NULMETING INFORMATIEBEVEILIGING

INZICHT IN DREIGINGEN, RISICO'S EN MAATREGELEN

Een nulmeting is een beoordeling van de huidige staat van informatiebeveiliging en risico's van uw organisatie. Het doel van de nulmeting is om inzicht te krijgen in de huidige situatie, zodat er gerichte maatregelen genomen kunnen worden om de informatiebeveiliging te verbeteren.

WAAROM EEN NULMETING?

Een nulmeting is belangrijk om een startpunt te creëren voor het inzichtelijk maken en vervolgens verbeteren van de beveiliging van uw organisatie.

Zwakke plekken worden geïdentificeerd en de effectiviteit van bestaande beveiligingsmaatregelen wordt beoordeeld. De uitkomst van de nulmeting biedt een basis voor het opstellen van een ICT-beveiligingsbeleid voor verbetering van informatiebeveiliging.

Ten slotte kan een nulmeting helpen bij het voldoen aan regelgeving en het aantonen van naleving van beveiligingsvereisten. Het uitvoeren van een nulmeting informatiebeveiliging is een belangrijke eerste stap om de beveiliging van de informatie binnen uw organisatie te verbeteren.

WAT DOEN WE?

BIJ HET UITVOEREN VAN EEN NULMETING INFORMATIEBEVEILIGING DOORLOPEN WE DE VOLGENDE STAPPEN:

Inventariseren van het informatiesysteem
We brengen alle systemen en processen in kaart waarop informatie wordt verwerkt, opgeslagen of uitgewisseld.

Identificeren van de risico's
We bepalen de mogelijke bedreigingen voor de informatie en de gevolgen daarvan.

Beoordelen van de huidige beveiligingsmaatregelen
We onderzoeken de bestaande beveiligingsmaatregelen, zoals toegangscontrole, back-up, authenticatie en encryptie, beveiliging van gebruikte (cloud-)applicaties en beoordelen of deze effectief zijn.

Analyseren van de gap
We vergelijken de beveiligingsmaatregelen met de huidige standaarden en best practices op het gebied van informatiebeveiliging en analyseren waar er mogelijkheden zijn voor verbetering.

Opstellen van een rapportage en optioneel ICT-beleid
We rapporteren onze bevindingen en geven aanbevelingen voor verbetering op basis van de prioriteiten en risico's. Optioneel zetten we hierbij een aansluitend ICT-beleid op. Gedocumenteerd beleid en procedures zijn belangrijk voor uw medewerkers om een duidelijk kader te hebben waarbinnen zij hun werk kunnen en mogen doen.

DE DRIE GROOTSTE VOORDELEN VAN EEN NULMETING

Identificatie van kwetsbaarheden
Bij een nulmeting worden kwetsbaarheden in de informatiebeveiliging van de organisatie geïdentificeerd. Dit biedt de mogelijkheid om tijdig maatregelen te nemen om de beveiliging te verbeteren en de kans op incidenten te minimaliseren.

Advies van professionals
U krijgt gedegen advies van een professional. Op basis hiervan kunt u bewuste keuzes maken om de beveiliging aan te scherpen of risico's te accepteren.

Voldoen aan wet- en regelgeving
Door een nulmeting uit te voeren en maatregelen te nemen, kunt u aantoonbaar voldoen aan de voor uw organisatie geldende wet- en regelgeving op het gebied van informatiebeveiliging en kunt u mogelijke boetes of reputatieschade voorkomen.