VERTROUWELIJK

RAPPORTAGE THREADMATURE

Thread Mature
SECURITY COMPLIANT

ALGEMENE INFORMATIE

Klant:	test partner 180724 - Own use
Partner:	test partner 180724
Datum:	28-09-2018

ThreadStone
CYBER SECURITY

ThreadStone Cyber Security B.V.
HSD Campus
Wilhelmina van Pruisenweg 104
2595 AN Den Haag
www.threadstone.eu

T: +31 (0)85 060 7000
M: info@threadstone.eu

Kvk : 614 262 02
BTW nummer: NL 85 43 36 631 B01
IBAN: NL34 RABO 0192 0442 14

ThreadStone Cyber Security kan op geen enkele manier aansprakelijkheid aanvaarden voor de gevolgen van onvolledigheid of onjuistheid van informatie en materiaal dat in dit rapport of de diensten van ThreadStone Cyber Security ter beschikking worden gesteld. Ook kan deze rapportage niet gezien worden als (bindend) advies. Het is niet mogelijk om garanties te bieden op 'compliant' zijn met de Algemene Verordening Gegevensbescherming of andere wetgeving op basis van de diensten of rapportages van ThreadStone Cyber Security.

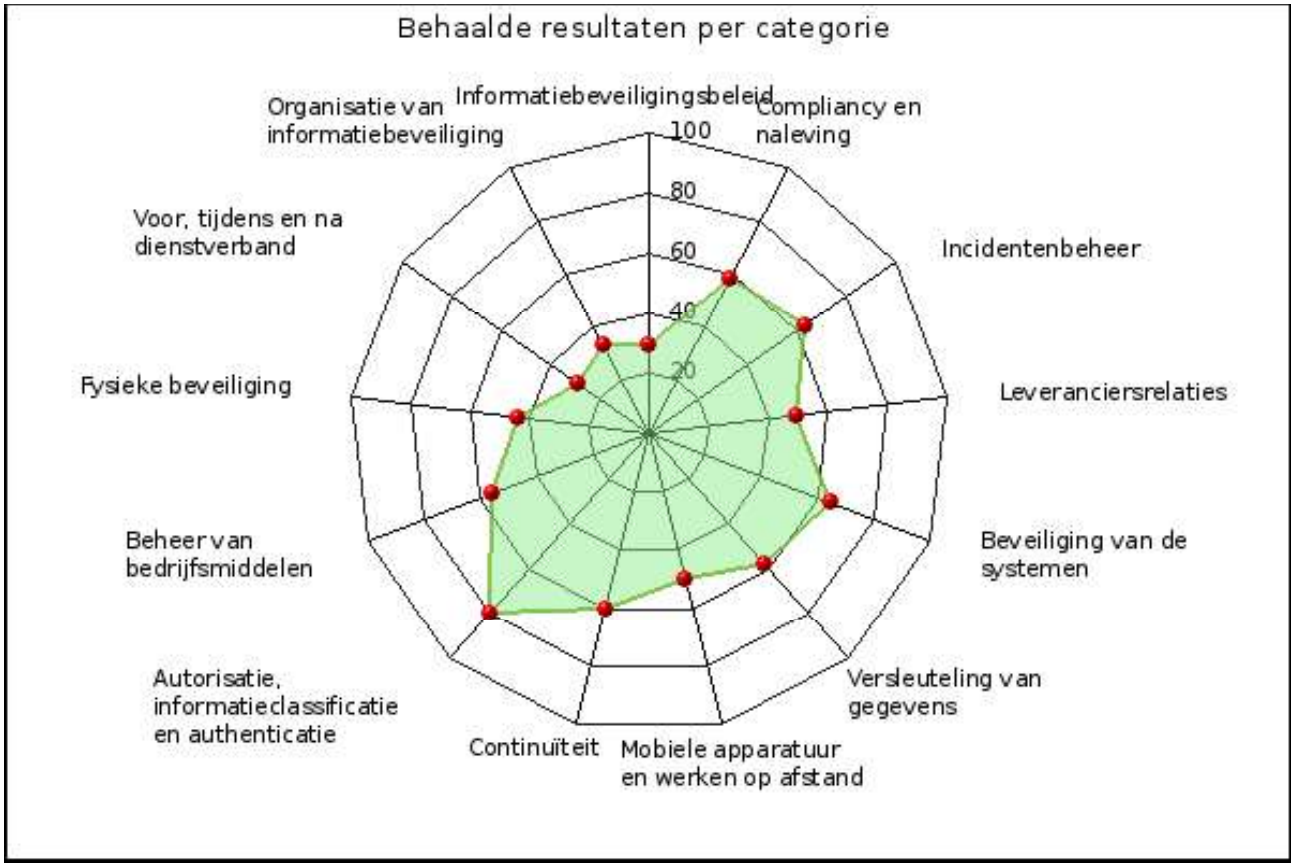
Met de diensten van ThreadStone Cyber Security wordt u mogelijk verwezen naar andere websites, rapporten en technische oplossingen die niet onder controle staan van ThreadStone Cyber Security. Wij hebben geen controle over de aard, inhoud en de beschikbaarheid van deze bronnen. Daarnaast zijn deze bronnen aan tussentijdse verandering onderhevig, waardoor bepaalde informatie mogelijk niet meer actueel of compleet kan zijn. De opname van welke informatie dan ook is niet noodzakelijkerwijs een aanbeveling of onderschrijving van standpunten die door (andere) bronnen of wetgever worden geuit en hebben slechts een informatieve strekking.

Management samenvatting 3

Uw resultaten 5

Resultaten per vraag 9

Op basis van de uitgevoerde ThreadMature assessment is onderstaande 'spinnenweb' gegenereerd. Hiermee heeft u in één visueel plaatje inzicht in waar u extra aandacht moet besteden om uw weerbaarheidsniveau te verhogen.



HET GEMIDDELDE VOLWASSENHEIDSNIVEAU VAN UW ORGANISATIE IS EEN 2,6.

De score van ThreadMature loopt van 0 (laagste score) tot 5 (hoogste score). Deze waarde houdt in dat basale maatregelen zijn gepland, geïmplementeerd en worden herhalend uitgevoerd. Zorg er voor dat de processen eenduidig worden beschreven en dat ze organisatie-breed worden geïmplementeerd.

In dit rapport worden de belangrijkste resultaten van het assessment toegelicht.

Voor de uitvoering van deze assessment hebben we gesproken met de volgende medewerkers binnen test partner 180724 - Own use.

De heer Dirk Teur - Directeur

Mevrouw An Troposoof - IT verantwoordelijke

De heer Ad Ministratie - Controller

De algemene conclusie en aanbevelingen van onze consultant zijn:

Deze organisatie met 3 vestigingen en 230 personeelsleden houdt zich bezig met het opzetten van concepten voor de gezondheidszorg. De organisatie bestaat uit de volgende afdelingen:

- directie - 3FTE

- sales - 12FTE

- marketing - 4FTE

- productie - 200 FTE

- ondersteuning en administratie - 11 FTE

Belangrijkste partners in de keten zijn de klanten (veelal ziekenhuizen). Vanuit de leverancierskant wordt veel gewerkt met onderaannemers (veelal freelancers), die worden ingehuurd via vaste bureaus.

De kroonjuwelen bestaan uit de klantdata en de nieuw opgezette concepten. Het zou zeer schadelijk zijn als deze concepten verminkt raken of in verkeerde handen komen (continuiteitsgevaar).

De systemen waarmee gewerkt wordt zijn standaard Office en een ERP systeem voor de projecten en uren. Voor de financiele administratie is een apart systeem dat wordt gebruikt. Verder worden veel kleinere pakketten gebruikt in de productieafdeling.

Belangrijkste mogelijke actoren zijn professionele criminelen (m.n. ransomware en hacks) en concurrenten die uit zijn op IP van de organisatie.

Als de organisatie > 4uur niet kan werken heeft dit grote financiÃ«le impact.

Als de gegevens van de organisatie verminkt raken, heeft dit grote financiÃ«le en immateriÃ«le impact.

Als de gegevens van de organisatie in verkeerde handen komen kan dit grote immateriÃ«le impact hebben.

De resultaten en aanbevelingen zijn per vraag vermeld in de bijlage.

Een goed informatiebeveiligingsbeleid is afhankelijk van vele factoren. Met ThreadMature ontvangt u een self-assessment (eventueel ondersteund door een consultant), waarmee u kunt bepalen welke acties u (nog) moet ondernemen om naar een hoger volwassenheidsniveau te groeien. Bij elke vraag wordt extra achtergrond informatie geboden en worden concrete adviezen en aanbevelingen gegeven.

De assessment van ThreadMature bestaat uit 79 vragen, welke zijn ingedeeld in de volgende categorieën:ën:

Categorie	Toelichting
Informatiebeveiligingsbeleid	Informatiebeveiliging start op het hoogste niveau van de organisatie. Het vastleggen en uitdragen van een informatiebeveiligingsbeleid door het hoger management/directie is daarom een belangrijk criterium.
Organisatie van informatiebeveiliging	Er wordt gekeken op welke wijze de informatiebeveiliging binnen de organisatie is georganiseerd, waarbij onder andere wordt gekeken of er duidelijke verantwoordelijkheden, taken en bevoegdheden zijn vastgelegd.
Voor, tijdens en na dienstverband	De menselijke factor blijft binnen informatiebeveiliging een essentieel onderdeel. Er wordt bekeken of medewerkers of contractors voor, tijdens en na hun dienstverband goed begrijpen wat er van hen wordt verwacht rond informatiebeveiliging.
Fysieke beveiliging	Er wordt gekeken naar de toegang tot fysieke ruimtes en apparatuur en bijvoorbeeld de omgang met bezoekers binnen uw organisatie.
Beheer van bedrijfsmiddelen	Tijdens de gehele levensduur van bedrijfsmiddelen, van in gebruik name tot verwijdering/vernietiging moet goed worden omgegaan met informatiebeveiliging.
Autorisatie, informatieclassificatie en authenticatie	Informatieclassificatie en autorisatie zijn nauw aan elkaar gekoppeld. Hebben alleen die personen toegang tot informatie die daarvoor geautoriseerd zijn? Authenticatie is het proces van controleren of de persoon die zich aanmeld ook werkelijk die persoon is.
Continuïteit	Bedrijfscontinuïteit en informatiebeveiliging zijn nauw aan elkaar verbonden. Als uw organisatie te maken zou krijgen met bijvoorbeeld een ransomware aanval, dan zult u zich moeten afvragen of u weer tijdig kunt herstellen en of er niet meer data verloren is gegaan dan gewenst.
Mobiele apparatuur en werken op afstand	Zakelijke data staat steeds vaker op mobiele apparatuur, zoals telefoons, tablets, laptops, USB sticks etc. In deze sectie wordt ingegaan op de beveiliging van deze apparatuur en het werken op afstand.

Categorie	Toelichting
Versleuteling van gegevens	Door gegevens te versleutelen zorgt u voor een extra beveliiging waardoor - ook bij inbraak in systemen of verlies van bijvoorbeeld een laptop - gegevens niet direct op straat liggen. In deze sectie wordt gekeken naar de omgang met versleuteling van gegevens.
Beveiliging van de systemen	De systemen die worden gebruikt, inclusief applicaties en data, moeten op een passend niveau worden beveiligd.
Leveranciersrelaties	Door duidelijke afspraken met leveranciers te maken rond de omgang met informatiebeveiliging voorkomt u dat ook zij zich houden aan het door u gestelde of gewenste beveiligingsniveau.
Incidentenbeheer	Het betreft hier het beleid, processen, procedures en afspraken die gelden op het moment dat zich incidenten voordoen.
Compliancy en naleving	Er is veel wetgeving die betrekking heeft op informatiebeveiliging. Dit hoofdstuk gaat in op deze wetgeving en de naleving daarop door uw organisatie.

Het model is zodanig opgezet, dat het aansluit op de werking van informatiemanagementsystemen. Denk hierbij aan het implementeren van een Plan-Do-Check-Act (PDCA) cyclus, zoals de kwaliteitsnorm ISO27001 beschrijft voor informatiebeveiliging. In dit maturity model zijn vijf niveaus van volwassenheid omschreven. Door het gebruik van het security volwassenheidsmodel kan middels een nulmeting en de gewenste ambitie de 'security roadmap' gedefinieerd worden.
Om de volwassenheid van de informatiebeveiliging van uw organisatie te bepalen en te meten, worden volwassenheidsmodeelen gebruikt. Binnen ThreadMature worden de volgende niveaus gebruikt:

Niveau (cijfer / omschrijving)		Toelichting
-	Niet van toepassing	Niet van toepassing
0	Wordt niet uitgevoerd	Er zijn geen security maatregelen of beleid aanwezig. De middelen ter controle ontbreken.
1	Gebeurt ad hoc, is in initiële fase	Maatregelen worden over het algemeen uitgevoerd op ad-hoc basis en zijn incident gedreven.
2	Is wel procesmatig aanwezig, maar niet beschreven	Basale maatregelen zijn gepland, geïmplementeerd en worden herhalend uitgevoerd.
3	Is procesmatig en beschreven	T.o.v. niveau 2 zijn de gebruikte processen meer volwassen: gedocumenteerd, eenduidig in uitvoering en organisatie-breed geïmplementeerd.
4	Is een beheerst en meetbaar proces	T.o.v. niveau 3 wordt het proces periodiek gemeten, gecontroleerd en geverifieerd (bijvoorbeeld t.b.v. audits).
5	Geoptimaliseerd proces	T.o.v. niveau 4 zijn de gedefinieerde en gestandaardiseerde processen regelmatig worden herzien en bijgewerkt en daarmee up-to-date gehouden. Verbeteringen geven inzicht in en reageren op de impact van relevante kwetsbaarheden.

Het niveau van volwassenheid voor een 'gezonde' informatiebeveiliging wordt in dit model op een minimale score van 3 beschouwd.

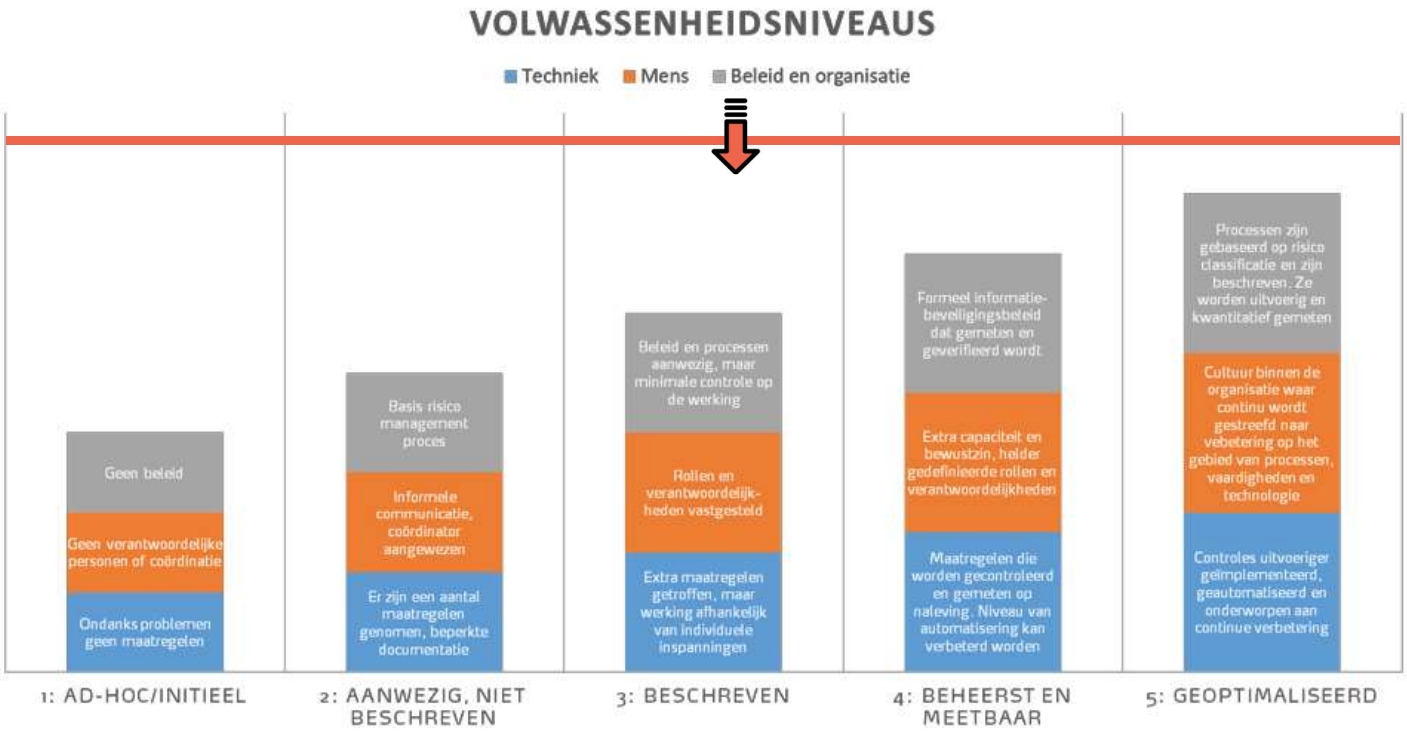
Op dit niveau zijn processen gedefinieerd en beschreven en organisatie breed geïmplementeerd.

Ons advies is om alle aanbevelingen die in dit rapport zijn vermeld door te lopen en per punt:

- Een prioriteitsstelling te geven;
- Een verantwoordelijke te bepalen;
- Een deadline te koppelen aan de acties die uitgevoerd moeten worden.

Op deze wijze kunt u naar een hoger volwassenheidsniveau groeien.

Hieronder een weergave van het maturity model. Uw organisatie bevind zich op dit moment op niveau 2.6



Op de volgende pagina's volgt per vraag de extra toelichting, het door u gegeven antwoord, het advies/aanbeveling en een extra toelichting/commentaar die bij de vraag is gegeven.

Vraag

1. Is er een beleid omtrent informatiebeveiliging dat door de directie of het management is goedgekeurd?

Antwoord

Gebeurt ad hoc, is in initiële fase

Commentaar

Er is wel iets, maar om dit een volledig informatiebeveiligingsbeleid te noemen gaat te ver.

Extra informatie

Cybersecurity heeft geen 'eindpunt', maar is een reis waarbij continue wordt gestreeft naar verdere verbetering (er is geen eindpunt). Binnen de organisatie - beter geformuleerd, vanuit de directie - zal er aandacht en commitment moeten zijn om tijd, geld en middelen ter beschikking te stellen om continue verbeteringen door te voeren. Er zal aandacht moeten zijn voor beleid (organisatie, processen, procedures), mens en techniek. De zwakste schakel bepaalt de sterkte van de beveiliging van de organisatie.

Advies

Zorg er voor dat beleid rond informatiebeveiliging en een verklaring vanuit de directie wordt opgezet, waarin wordt aangegeven dat ze zich continue inzet voor het verbeteren van de cybersecurity en zo de risico's op schade als gevolg van cybercriminaliteit wil verlagen. Daarnaast zal het management uiteraard het goede voorbeeld moeten geven t.a.v. cybersecurity!

Vraag

2. Maakt een risico beoordeling onderdeel uit van dit informatiebeveiligingsbeleid?

Antwoord

Wordt niet uitgevoerd

Extra informatie

Door eerst de risico's inzichtelijk te hebben kan er een goede beleid worden opgezet. Risico's kunnen zich voordoen op het gebied van beschikbaarheid (het continue beschikbaar hebben van processen, systemen en/of data), integriteit (zeker weten dat de data correct is) en vertrouwelijkheid (informatie alleen te verwerken door personen die daarvoor gerechtigd zijn). Dit wordt in de kwaliteitsborging ook wel ook wel BIV genoemd.

Advies

Zorg er voor dat de kroonjuwelen van de organisatie (veelal data) in kaart wordt gebracht en welke risico's hierop van toepassing (kunnen) zijn. Zet daarop een 'passend' beveiligingsbeleid en -maatregelen in. Denk bij dit beleid zowel aan de processen, de systemen als de data.