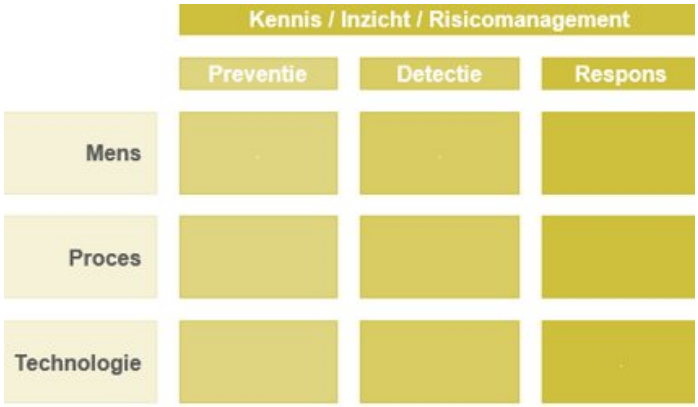
VAN OERS
it advies

CYBERSECURITY ASSESSMENT

Met een cybersecurity assessment kunt u de beveiligingsmaatregelen en -processen van uw organisatie evalueren en kwetsbaarheden, risico's en zwakke punten in het cybersecuritybeleid en de implementatie ervan identificeren. U verkrijgt hiermee inzicht in de volwassenheid van (informatie)beveiliging binnen uw organisatie en de verbeteringen die gedaan kunnen worden om potentiële bedreigingen te elimineren. Het assessment dient tevens als een goede nulmeting op basis waarvan u ow volgende stappen kunt bepalen.

9-VLAKSMODEL

Voor het uitvoeren van een cybersecurity assessment kan gebruik gemaakt worden van het 9-vlaksmodel. Dit model verdeelt cybersecurity in negen verschillende vlakken, elk met zijn eigen focusgebied. Het beoordeelt cybersecurity op basis van drie belangrijke aspecten: mens, proces & techniek en vanuit drie invalshoeken: preventie, detectie & respons.



Figuur 1. Het 9-vlaksmodel

Mens

Met mens worden medewerkers bedoeld die betrokken zijn bij het beveiligingsproces, dit kunnens managers zijn maar ook de werknemers op de vloer. Hieronder een aantal voorbeelden van de maatregelen die u per invalshoek kunt beoordelen:

- Preventief: wachtwoordbeleid, toegangsbeheer & awareness campagnes.
- Detectie: Logboekregistratie en phishing-incidentmeldingen.
- Respons: Datalekbeheer en herstelprocedures.

Proces

Onder proces vallen de beveiligingsprocessen en -procedures binnen de organisatie. Hierbij kunt u denken aan het volgende:

- Preventie: autorisatiebeheerprocedure en patchmanagement.
- Detectie: Intrusion Detection Systemen (IDS), security monitoring en Endpoint Detection and Response (EDR)
- Respons: Incident Response Plan (IRP), Forensisch onderzoek, communicatie, rapportage, evaluatie en analyse van incidenten.

Technologie

Alle technologische componenten die betrokken zijn bij de IT-infrastructuur van de organisatie, zoals servers, netwerken, endpoints en cloudservices. Voer kwetsbaahreidsscans uit om potentiële zwakke plekken te identificeren, beoordeel de beveiligingsconfiguratie van systemen en applicaties en evalueer de gebruikte beveiligingstools en -oplossingen (firewalls, antivirussoftware etc.).

HOE VOERT U EEN CYBERSECURITY ASSESSEMENT UIT MET HET 9-VLAKSMODEL?

Om een cybersecurity assessment uit te voeren wordt een stappenplan doorlopen. Op de volgende pagina volgt een uitleg van dit stappenplan.

1. Analyseer bevindingen

Breng alle verzamelde gegevens per aspect en invalshoek samen en analyseer ze om zwakke punten te identificeren. Maak een overzicht en geef hierbij per punt de urgentie voor verandering aan op basis van de potentiële impact en de waarschijnlijkheid van een aanval.

2. Opstellen van verbeteringsplannen

Ontwikkel verbeteringsplannen voor elk aspect (mens, proces en techniek). Stel doelen en actiepunten op om de beveiliging te versterken op basis van de bevindingen van de analyse en wijs een verantwoordelijke voor het implementeren van de verschillende verbeteringen.

3. Implementatie

Voer de verbeteringen door in overeenstemming met de opgestelde plannen. Zorg er daarnaast voor dat alle medewerkers getraind worden om eventuele veranderingen in beleid of procedures te begrijpen en op te volgen.

4. Monitoring

Stel continue monitoring in om de effectiviteit van de genomen maatregelen te beoordelen. Houd de beveiligingsomgeving up-to-date en reageer op nieuwe bedreigingen en kwetsbaarheden.

5. Herhaal het assessment

Voer periodiek (bijvoorbeeld jaarlijks) het cybersecurity assessment uit om te controleren of de verbeteringen hun vruchten afwerpen en om nieuwe bedreigingen aan te pakken.

6. Rapportage en communicatie

Communiceer de bevindingen en voortgang aan het management en relevante belanghebbenden binnen de organisatie. Blijf hierbij transparant over de status van cybersecurity in de organisatie.

BELANG VAN EEN CYBERSECURITY ASSESSMENT

Wanneer er in uw organisatie regelmatig een cybersecurity assessment wordt uitgevoerd met behulp van het 9-vlaksmodel, zorgt u ervoor dat de beveiligingsmaatregelen up-to-date blijft en kunt u de organisatie beter beschermen tegen potentiële cyberdreigingen.

VAN OERS IT ADVIES ONDERSTEUNT BIJ CYBERSECURITY ASSESMENTS

Onze IT & cybersecurityconsultants zijn gespecialiseerd in het uitvoeren van cybersecurity assessments met behulp van het 9-vlaksmodel. Voor de begeleiding van een cybersecurity assessment bieden wij verschillende pakketten aan, zo is er altijd een pakket dat past bij de behoeften en wensen van uw organisatie.

Meer informatie

Wilt u meer weten over het cybersecurity assessment of over de mogelijkheden? Neem dan contact met ons op:

Brechtje Brugman-Dekkers
Manager IT Advies
E. B.Brugman@vanoers.nl
T. +31 (0)6 82 04 64 65