BESCHERM WAT VAN **WAARDE** IS

AVAQ
Regie in risicomanagement

Fysieke beveiliging - inrichten van cameratoezicht

BESCHERM WAT VAN WAARDE IS

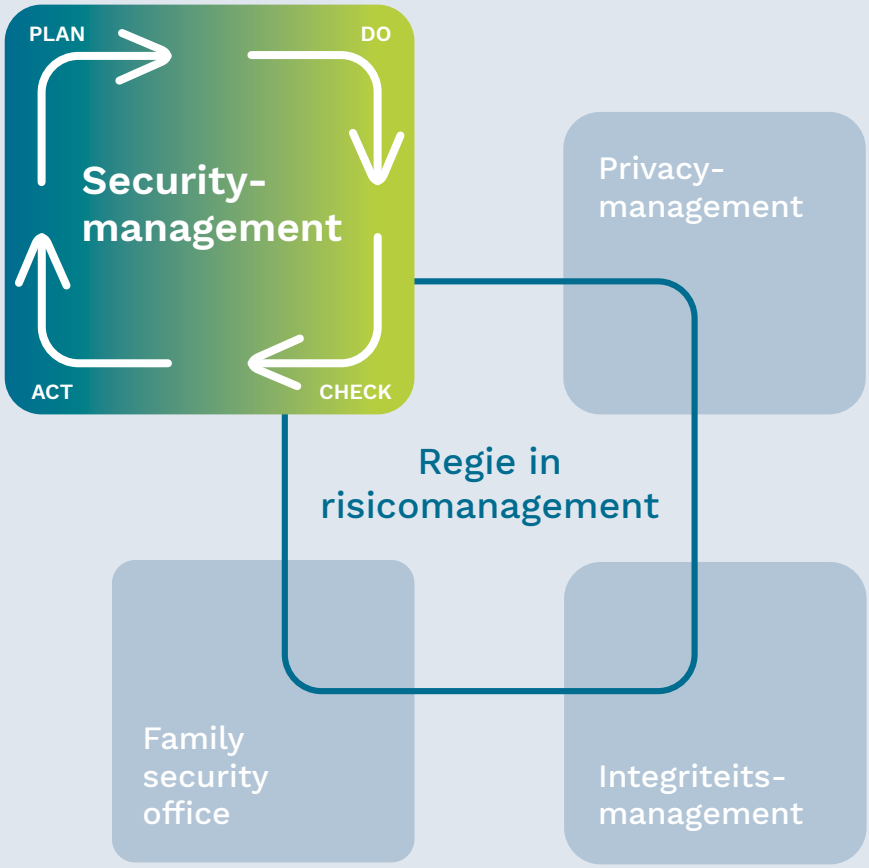
Wij beschermen personen, informatie, goederen, bedrijfsprocessen en -middelen. Dit doen we door een juiste inrichting van beveiliging, privacy en integriteit. Daarnaast beschermen we je familie tegen dreigingen. Zodat je met een gerust hart kunt leven en werken.

Om te beschermen wat van waarde is, is een integrale aanpak cruciaal (zie afbeelding 1). Beveiligingsmaatregelen en controlemechanismes hebben pas zin als duidelijk is wat en/of wie er beschermd moet worden en functioneren alleen optimaal door ze te implementeren in het proces. Bij het ophangen van beveiligingscamera's gaat dit vaak mis en dat is zonde.

Nieuwskoppen in landelijke media merken dit ook op:
'Bespied door de baas: werkgevers schenden privacy met cameratoezicht'

AVAQ ondersteunt organisaties en beveiligingsinstallateurs bij een volledige inrichting van cameratoezicht.
Onze specialisten zijn ervaren en deskundig op het gebied van security, privacy én integriteit.

AVAQ



Afbeelding 1. Inrichten van integrale beveiliging, waaronder cameratoezicht.

PLAN

Niet meer dan nodig

Van onnodige maatregelen wordt niemand beter. Het maken van een goed beveiligingsplan begint daarom met een analyse van reële dreigingen en kwetsbaarheden en inzicht in de normenkaders waaraan de maatregelen moeten voldoen. Hoe meer inzicht daarin, hoe beter je kunt beoordelen welke maatregelen voor je bedrijf zinvol en welke minder relevant zijn.

DO

Passende beveiligingsmaatregelen

Voor het adviseren en implementeren van – al dan niet verplichte – maatregelen en voor het vermijden of beperken van risico's gebruiken we verschillende methodieken. Denk aan de 'defense in depth'-strategie (meerdere verdedigingslagen in en rond een te beveiligen object of rond digitale informatie) en de INCI/DETAR-methode (tijdpadanalyse op basis van DHM®).

ACT

Bijsturen en ingrijpen

Verandert er iets in de dreigingen en/of kwetsbaarheid? Dan is het tijd om bij te sturen. Gaat er toch iets fout, bijvoorbeeld bij een datalek, fysieke dreiging of fraude, dan regisseren wij het crisismanagement. Zijn er vermoedens dat een medewerker is betrokken? Of signalen die wijzen op lekken van gevoelige bedrijfsinformatie? Dan kunnen wij een integriteitsonderzoek uitvoeren.

CHECK

Werkt het?

AVAQ ondersteunt bij het analyseren van veranderingen in de dreigingen en kwetsbaarheden en het in kaart brengen van het effect van de genomen maatregelen. Voor het monitoren en controleren kunnen we verschillende tools inzetten. Denk aan interne audits, managementreviews en intrudertests.

Beveiligingscamera's

Veel organisaties maken gebruik van beveiligingscamera's, maar lang niet iedere organisatie kan onderbouwen hoe hun beveiligingscamera's daadwerkelijk personen beschermen en gebouwen en eigendommen beveiligen of aantonen dat beveiligingscamera's echt nodig zijn. Terwijl dit waarschijnlijk wel de intentie is geweest om ze te installeren. Nog minder organisaties kunnen de privacy van betrokkenen voldoende garanderen.

Met alléén het ophangen van beveiligingscamera's – en dus het ontbreken van een volledige en adequate inrichting van cameratoezicht - ontstaan er mogelijk meer risico's dan dat je risico's aanpakt. Risico's die kunnen ontstaan zijn onder andere het niet voldoen aan het arbeidsrecht, de AVG, een datalek, imagoschade, onbruikbaar bewijs na een incident of strafrechtelijk voorval en sancties van de toezichthouder.

Inrichten van cameratoezicht

Het vertrekpunt voor de inrichting van cameratoezicht is:

- Aantonen dat het echt nodig is (noodzakelijkheid). Hiervoor moet dus duidelijk zijn wat er beschermd moet worden (personen, informatie, materieel, goederen, etc.), waarmee ook de doeltreffendheid en het gerechtvaardigd belang inzichtelijk worden;

- Afwegen van belangen en rechten van betrokkenen ten opzichte van het belang van de organisatie (proportionaliteit);

- Het uitsluiten van (minder ingrijpende) alternatieven (subsidiariteit);

- Uitvoeren privacytoets (DPIA);

Dit zijn niet alleen wettelijke vereisten, je beveiligingsplan wordt er daadwerkelijk beter van.

Om cameratoezicht te kunnen verantwoorden moet je beveiligingsplan aantoonbaar bestaan uit een combinatie van organisatorische, bouwkundige en elektronische maatregelen *(zie afbeelding 1).*

"GOEDE TECHNISCHE BEVEILIGINGSMAATREGELEN ZIJN ZINLOOS ÉN ZELFS RISICO VERHOGEND ZONDER DE JUISTE ORGANISATORISCHE MAATREGELEN."

“HET INRICHTEN VAN CAMERATOEZICHT BETEKENT MEER DAN “ALLEEN” HET OPHANGEN VAN BEVEILIGINGSCAMERA’S.”

Camerareglement

In een camerareglement worden alle onderdelen met betrekking tot cameratoezicht uiteengezet voor de organisatie. Hierin staan ten minste de volgende onderdelen:

- De verwerkingsverantwoordelijke;
- De grondslag en het doel;
- De noodzakelijkheid en toepassing;
- Heimelijk cameratoezicht;
- Privacytoets (DPIA);
- Toelichting beveiligingsmaatregelen;
- De posities van de camera’s;
- Systeem en opslag (bewaartermijn);
- Verantwoordelijkheid en autorisaties;
- Contactgegevens betrokken installateurs;
- Borging;
- Wijze van informeren medewerkers en bezoekers (kennisgeving en informatieplicht);
- Inzage en uitgifte aan derden;
- De rechten van medewerkers en bezoekers (betrokkenen);

Uitvoeren privacytoets (DPIA)

Een privacy impact assessment (privacytoets) is verplicht als een organisatie structureel of gedurende een langere periode beveiligings-camera's inzet.

Doormiddel van een DPIA wordt getoetst of de organisatie (verwerkingsverantwoordelijke) voldoet aan de uitgangs-punten en wettelijke normen (zoals eerder genoemd).

Een goed uitgevoerde DPIA geeft inzicht in de risico's die de verwerking (van persoonsgegevens, in dit geval door cameratoezicht) oplevert voor betrokkenen (medewerkers en bezoekers). Deze risico's dienen vervolgens afgedekt te worden door passende maatregelen. Veelal gaat dit over één van de onderdelen uit het camerareglement.

Bij veranderingen van bijvoorbeeld gegevensverwerking en/ of systemen moet een PIA opnieuw worden uitgevoerd.

Instemming OR

Een ondernemingsraad (OR) heeft instemmingsrecht (conform Wet op de ondernemingsraden) indien de organisatie beveiligingscamera's wil inzetten op de werkplek. Een volledige en adequate inrichting van cameratoezicht zorgt ervoor dat een OR ook kan instemmen. AVAQ ondersteunt organisaties hierbij.

Overige documenten

Cameratoezicht is gerelateerd aan allerlei andere processen die je als organisatie ingeregeld wilt hebben (conform wet- en regelgeving, maar ook om te beschermen wat van waarde is). Denk hierbij aan:

- Verwerkingsregister (privacymanagement);
- Bedrijfsreglement en integriteitsonderzoek (integriteitsmanagement).

Werkwijze AVAQ

Benieuwd of jouw organisatie cameratoezicht volledig en adequaat heeft ingericht?

Laat het toetsen door AVAQ.
Onze toetsing bestaat uit:

- Documentonderzoek;
- Technische beoordeling systeem;
- Schouw op locatie;
- Rapportage met vaststellingen (kwetsbaarheden) en actiepunten.

Bij deze toetsing beoordelen we bijvoorbeeld ook of de beelden adequaat veiliggesteld kunnen worden ten behoeve van onderzoek bij misstanden (bedrijfsrecherche).

In geval van gebreken kunnen onze consultants ondersteunen bij het uitvoeren van de actiepunten.

Ben je beveiligingsinstallateur en wil je cameratoezicht volledig inrichten bij je klant?

AVAQ werkt graag samen met beveiligingsinstallateurs. Samen kunnen we ervoor zorgen dat de beveiligingscamera's écht beschermen wat waarde is.

Contact

+31(0)85 0825 580 | info@avaq.eu | www.avaq.eu
Gevestigd in Dronten, Zwolle en Brasschaat (BE)

Voor meer info over AVAQ, kijk op de website avaq.eu of scan de QR code.