VAN OERS
it advies

CYBERSECURITY VOLWASSENHEIDSMODEL

Cybersecurity is een van de grote en urgente uitdagingen waar organisaties vandaag de dag mee geconfronteerd worden. Het voortdurend evoluerende landschap vereist een proactieve aanpak om de risico's te beheren en de digitale activa van een organisatie te beschermen. Het Cybersecurity Volwassenheidsmodel is een raamwerk waarmee u de cybersecurity-capaciteiten van uw organisatie kunt monitoren, evalueren, en verbeteren.

HET BELANG VAN EEN CYBERSECURITY VOLWASSENHEIDSMODEL

Organisaties worden dagelijks geconfronteerd met geavanceerde cyberdreigingen die variëren van malware-aanvallen en phishing-pogingen tot datalekken en ransomware-aanvallen. Het is van vitaal belang dat organisaties niet alleen reactief, maar ook proactief zijn in het beschermen van hun digitale activa. Een volwassenheidsmodel voor cybersecurity biedt een gestructureerde aanpak om de cybersecuritycapaciteiten van een organisatie te begrijpen en te verbeteren.

HET CYBERSECURITY VOLWASSENHEIDSMODEL

In het Cybersecurity Volwassenheidsmodel wordt een reeks volwassenheidsniveaus omschreven, van onvolwassen (niveau 1) tot volwassen (niveau 5). Elk niveau vertegenwoordigt een bepaalde cybersecurityvolwassenheid en bestaat uit verschillende domeinen die de belangrijkste aspecten van cybersecurity omvatten: mens, proces en techniek. Figuur 1 omvat het volwassenheidsmodel, we geven u hieronder een korte samenvatting van de vijf niveaus.

Niveau 1: Initieel

- Cybersecurity-inspanningen zijn ongeorganiseerd en reactief.
- Er is geen duidelijk cybersecuritybeleid.
- Beveiligingsmaatregelen zijn fragmentarisch en inconsistent.

Niveau 2: Herhaalbaar

- Er is een basisstructuur voor cybersecurity ingevoerd.
- Beleid en procedures zijn gedeeltelijk gedocumenteerd.
- Incident response processen zijn aanwezig maar nog niet geoptimaliseerd.

Niveau 3: Gedefinieerd

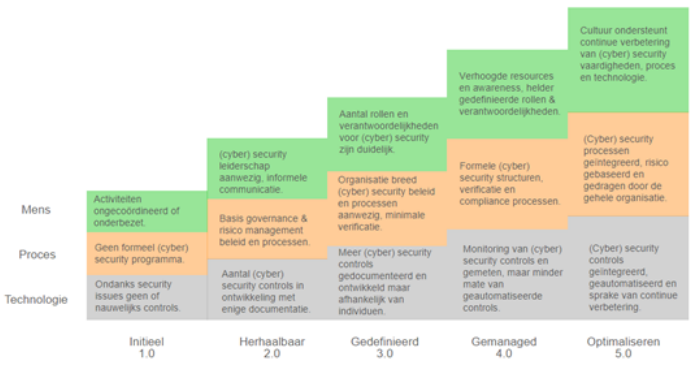
- Cybersecurityprocessen en -procedures zijn goed gedefinieerd.
- Er is een formeel incident response team.
- Beleid wordt actief gehandhaafd en bijgewerkt.

Niveau 4: Gemanaged

- Proactieve monitoring en dreigingsdetectie zijn geïmplementeerd.
- Risicobeheer en compliance worden actief gevolgd.
- Er is betrokkenheid op directieniveau in cybersecurity.

Niveau 5: Optimaliseren

- Cybersecurity wordt beschouwd als een integraal onderdeel van de bedrijfsstrategie.
- Continue verbetering is ingebed in alle aspecten van cybersecurity.
- Er is een cultuur van cybersecurity bewustzijn in de hele organisatie.



Figuur 1. Cybersecurity Volwassenheidsmodel

HOE GEBRUIKT U HET MODEL VOOR EEN EFFECTIEVE CYBERSECURITYSTRATEGIE?

Het ontwikkelen van een effectieve cybersecuritystrategie is nauw verbonden met het gebruik van het Cybersecurity Volwassenheidsmodel en kan als volgt worden toegepast:

Evaluatie met behulp van een effectieve strategie

Begin met het beoordelen van de huidige staat van uw organisatie met betrekking tot cybersecurity met behulp van het Cybersecurity Volwassenheidsmodel. Identificeer op welk volwassenheidsniveau uw organisatie zich momenteel bevindt in verschillende domeinen van cybersecurity, zoals beleidsontwikkeling, technologische maatregelen, training, en incidentresponse.

Doelstelliingen bepalen op basus van de evaluatie

Op basis van de resultaten van de evaluatie, kunt u duidelijke doelstellingen voor elk domein vaststellen. Deze doelen moeten gericht zijn op het verhogen van het cybersecurity volwassenheidsniveau van uw organisatie in zwakkere domeinen. Prioriteer de doelstellingen op basis van het risico dat ze vertegenwoordigen en de impact op uw organisatie.

Ontwikkeling van een cybersecuritystrategie

Gebruik de vastgestelde doelstellingen als leidraad voor de ontwikkeling van uw cybersecuritystrategie. De strategie moet beschrijven hoe uw organisatie de stap kan maken van het huidige volwassenheidsniveau naar het gewenste niveau. In de strategie moeten elementen zoals beleidsontwikkeling, technologische implementaties, training en bewustzijn, en incident response planning worden opgenomen.

Implementatie

Heeft u uw cybersecuritystrategie ontwikkeld? Begin dan met de implementatie van de voorgestelde maatregelen en activiteiten. Dit kan betrekking hebben op het verbeteren van de beleids-documentatie, het investeren in nieuwe beveiligings-technologieën, het opleiden van medewerkers en het opzetten van een incident response plan. Zorg dat er voldoende middelen beschikbaar zijn om de strategie uit te voeren.

Monitoring en aanpassing

Voer continue monitoring uit om de voortgang te volgen en ervoor te zorgen dat de implementatie in lijn is met uw strategie. Stel indicatoren voor cybersecurityvolwassenheid op en meet regelmatig de voortgang om te bepalen of u op de goede weg bent om uw doelen te bereiken. Pas de strategie aan op basis van nieuwe dreigingen, technologische veranderingen en lessen geleerd uit incidenten.

Borging van de cultuur

Een belangrijk aspect van zowel het Cybersecurity Volwassenheidsmodel als de cybersecuritystrategie is het behouden van een cybersecuritybewuste cultuur binnen uw organisatie. Zorg ervoor dat alle medewerkers begrijpen hoe hun acties bijdragen aan de veiligheid van de organisatie. Investeer in voortdurende training en bewustwordingsinitiatieven om deze cultuur te versterken.

Het Cybersecurity Volwassenheidsmodel dient als een raamwerk om uw huidige stand van zaken te begrijpen en de strategie helpt u bij het plannen en implementeren van maatregelen om uw cybersecuritycapaciteiten te verbeteren. Samen vormen ze een krachtige aanpak om uw organisatie te beschermen tegen cyberdreigingen en de volwassenheid van uw cybersecurityprogramma te verhogen.

CONCLUSIE

Het Cybersecurity Volwassenheidsmodel is een waardevol hulpmiddel voor organisaties om hun cybersecuritycapaciteiten te begrijpen en te versterken. Door dit model te gebruiken, kunnen organisaties proactief reageren op de steeds veranderende cybersecuritylandschap en hun digitale activa effectiever beschermen. Het is essentieel dat organisaties zich inzetten voor een hoge cybersecurityvolwassenheid op alle niveaus om een solide verdediging tegen cyberdreigingen te bieden.

Meer informatie

Wilt u weten hoe u dit model in uw organisatie kunt implementeren en gebruiken binnen uw strategie? Neem contact op met één van onze specialisten:

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