9 gaat over de gebouwen en terreinen van de gemeente. Uitgangspunt is dat deze voldoende weerstand bieden bij gewelddadige aanvallen zoals inbraak en vandalisme. De baseline geeft aan hoe de gemeente ten aanzien van de beveiliging gebouwen een en ander dient in te richten. Zo dient de gemeente haar gebouwen en terreinen in te delen in zones, het zogenaamde zoneringsplan. De baseline spreekt over minimaal 4 beveiligingszones. De meeste gebruikte zones bij gemeente zijn; Openbaar; wachtruimten en spreekkamers, Werkruimten, ICT-ruimte/beveiligde ruimte (paspoort opslag of WBP art. 16 informatie of gevoelige gegevens). De beveiligingszones worden door middel van fysieke barrières gecreëerd. Doordat de gebouwen en terreinen zijn ingedeeld in zones is het eenvoudig om hieraan autorisatie modellen te koppelen zodat de toegang kan worden gereguleerd. Toegang tot gebouwen en/of ruimtes is alleen mogelijk na autorisatie voor desbetreffende zone. Het spreekt voor zich dat de wijze waarop men toegang krijgt tot een zone afhankelijk is van het type zone. Zo zal bijvoorbeeld een spreekkamer kunnen worden voorzien van een eenvoudig mechanisch slot en zal de ICT ruimte worden voorzien van een biometrielezer en misschien wel een camera. Het type toegangsmiddelen hoort dus in overeenstemming te zijn met de zonering en het risico.

Het autorisatie proces dient zo te zijn ingericht dat sprake is van doelbinding zoals (ICT)-Beheer, BHV, GBA, PUN voor speciale ruimtes. Een andere verplichting uit de baseline is dat beveiligingspersoneel toezicht houdt op de toegang van de zones en hiervan een registratie bijhoudt. Verder dient de toegangsbeveiliging zo te zijn ingericht dat ongeautoriseerden alleen onder begeleiding van bevoegd personeel en als er een noodzaak is toegang krijgen tot de beveiligde zones.

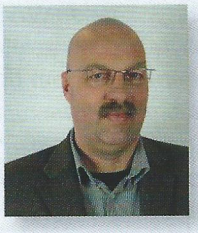
Risico zones

In veel gemeentelijke gebouwen zijn er zones met een verhoogd risico op bijvoorbeeld geweld en agressie. Daarbij moet worden gedacht aan wacht- en spreekkamers en de ruimtes waar bezoekers in contact komen met gemeente ambtenaren. In deze zone behoren zogenaamde overval alarmknoppen te zijn geplaatst. Deze knoppen geven na het indrukken een direct alarm bij de aanwezige beveiligers.

Omdat de gebouwen 's avonds, 's nachts en in de weekenden gesloten zijn dienen de gebouwen voorzien te zijn van een inbraakdetectiesysteem dat gekoppeld is aan een alarmcentrale. Uitgangspunt van de baseline is dat er 24 uur, 7 dagen per week bewaking is en dat de inbraakdetectie gekoppeld is aan een particuliere alarmcentrale. Uiteraard dienen er dan afspraken gemaakt te worden over alarm opvolging, aanrijroutes en follow-up door politie. Verder dient ook het gehele stelsel van organisatorische maatregelen te zijn ingericht. Onderdeel daarvan is onder andere de procedure wat te doen bij een overval. Ten slotte gaat de baseline er vanuit dat gemeente voor haar terreinen, gebouwen en beveiligde ruimtes gebruik maakt van cameratoezicht.

Wat moet ik er mee?

Als informatiebeveiliger kun je je afvragen wat moet ik hier nu mee? Veel technieken die gebruikt worden binnen de fysieke beveiliging zijn op IT-technologie gebaseerd. De integratie tussen fysieke beveiligingssystemen en IT neemt komende jaren alleen maar toe. Denk bijvoorbeeld aan IP camera's of intercoms met daarop een app. Maar ook nu al zijn veel toegangscontrole systemen uitgerust met een server met daarop een applicatie die onder andere de deurcontroles aanstuurt. Ook camera systemen zijn vaak gewoon een server met daarop een applicatie en daaraan een IP netwerk met IP camera's. Kortom je kunt bijna alle IT beveiligingsaspecten uit de baseline los laten op de techniek die bij fysieke beveiliging wordt gebruikt. Zelfs aspecten zoals hardening, patchmanagment en antivirus kunnen allemaal worden geïmplementeerd. Kortom de fysieke beveiliging is goed in lijn te brengen met de Baseline Informatiebeveiliging Nederlandse Gemeenten.



RONALD EYGENDAAL *schrijft sinds 1990 over informatiebeveiliging, elektronische & technische beveiliging, fraudedetectie & -bestrijding, en bewaking & beveiliging voor toonaangevende vakbladen in Nederland en België*