

Beveiligingsconcept EMA 1.0

Naast de logische beveiliging van haar ICT systemen zullen er ook fysieke beveiligingsmaatregelen worden genomen. Dit concept is hier op hoofdlijnen weergegeven en zal in overleg met de gebruiker verder worden uitgewerkt om te komen tot een gebouw en organisatie specifiek concept. Doel is de bedrijfscontinuïteit te waarborgen, te zorgen voor veiligheid van medewerkers en bij te dragen aan informatiebeveiliging.

Er wordt een zoneringsmodel toegepast waarbij de gebieden zijn ingedeeld in beveiligingszones die passen bij de activiteiten die in de gebieden worden uitgevoerd. Per zone is er een vastgesteld maatregelenpakket zodat er een eenduidig en evenwichtig beveiligingsconcept ontstaat. Op basis van risico analyses en de specifieke bedrijfsvoering wordt, indien noodzakelijk, maatwerk toegepast waarbij het standaard beveiligingsconcept het vertrekpunt is. Door deze schaalbaarheid, standaard toegepast door de Nederlandse Rijksoverheid, kunnen gebouwen geschikt gemaakt worden als standaard kantooromgeving maar ook voor de huisvesting van diensten met een specifiek en hoger risico profiel.

Zone 0 is het openbare gebied. Dit gebied is algemeen en openbaar toegankelijk voor medewerkers, functionele bezoekers en publiek. Daarbij moet worden gedacht aan de openbare ruimte rondom het gebouw en de ontvangsthal bij de receptiefunctie;

Zone 1 is een beveiligd gebied zonder een openbaar karakter. Dit gebied is onder voorwaarden toegankelijk voor bezoekers maar niet vrij toegankelijk. Dit gebied is bedoeld voor activiteiten waar niet structureel vertrouwelijke informatie wordt verwerkt maar desondanks vrije toegang door derden ongewenst is. Te denken valt daarbij aan ruimtes voor ontmoeten, parkeren, vergaderen en de restaurantvoorzieningen.

Zone 2 is een beveiligd werkgebied voor de primaire bedrijfsvoering. Hier kan vertrouwelijke informatie worden verwerkt. Dit kantoorgebied is toegankelijk voor geautoriseerde medewerkers en functionele bezoekers binnen de randvoorwaarden van de bezoekersregeling. In dit gebied kunnen ook vergaderfuncties zijn voor het voeren van overleg waarbij regelmatig vertrouwelijke informatie wordt gedeeld.

Zone 3 is een extra beveiligd werkgebied voor de meest kritische bedrijfsvoering. Te denken valt aan de ICT ruimtes en ruimtes waar informatie met een hogere rubricering wordt verwerkt en opgeslagen.

Per zone worden er bouwkundige en elektronische maatregelen genomen. Aangevuld met de organisatorische beveiligingsmaatregelen ontstaat er een integraal beveiligingsconcept.

Dit concept bestaat uit:

- perimeterbeveiliging om vroegtijdig ongewenste invloeden te onderkennen en tegen te houden;
- inbraakwerende kwaliteit van de schillen van het gebouw en de zones om weerstand te bieden tegen scenario's met braak;
- beveiligde doorgangen bij de overgang tussen zones en de ingangen van het gebouw om weerstand te bieden tegen scenario's waarbij er sprake is van insluiping/ meelopen;
- CCTV systemen gericht op de omgeving, beveiligingsschillen, doorgangen, verkeersgebieden en kritische ruimtes vanwege de preventieve werking, om afwijkend gedrag vroegtijdig te onderkennen, bij incidenten te verifiëren en de interventie te ondersteunen en ten slotte vanwege de bewijslast na incidenten;
- Toegangscontrole systeem om aan de hand van autorisatieprofielen het gebouw toegankelijk te laten zijn voor de mensen die er moeten werken en tegelijk te voorkomen dat medewerkers en derden toegang krijgen tot gebieden waar ze niet mogen zijn.
- Detectie en alarmeringsystemen zodat bovenstaande scenario's en ongeoorloofde aanwezigheid vroegtijdig worden opgemerkt. Door de combinatie van detectie en alarmering, voldoende weerstand en tijdige interventie wordt er een positief beveiligingsrendement gecreëerd.
- Bovenstaande systemen worden in een meldkamer ondersteund door systemen voor onder meer deurbediening, communicatie en een overkoepelend security management systeem.