Secura
A BUREAU VERITAS COMPANY

Security Maturity Assessment

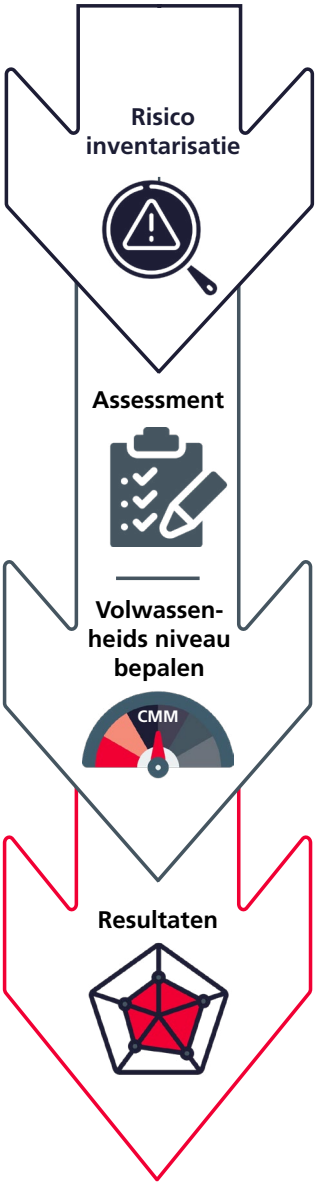
Cybersecurityrisico's nemen sterk toe: complexe digitale aanvallen komen steeds vaker voor. Een belangrijke factor is de professionalisering van cybercriminelen en onze afhankelijkheid van digitale middelen en data. Een hack, datalek of in het slechtste geval een **ransomware-aanval** kunnen een enorme impact hebben op uw bedrijfscontinuïteit. De gevolgen variëren van reputatieschade, boetes en verlies van waardevolle en gevoelige data tot het herstellen van de bedrijfsvoering, met alle kosten van dien. Problemen met de digitale infrastructuur kunnen een bedrijf zelfs fataal worden. **Hoe bepaalt u of uw organisatie weerbaar is tegen deze cybersecurityrisico's?**

De noodzaak van cybersecurity

De afgelopen tien jaar zijn cyberaanvallen niet alleen een dagelijkse, maar ook een existentiële bedreiging geworden voor bedrijven. Veel bedrijven hebben geen compleet inzicht in de staat van hun digitale veiligheid, de mate van volwassenheid van hun informatiebeveiliging en de cyberweerbaarheid van de organisatie. 'Hoe veilig zijn we?' is een vraag die zonder dit inzicht moeilijk te beantwoorden is. Daarnaast is het zonder dit inzicht moeilijk om structureel werken aan het verkleinen van digitale risico's.

Om organisaties meer inzicht te geven in hun digitale veiligheid heeft Secura het **Security Maturity Assessment** (SMA) ontwikkeld. Het SMA helpt uw organisatie te bepalen hoe volwassen deze is op het gebied van informatiebeveiliging. Daarnaast identificeert het assessment beveiligingsrisico's en verbeterpunten. Tot slot monitort het de voortgang op deze gebieden. Het SMA omvat de drie belangrijkste pijlers van cyberbeveiliging: **mens, proces en technologie.** Omdat het SMA gebaseerd is op **(inter)nationale standaarden en kaders**, kunt u de volwassenheid van de informatiebeveiliging van uw eigen organisatie op een betrouwbare manier vergelijken met die van andere organisaties.

Zo werkt een SMA



KENNISMAKING

Om u het beste van dienst te zijn, is het van belang dat onze consultants uw organisatie goed leren kennen. In deze fase bekijken en bepalen wij bedrijfsgrootte, doelen, complexiteit en de scope van het assessment. Met een **op maat gemaakte risk inventory**, of risico-inventarisatie, brengen wij de belangrijkste risico's van uw organisatie in kaart. Afhankelijk van de doelstellingen van de organisatie doen wij dit ofwel met een top-down aanpak (meer algemeen), ofwel bottom-up (meer gedetailleerd). Deze informatie gebruiken wij om weging toe te kennen aan bepaalde beheersmaatregelen of hoofdstukken.

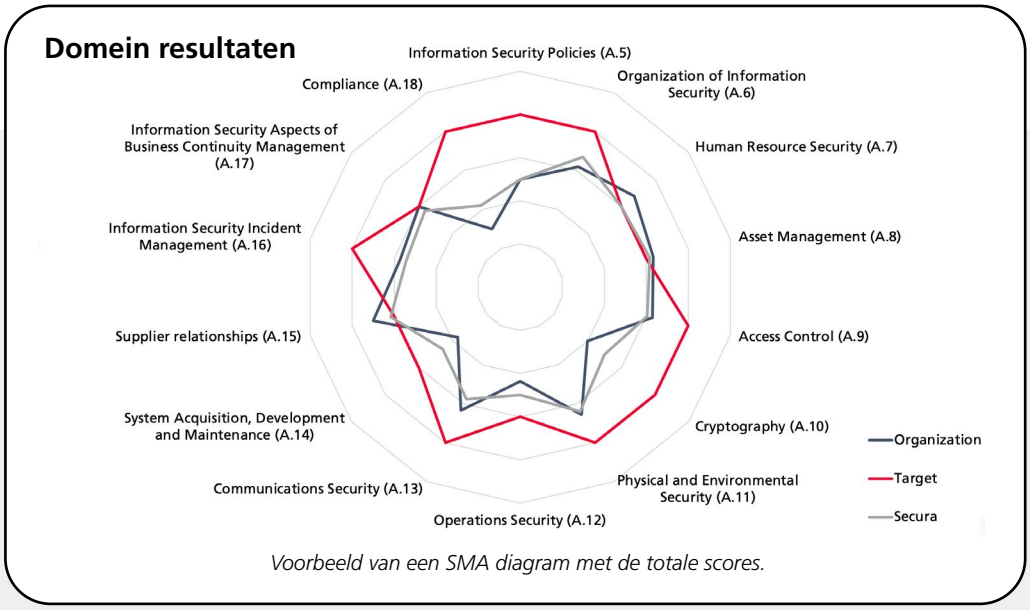
Als u wilt kunt u met hulp van een Secura consultant een **zelfevaluatie** doen, volgens de gekozen norm of standaard. Secura vergelijkt de resultaten van uw zelfevaluatie in een later stadium van het SMA met de eigen bevindingen. Zo komt u erachter hoe goed u uw eigen informatiebeveiliging doorgrondt.

UITVOERING

Het is van belang om de volwassenheid van uw organisatie gestructureerd te beoordelen, zodat de beoordeling herhaalbaar is. Daarom gebruiken wij **verschillende (inter)nationale kaders** (zie onderaan van pagina 3 voor een lijst van deze kaders) om de **opzet, het bestaan en de werking** van de beheersmaatregelen te controleren. Met hulp van deze kaders kennen wij een van de vijf volwassenheidsniveaus toe aan de verschillende beheersmaatregelen van uw organisatie. Deze niveaus zijn gebaseerd op het **Capability Maturity Model (CMM)**. De adviseur zal in eerste instantie gebruik maken van de documentatie die u geleverd hebt. Als er meer informatie is vereist, zullen wij extra documenten opvragen en relevante personen interviewen.

RESULTATEN

Na afloop van het assessment ontvangt u een rapport en de SMA-tool. Daarin staan de resultaten van de optionele zelfevaluatie en de volwassenheid die Secura heeft vastgesteld. Het rapport bevat allereerst een managementsamenvatting. Die beschrijft de belangrijkste bevindingen, de hiaten in relatie tot de gewenste volwassenheid en een totaalscore. De rest van het rapport gaat in op de details van onze bevindingen. Zowel het rapport als de tool bevatten dashboards. Die geven u duidelijk inzicht in de volwassenheid van de informatiebeveiliging van uw organisatie. Als u dat wilt kan de consultant een plan van aanpak opstellen om uw volwassenheid naar een hoger niveau te brengen.



Voorbeeld van een SMA diagram met de totale scores.

Verschillende soorten SMA's

Onze aanpak bij een SMA kent drie niveaus: de Security Workshop, de Security Maturity Review en het Security Maturity Audit. Sowieso start ieder assessment met een workshop om de organisatie te leren kennen. Afhankelijk van uw wensen kunnen we dit uitbreiden tot een review of volledige audit. Een volledige risicoanalyse en het maken van een plan van aanpak na het assessment zijn optionele extra's.

SECURITY **WORKSHOP** 1 DAG

Tijdens deze workshop bekijken en bepalen onze experts de bedrijfsgrootte, doelen, complexiteit en de scope van het assessment. Wij voeren een **quick scan** uit op basis van de gekozen standaard of norm. Dat doen we door een halve dag interviews af te nemen belangrijke documentatie te lezen. Daarna kunnen wij een **eerste inschatting geven van het volwassenheidsniveau van de beveiliging**. Het resultaat van de workshop is een beknopt rapport met aanbevelingen.

SECURITY MATURITY **REVIEW** 2-10 DAGEN

Na de workshop kunnen een maturity review uitvoeren. Onze **deskundigen beoordelen de volwassenheid** van uw organisatie via een diepgaande documentatie-review en interviews. Deze bevindingen kunnen wij, als u dat wilt, vergelijken met een zelfevaluatie. Wij bepalen de volwassenheid van uw organisatie **op basis van de vijf CMM-volwassenheidsniveaus**, naar maatstaven die wij hebben vastgesteld voor elke beheersmaatregel. Met uw hulp controleren wij steekproefsgewijs ook de kwaliteit van de **operationele effectiviteit**. Het resultaat van de review is een rapport en SMA-tool. Deze bevatten de bevindingen en de details van de review, evenals dashboards die de resultaten visualiseren.

SECURITY MATURITY **AUDIT** 10-20 DAGEN

In plaats van een review kunnen we na de workshop ook een volledige audit uitvoeren. Het proces is grotendeels gelijk, maar **wij verifiëren de kwaliteit van de operationele effectiviteit nog grondiger**. Ook besteden we meer tijd aan het verifiëren van de volwassenheid van de verschillende beheersmaatregelen. Dat betekent dat dit assessment ideaal is voor grotere organisaties of organisaties die al een hoog volwassenheidsniveau hebben.

OPTIONEEL: RISICO ASSESSMENT 2-5 DAGEN

Het SMA start met een risico assessment volgens de ISO/IEC 27005:2018 norm.

OPTIONEEL: PLAN VOOR VERBETERING 2-5 DAGEN

Na afloop van het assessment stellen wij een lijst op van concrete actiepunten en prioriteiten.

Het SMA volgt standard de volgende normenkaders. In overleg is een op maat gemaakt assessment ook mogelijk.

- ISO/IEC 27001 (2013 en 2022)
- NIST Cyber Security Framework (CSF)
- NIST CSF – Ransomware Resilience (RR)
- IEC62443 voor OT omgevingen
- NEN7510 voor medische omgevingen

Gerelateerde diensten

Secura's Security Maturity Assessment is ontworpen om verschillende soorten klanten uit diverse marktsegmenten direct inzicht te geven in de volwassenheid van hun informatiebeveiliging. Iedere klant staat echter voor unieke uitdagingen. Gerelateerde diensten die u kunnen helpen om uw cyberweerbaarheid te vergroten zijn:

IMPLEMENTATION SUPPORT

Naast het in kaart brengen van hiaten en risico's, kan Secura ook helpen bij het implementeren van een breed scala aan normen en kaders.

INTERNAL AUDIT

Bereidt u zich voor op certificering? Secura verzorgt interne audits. Wij evalueren en dragen mogelijke verbeteringen voor, voor de effectiviteit van uw risicobeheer, controle en governance processen.

CISO-AS-A-SERVICE

Secura's CISO-As-A-Service biedt kleine en middelgrote bedrijven de mogelijkheid om uw cyberbeveiligingsbeheer te prioriteren en uit te voeren. U wordt ondersteund door een professional zonder dat u iemand in dienst hoeft te nemen. Deze service helpt u bij het beheersen van beveiligingsuitdagingen die het gevolg zijn van het snelle en steeds veranderende risicolandschap.

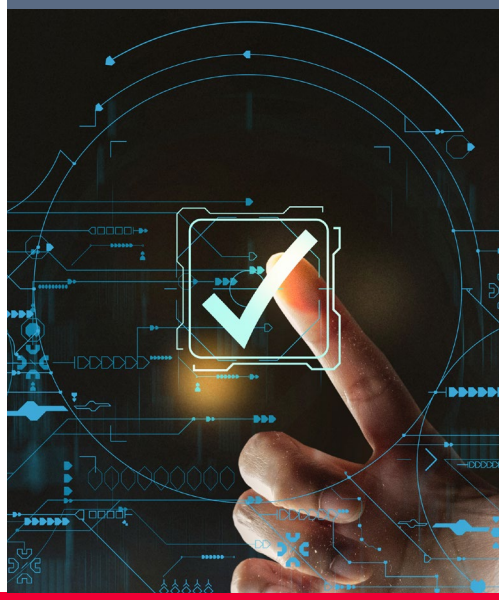
THREAT MODELING

Het SMA biedt u inzicht in de volwassenheid van de informatiebeveiliging van uw organisatie. Om de digitale veerkracht van uw netwerkarchitectuur te testen, is een Threat Modeling sessie geschikt. Deze dienst identificeert de grootste technische zwakheden in uw netwerkontwerp en geeft u concreet advies over mitigatie.

Secura
A BUREAU VERITAS COMPANY

Over Secura

Secura is een vooraanstaand expert in digitale beveiliging. Wij helpen onze klanten - van de overheids- en zorgsector tot aan de financiële en industriële sector - om hun **cyberweerbaarheid te vergroten**. U kunt van onze experts hoogwaardig beveiligingsadvies, testen, training en certificeringsdiensten verwachten. Wij geloven in een **geïntegreerde aanpak voor cybersecurity**: mensen, proces en technologie zijn even belangrijk. Sinds 2021 maakt Secura deel uit van de internationale Bureau Veritas Groep.



Secura
A BUREAU VERITAS COMPANY

Interesse?
Neem contact op via:
Volg ons op:

+31 88 888 31 00
info@secura.com
secura.com

BUREAU VERITAS
1828
Shaping a World of Trust