vrije universiteit *Amsterdam*
Postgraduate Opleiding
IT Audit, Compliance & Advisory

Security Operations Center (SOC):

Modelleren en meten van effectiviteit

Definitieve versie: 1.02

Vrije Universiteit, PGO ITACA

Auteurs	S. Schinagl	stef@noordbeek.com
	K.C. Schoon	keith@noordbeek.com

Status	Definitief
Datum	16 april 2014
Filenaam	Scriptie SOC 2014

Inhoud

1. Managementsamenvatting

Het onderzoek naar modelvorming voor een Security Operations Center (SOC) is uitgevoerd als een empirische studie, door middel van interviews met experts op het gebied van informatiebeveiliging, binnen meer dan tien verschillende organisaties en het bestuderen van informatie uit publiekelijk toegankelijke bronnen. Voor de onderzoeksaanpak worden de richtlijnen in het boek 'Case study research, design and methods' van Robert K. Yin benut [YIN2009]. Dit is een lineaire en iteratieve aanpak.

Regelmatig vinden binnen de overheid incidenten plaats op het gebied van informatiebeveiliging, die door de media worden uitvergroot. Incidenten vanuit de cyberwereld prikkelen de politiek, die daarna druk uitoefent op het senior management binnen de overheidsorganisaties. Het begrip 'cyberaanvallen' blijft echter te generiek en te vaag voor veel bestuurders, en is het voor hen niet concreet waartegen zij hun organisaties moeten beschermen. Dit leidt tot inefficiënte investeringen.

Het is voor iedere organisatie belangrijk om in kaart te brengen welke IT-gerelateerde objecten kunnen worden aangevallen en tegen welke dreigingen men zich daadwerkelijk moet beschermen. Binnen deze IT-gerelateerde objecten worden gegevens met een bepaalde waarde uitgewisseld, zoals financiële transacties, privacygevoelige informatie, vertrouwelijke informatie etc. Sommige gegevens hebben een lage waarde, terwijl andere gegevens een hoge waarde kunnen vertegenwoordigen. De informatiestromen kunnen worden gezien als de 'te beschermen belangen' van een organisatie. Voor deze bescherming kan een SOC worden ingezet.

De term SOC is binnen de overheid inmiddels een modewoord geworden. Allerlei organisaties die zich bedreigd voelen door cyberaanvallen en IT-misbruik denken dat het inrichten van een SOC de ultieme oplossing is. Zij zien het SOC dan als '*Haarlemmerolie*'. Het ontbreekt echter vaak aan consistentie bij de inrichting van de SOC's, waarbij de optredende pluriformiteit geen garantie levert voor hun effectiviteit. Desalniettemin denken veel van deze organisaties dat zij al over een effectief werkend SOC beschikken. Soms is deze opinie terecht, maar helaas niet altijd.

Het primaire probleem is dat de literatuur geen eenduidig model biedt voor een SOC. De beschrijvingen van de taken, verantwoordelijkheden en bevoegdheden van SOC's lopen in de literatuur sterk uiteen [PvIB2012]. Hierbij ontbreekt het aan een wetenschappelijke basis en consistentie. White papers van toonaangevende leveranciers gaan elk uit van hun eigen bedrijfsspecifieke inrichting, waarbij eenieder redeneert vanuit het eigen commerciële belang [HP2011] [IBM2013] [RSA2013] [McaFee2012]. Doordat er geen synergie bestaat voor de invulling van een SOC, ontstaan op gefragmenteerde en bijna willekeurige wijze security taken die mogelijk wel of niet binnen een SOC kunnen worden ondergebracht. Er is sprake van een diffuus beeld van de term SOC.

In deze scriptie is het gehele stelsel van maatregelen voor informatiebeveiliging en privacybescherming als uitgangspunt genomen, dus gekozen voor een brede benadering. Dit leidt tot de volgende definitie van een SOC.

> *Een SOC is een groep competente medewerkers welke vanuit een integraal stelsel van maatregelen de gewenste bescherming biedt tegen cyberdreigingen en IT-misbruik.*

Met het doel de gewenste bescherming te bieden tegen cyberdreigingen en IT-misbruik, biedt het SOC diensten, informatie, advies en ondersteuning aan de gebruikersorganisaties en beheerorganisaties. Deze interne dienstverlening heeft drie doelstellingen, namelijk (1) het geven van sturing binnen het voortbrengingsproces, (2) het bewaken van de operationele omgeving en (3) het ingrijpen in de bedrijfsprocessen. Vanuit deze doelstellingen zijn vier groepen van taken te onderscheiden, conform een ontwikkeld meetmodel voor het bepalen van de effectiviteit van een SOC. Deze betreffen de taakgebieden (1) kennisdeling, (2) het vervaardigen van veilige (web)applicaties, (3) continuous monitoring en (4) schadebeperking. Dit meetmodel is gebruikt tijdens het veldonderzoek.

Tijdens het veldonderzoek zijn er grofweg vier verschillende verschijningsvormen van SOC's naar voren gekomen. Deze verschijningsvormen kennen per taakgebied elk specifieke sterke en zwakke punten. Onze waarnemingen gaven echter aan dat binnen een bepaald taakgebied de effectiviteit per individuele taak heel sterk kan fluctueren. Deze fluctuaties geven aan dat er, naast de verschijningsvorm, andere bepalende factoren zijn, die de volledigheid van het takenpakket van een SOC sterk beïnvloeden. Dit leidde tot nader onderzoek, namelijk het uitvoeren van een decompositie van de elementaire basisfuncties binnen een SOC. Dit zijn in feite de bouwblokken waarmee een SOC is opgebouwd.

De introductie van deze bouwblokken maakt het ontwerp van een nieuw SOC overzichtelijk en maakt standaardisatie mogelijk. Men kan een SOC nu modulair opbouwen en tevens zo inrichten dat meerdere gebruikersorganisaties met hun eigen bedrijfsprocessen, en meerdere beheerorganisaties met hun eigen infrastructuren, parallel kunnen worden bediend. Een dergelijk 'SOC as a Service' levert diensten aan organisaties die behoefte hebben aan meer weerbaarheid tegen cyberaanvallen. Binnen de Rijksoverheid kan men hierbij denken aan een (Multi)Departementaal SOC, dat voor één of meer Ministeries zorgt voor cybersecurity en het voorkomen van IT-misbruik.

Een (Multi)Departementale aanpak lost een aantal praktische problemen op, zoals de huidige schaarste aan expertise van analisten, het nergens functioneren van een Security Information Event Monitoring (SIEM), het op vele plaatsen opnieuw uitvinden van het wiel door allerlei verschillende SOC's te ontwikkelen etc. Door schaalvergroting en het schaalbaar maken van het SOC, krijgt men een verhoging van de effectiviteit en de efficiëntie.

In deze scriptie hebben wij vele ideeën gebundeld die zijn geopperd door vakgenoten, experts en collega's. Wij zijn hen heel dankbaar voor hun actieve participatie en hun stimulerende interactie.

2. Inleiding

Cyberaanvallen vormen een steeds ernstigere bedreiging voor de Nederlandse economie en de nationale veiligheid. De Algemene Inlichtingen en Veiligheid Dienst signaleert dat digitale aanvallen toenemen in aantal, complexiteit en impact [AIVD2012]. In een brief aan de Tweede Kamer op 5 april 2013 spreekt de Minister van Binnenlandse Zaken en Koninkrijksrelaties, R.H.A. Plasterk, zijn zorgen uit over de steeds grotere bedreiging van de nationale veiligheid, die is ontstaan door een toenemende mate van internationalisering en technologisering. Daarin stelt de Minister dat bedrijven, overheden en burgers kwetsbaarder worden door een aantal trends en ontwikkelingen. Steeds meer informatie wordt namelijk door bedrijven, overheden en burgers digitaal opgeslagen, gekoppeld en via internetverbindingen en cloud computing (inter)nationaal gedeeld. De ICT-infrastructuur, maar ook de economie en de samenleving, wordt hierdoor kwetsbaarder voor aantastingen door zowel staten als criminele en extremistische groepen. De dreiging van Ccyber-inbreuken op de nationale veiligheid manifesteert zich steeds nadrukkelijker.

Nederland behoort tot de top vijf kenniseconomieën ter wereld en heeft de ambitie die positie in de nabije toekomst te versterken. Om deze reden, en vanwege de open Nederlandse samenleving en de uitstekende ICT-infrastructuur, vormt ons land een aantrekkelijk doelwit voor economisch en technisch-wetenschappelijk gewin. Adequate bescherming en bestrijding tegen deze cyberdreiging is van het grootste belang om de Nederlandse samenleving en economie draaiende te kunnen houden.

De ‘klassieke informatiebeveiliger’ blijkt moeite te hebben het hoofd te bieden tegen de hedendaagse intensieve en geavanceerde cyberaanvallen. Generaal Dick Berlijn, Oud Commandant der Strijdkrachten, sprak op 30 oktober 2013 tijdens het seminar ‘Fighting cybercrime’ van de Vrije Universiteit Amsterdam, over oorlogsvoering binnen de cyberwereld. Menige Nederlander herinnert zich de cyberaanvallen waar onder meer de ING, Rabobank, ABN AMRO, KLM, DigID en Diginotar de afgelopen twee jaar mee hadden te kampen, welke resulteerden in een abrupte verstoring van hun bedrijfsvoering. Voor de gebruiker veroorzaakte dit een gevoel van onbehagen, mede door de onduidelijkheid over wanneer de dienstverlening zou worden hervat. Dit is ongewenst voor het bedrijfsleven, de overheid en alle betrokkenen. Voor de organisaties in kwestie resulteert dit onder andere in reputatieschade en financiële schade. Dit betekent dat deze organisaties meer geavanceerde middelen moeten ontwikkelen om zich te beschermen tegen cyberaanvallen en de weerbaarheid te verhogen.

2.1. Achtergrond

In het verleden werd het hacken van computers en computernetwerken veelal uitgevoerd door onschuldige hobbyisten. Deze wilden soms laten zien dat zij slimmer waren dan de technici die computers en netwerken moesten beveiligen. Opschepperij, aanzien en verveling waren de grootste drijfveren voor de hackers. Financieel gewin was tot dan toe nauwelijks het motief. Zo ontdekten hackers in de jaren 70 dat het Amerikaans telefoonsysteem werkte met bepaalde tonen. Het bleek mogelijk gratis te kunnen bellen door deze tonen met een fluit te imiteren. Om dit lek te demonstreren gingen zij gratis vanuit Amerika naar het Vaticaan bellen. Deze zogeheten ‘prank calls’ waren veelal onschuldig.

In de loop der tijd is het gebied van hacken verlegd van een onschuldige bezigheid naar een serieuze bedreiging die organisaties miljoenen kunnen kosten en zelfs de Nationale veiligheid in gevaar kunnen brengen. Vandaag de dag zijn inlichtingen- en veiligheidsdiensten bezig met de ontwikkeling van cyberwapens. Internationale criminele organisaties richten zich steeds meer op frauderen via het internet voor financieel gewin. Het NCSC stelt vast dat er gesproken kan worden van cybercrime-as-a-service [NCSC 2013]. Dit wordt gezien als een cyberdienstensector waarin hulpmiddelen commercieel beschikbaar worden gesteld. Cyberaanvallen worden enerzijds steeds professioneler en meer centraal georganiseerd, maar ook worden de middelen steeds laagdrempeliger beschikbaar gesteld aan de verschillende actoren.

Dick Berlijn vergelijkt het huidige internet met een oorlogsgebied. Hij neemt de cyberaanvallen heel serieus en stelt dat via cyberwapens een vitaal deel van de samenleving kan worden platgelegd. Stel dat de SCADA computers van de waterkeringen worden beïnvloed door hackers, criminelen of vijandige partijen, dan kan in theorie een deel van Nederland met natte voeten komen te staan. Hetzelfde geldt voor de SCADA computers binnen de energievoorziening. Zonder electriciteit en benzine stagneert onze moderne maatschappij.

2.2. Probleemstelling

De overheid maakt zich zorgen omtrent het toenemend aantal beveiligingsaanvallen op de netwerken en websites van de overheid, de cyberdreigingen voor de vitale infrastructuur en het misbruik van financiële, privacygevoelige en vertrouwelijk gegevens. Dit heeft geleid tot de oprichting van het Nationale cyber Security Centrum (NCSC), de uitrol van de ‘Baseline Informatiebeveiliging Rijksdienst’ (BIR) en het inrichten van diverse samenwerkingsverbanden, zoals via het Centrum voor Informatiebeveiliging en Privacy (CIP).

De Rijksoverheid is gezien haar unieke taken een interessant aanvalsobject voor hackers, criminelen of vijandige partijen. Dit komt niet alleen door de vertrouwelijkheid van de informatie, tot en met Staatsgeheim Zeer Geheim, maar ook door de verwerking van enorme financiële geldstromen. De geldstroom door de Rijksoverheid is jaarlijks meer dan 250 miljard euro. Dit is een bedrag van € 250.000.000.000,-, uitgeschreven met het juiste aantal nullen voor de komma. Iedere crimineel droomt van het afromen van deze geldstroom, al is het maar met één procent. Daarnaast heeft het Rijk een reputatie hoog te houden wat het voor de actoren interessant maakt om hier schade aan toe te brengen.

In reactie op de toegenomen dreiging schieten Security Operations Center (SOC’s) als paddenstoelen uit de grond. De realiteit leert ons echter dat er hiervoor weinig echt effectieve best practices zijn, zoals blijkt uit:

- European Network and Information Security Agency [ENISA2006] adviseert een team van specialisten met aanvullende competenties, maar wordt op dit punt niet concreet;
- Een Expert Groep van het PvIB concludeert dat er geen eenduidige inrichting mogelijk is voor een SOC. Er wordt gesteld dat de doelstelling en taken per organisatie te ver uiteenlopen om handvatten te kunnen geven aan de inrichtingen van een SOC [PvIB2011];
- Het CIP heeft een periodiek informatiebeveiligingoverleg (PIO) ingeregeld waarbij het inrichten en in stand houden van SOC‘s centraal staat. Hierbij is een bijeenkomst georganiseerd op 10 december 2013 waarna verschillende lessons learned naar voren zijn gekomen.

> Zo lijkt het inrichten van het SOC een lastige opgave door de complexiteit van een IT-omgeving.

Een verkennende literatuurstudie geeft geen handvatten voor het concreet inrichten van een SOC. Een concrete visie hoe een SOC te organiseren en in te richten binnen een organisatie ontbreekt. Het risico bestaat dat het SOC niet zal bijdrage aan het tegengaan van de huidige cyberdreiging. Het aanreiken van concrete handvatten voor het organiseren en inrichten van een SOC is dan ook gelijk de meerwaarde van deze scriptie.

2.3. Scope

De afbakening en scope van de opdracht omvat in theorie alle overheidsinstanties die moeten voldoen aan de Baseline Informatiebeveiliging Rijk (BIR). Tevens zijn instanties die persoonsgegevens van burgers verwerken gebonden aan de Wet Bescherming Persoonsgegevens (Wbp), waardoor een verplichting ontstaat haar informatiebeveiliging op orde te hebben. Hier kan een SOC een essentiële bijdrage aan leveren.

2.4. Onderzoeksvraag

De centrale vraag van ons onderzoek is:

> *Op welke wijze dient een SOC te worden georganiseerd en ingericht om de IT-dienstverlener en haar klanten binnen de overheid weerbaar te maken tegen cyberaanvallen en IT-misbruik?*

2.4.1. Deelvraag 1: Literatuurstudie naar een model

De eerste deelvraag is inventariserend van aard:

1. *Is er vanuit de literatuur een model of een voorbeeld beschikbaar voor de inrichting van een effectief SOC of voor de optimalisatie van een bestaand SOC?*

Aan de hand van literatuurstudie wordt onderzocht in hoeverre deze kant en klare concepten biedt voor het organiseren en inrichten van een effectief SOC, en in hoeverre er synergie bestaat tussen de meningen van de diverse auteurs. Tevens toetsen wij de theorie aan de praktijk, namelijk in hoeverre passen de in de literatuur beschreven modellen bij de realiteit van de werkvloer?

2.4.2. Deelvraag 2: Veldonderzoek voor daadwerkelijke realisaties

De tweede deelvraag is analyserend van aard:

2. *Hoe zien SOC's er uit in de praktijk en is hieruit een generieke verschijningsvorm af te leiden en een decompositie van de functionaliteit?*

Verschillende operationele SOC's of SOC's in ontwikkeling worden bezocht binnen de Rijksoverheid. Aan de hand van deze praktijkvoorbeelden wordt de basisfunctionaliteit vastgesteld en

deze gesplitst in samenhangende bouwblokken. Voor ieder bouwblok wordt bekeken hoe deze optimaal kan worden benut.

2.4.3. Deelvraag 3: 'SOC as a Service'

De derde deelvraag is eveneens analyserend. Deze gaat zowel over de effectiviteit van een SOC als over efficiëntie, namelijk tegen de laagst mogelijke kosten het hoogst mogelijke beveiligingsniveau te verkrijgen:

3. *Kan een SOC dusdanig worden ingericht dat deze ook diensten kan leveren aan meerdere gebruikersorganisaties en beheerorganisaties binnen de overheid?*

Deze deelvraag wordt opgepakt vanuit de theorie en wordt gebaseerd op het model dat in het kader van het beantwoorden van de tweede deelvraag wordt ontwikkeld. Hierbij is het de bedoeling met de bouwblokken een bouwwerk te realiseren, dat leidt tot een optimaal overall resultaat om de overheid weerbaar te maken tegen cyberaanvallen en IT-misbruik.

2.4.4. Deelvraag 4: Consultatie van vakgenoten

De vierde deelvraag is beschouwend van aard:

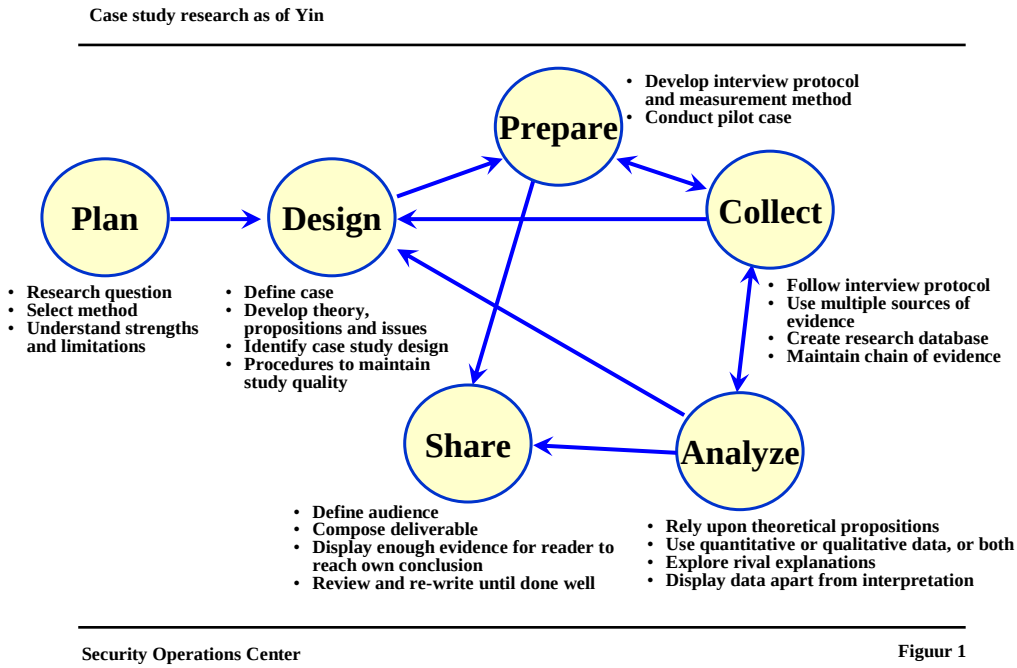
4. *Wat is de professionele opinie van vakgenoten over het ontwikkelde model?*

Het model met bouwblokken wordt getoetst om vast te stellen of dit tot een effectief en efficiënt opererend SOC leidt. Deze toetsing heeft de vorm van een review door een forum van professionals en leidinggevenden binnen het vakgebied (informatie)beveiliging en bij de bezochte SOC's.

2.5. Onderzoeksmethode

Het onderzoek naar aanleiding van deze scriptie zal worden uitgevoerd als een empirische studie via interviews met vakgenoten uit verschillende organisaties en het bestuderen van informatie uit publiekelijk toegankelijke bronnen.

Voor de onderzoekaanpak wordt Robert K. Yin benut, zoals beschreven in het boek 'Case study research, design and methods', fourth edition [YIN2009].Yin gaat uit van een lineaire en iteratieve aanpak, conform de onderstaande figuur.



Figuur 1

De 'Plan' fase is inventariserend van aard. In deze fase worden de onderzoeksvragen opgesteld en wordt geschetst wat de aanpak is met bijbehorende scope. Tevens wordt in deze fase literatuurstudie gedaan naar werkende modellen van SOC's. De informatie die wordt opgedaan tijdens deze studie zal dienen als input bij de volgende fases.

De 'Design' fase is inventariserend, namelijk het opstellen van vragenlijsten voor de interviews. Om structuur te geven aan de interviews, wordt vooraf een meetmethode opgesteld om inzicht te krijgen in de bestaande SOC's binnen het Rijk. Tevens wordt in deze fase een selectie gedaan, in overleg met de opdrachtgever, voor de te interviewen SOC's en enkele organisaties die nog geen SOC hebben, maar wel hiervoor in aanmerking komen.

De vragenlijst is generiek opgesteld en wordt per organisatie specifiek gemaakt. De onderzoeksvragen worden hierin meegenomen. Het doel van de meetmethode is inzicht te krijgen in de bestaande SOC's en het hieruit afleiden van een generieke verschijningsvorm.

In de 'Prepare' fase wordt de ontwikkelde vragenlijst en meetmethode getoetst in de vorm van een Pilot bij een bestaand SOC. Hierna kunnen de nodige aanpassingen aan de vragenlijst en meetmethode worden doorgevoerd.

In de 'Collect' fase worden de geselecteerde organisaties bezocht. Ter voorbereiding wordt de vragenlijst en meetmethode toegezonden. Per onderzocht object volgt een gespreksverslag welke

ondersteunend is aan de invulling van de meetmethode. Deze resultaten dienen vertrouwelijk te blijven. Om tijdens het onderzoek te kunnen komen tot resultaten zal de kennis worden gebundeld en in verschillende hypothetische situaties worden opgesteld.

In de 'Analyze' fase wordt de detailanalyse uitgevoerd. Hierbij worden verkregen resultaten verwerkt waarbij wordt getracht adequaat antwoord te geven op de onderzoeksvragen.

Bij deze detailanalyse worden de meest gebruikelijke verschijningsvormen en elementaire basisfuncties van een SOC uitgewerkt, gebaseerd op de ervaring opgedaan vanuit de theoretische en praktische situaties. Aan de hand van de verkregen resultaten wordt vervolgens uitgewerkt wat de meest effectieve inrichting van SOC's binnen het Rijk zal zijn.

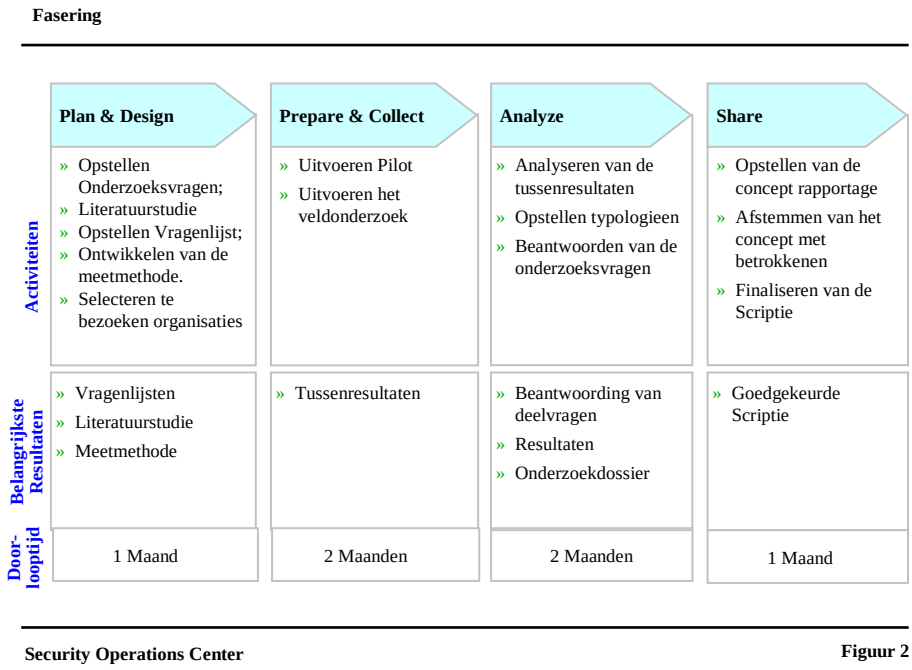
In de 'Share' fase wordt de scriptie beschikbaar gesteld aan diverse geïnteresseerden binnen het vakgebied en gedeeld met de betrokkenen welke een bijdrage hebben geleverd aan de totstandkoming van het eindproduct. Met hen wordt ook de discussie gevoerd over de relevantie en de herkenbaarheid van het ontwikkelde model.

2.6. Fasering, activiteiten, planning en producten

De opdrachtuitvoering bestaat uit vier fasen, ieder met een vooraf gedefinieerde doorlooptijd, namelijk:

- Fase 1 'Plan & Design', start december 2013 en heeft een doorlooptijd van 1 maand;
- Fase 2 'Prepare & Collect', start parallel in december 2013 en zal gedurende 2 maanden worden uitgevoerd;
- Fase 3 'Analyze', start in februari 2014 en heeft een doorlooptijd van 2 maanden;
- Fase 4 'Share', start nadat de resultaten uit het onderzoek zijn verkregen. Het conceptrapport wordt dan opgeleverd in april 2014 waarna afstemming kan plaatsvinden. Deze fase heeft een doorlooptijd van een maand;
- Finale Scriptie uiterlijk op 31 mei 2014.

De fasering is als volgt:



Figuur 2

2.7. Uitgevoerd onderzoek

De scriptie is gebaseerd op door de auteurs uitgevoerde opdrachten bij cliënten van hun werkgever.

Tevens is gebruik gemaakt van door een van de auteurs uitgewerkte modellen in het kader van een opdracht voor het Directoraat-generaal Organisatie Bedrijfsvoering Rijksdienst, Directie Informatiseringbeleid Rijksdienst (DGOBR/DIR) van het Ministerie voor Binnenlandse Zaken en Koninkrijksrelaties. Dit laatste onderzoek is gericht op de wijze waarop een Rijksbrede samenwerking tussen de Security Operations Centers (SOC's) binnen het Rijk mogelijk en haalbaar zou zijn, en hoe een dergelijke samenwerking kan worden vormgegeven en ontwikkeld. De overheid zou graag toewerken naar een situatie waarin kennisdeling over cyberweerbaarheid en samenwerking een meer gestructureerde vorm krijgt.

Het onderzoek voor DGOBR/DIR is gericht op het identificeren van mogelijke vormen van participatie tussen SOC's van Rijksdiensten, gemeentes en ZBO's. Hierbij wordt inzichtelijk gemaakt welke partijen willen aansluiten bij een Rijksbrede aanpak, wat hun individuele bijdrage is en welke voordelen zij daarin zien.

2.8. Relatie met andere onderzoeken

In de literatuur zijn een groot aantal white papers te vinden over SOC's. De meeste van deze artikelen zijn geschreven door personen die een SOC hebben ingericht en beschrijven een specifieke implementatie, met een toelichting waarom zij goed werk hebben verricht. Andere artikelen zijn opgesteld door leveranciers van tooling, die willen laten zien dat de door hen geleverde instrumenten waardevol zijn. Al deze artikelen hebben een bepaalde, op zich prima, intentie namelijk iets overbrengen of verkopen, maar missen een wetenschappelijke basis.

Een andere categorie artikelen en handboeken is gepubliceerd door beroepsorganisaties en onderzoeksinstituten, zoals PvIB, ENISA, NIST, CIP etc. Deze zijn vaak pragmatisch en doelgericht, met goede adviezen, maar missen veelal samenhang en consistentie.

Gezien het ontbreken van een wetenschappelijke basis hebben de auteurs van deze scriptie besloten veldwerk te gaan uitvoeren en een model te ontwerpen voor de elementaire basisfuncties van een SOC, met de intentie hiermee een SOC te kunnen vormgeven en te positioneren binnen diverse doelorganisaties.

2.8.1. Vraagstelling voor het veldonderzoek

Bij het onderzoek is de volgende vragenlijst opgesteld door de opdrachtgever DGOBR/DIR om richting te geven aan de interviews:

1. Welke partijen binnen het Rijksdomein beschikken op dit moment over een SOC of werken aan de ontwikkeling of inrichting ervan? Welke partijen binnen het Rijk beschikken niet over een SOC maar zouden logischerwijs, bijvoorbeeld ten gevolge van Rijksbrede beveiligingskaders, hier wel over moeten beschikken?
2. Hoe zijn de bestaande en in ontwikkeling zijnde SOC's op dit moment te typologiseren, bijvoorbeeld op basis van de PvIB indeling?
3. Hoe vindt op dit moment samenwerking plaats tussen de bestaande en zich ontwikkelende SOC's binnen het Rijk?
4. Hoe kan deze samenwerking zodanig worden versterkt of ontwikkeld zodat één Rijksbreed samenwerkingsverband is te realiseren? Wat is er voor nodig om dit samenwerkingsverband te laten ontstaan?
5. Hoe kunnen partijen die nu nog niet over een SOC beschikken of aan de ontwikkeling ervan werken worden gestimuleerd om zich bij dit netwerk aan te sluiten? En wat staat de ontwikkeling van een SOC bij deze partijen nu in de weg?
6. Hoe kunnen partijen waarbij de ICT infrastructuur, -beheer of -dienstverlening geheel of in belangrijke mate is of zal worden uitbesteed naar commerciële marktpartijen toch een SOC inrichten of zijn andere oplossingen mogelijk?
7. In hoeverre bestaat de mogelijkheid, de vraag en de bereidheid om SOC diensten van de ene Rijkspartij te leveren aan een partij die dit nog niet heeft? Wat is nodig om dit mogelijk te maken?
8. Welke stappen dienen te worden gezet om één virtuele Rijks SOC te realiseren, zoals hierboven beschreven? Op welke punten kan dit virtuele Rijks SOC van toegevoegde waarde zijn?
9. Wat is, gegeven de ontwikkelingen in de markt en stand der techniek, de meest effectieve en efficiënte inrichting en taakstelling van dit virtuele Rijks SOC?

De specifieke waarnemingen zijn vertrouwelijk. Met toestemming van de opdrachtgever DGOBR/DIR zijn de meer generieke conclusies opgenomen in deze scriptie, waarbij de individuele bronnen niet herkenbaar zijn.

2.9. Begeleiding

De auteurs zijn tijdens hun onderzoek begeleid door:
- Ronald Paans, Werkgever, Directeur Noordbeek;
- René Matthijssen, Scriptiebegeleider, Vrije Universiteit.

2.10. Visie op het onderzoek

Zoals betoogd door Ronald Paans tijdens het door hem geleide seminar 'Fighting cybercrime' aan de Vrije Universiteit op 30 oktober 2013, in aanvulling op de keynote toespraak van generaal b.d. Dick Berlijn, zijn de twee kenmerken van een SOC:
- Aanvallen is mensenwerk, verdedigen is ook mensenwerk. Door een groep gedreven en competente verdedigers te bundelen in een SOC verhogen wij onze weerbaarheid;
- Meten is weten. Met de tooling van een SOC weten wij wanneer wij worden aangevallen en kunnen snel reageren.

Een SOC bestaat uit experts op het gebied van monitoring, detectie, analyse en preventie. Door hun kennis te bundelen in een hybride SOC, gericht op zowel bewaking van de operationele netwerken en systemen, als op participatie in de ontwikkel- en onderhoudstrajecten, wordt gezorgd dat zowel de voordeur als de achterdeur op slot zitten en worden bewaakt.

Het SOC speelt een belangrijke rol bij het deel Continuous Monitoring, waarbij actuele signalen in de netwerken en systemen worden verzameld, gebundeld en geanalyseerd. Hierbij worden verschillende technische hulpmiddelen gebruikt, zoals de output van Anti Virus, Intrusion Detection Systems (IDS) en Intrusion Prevention Systems (IPS), de Control Compliance Suite en vulnerability scans, en de Security Information and Event Manager (SIEM). Het doel van deze activiteiten is het actief opsporen en aanpakken van kwetsbaarheden, om zo aanvallen in een vroeg stadium te kunnen detecteren en preventief acties te ondernemen.

Daarnaast is het belangrijk naar de nabije toekomst te kijken via het deel Intelligence. Hierbij volgen de medewerkers van het SOC signalen, afkomstig van andere partijen zoals NCSC, en de gemeenschappen die mogelijk schade kunnen toebrengen. Dit zijn groepen zoals hackers, die via fora en social media communiceren. In het Intelligence deel wordt informatie uitgewisseld met de interne of externe vertrouwde partners, om voorbereid te kunnen zijn op naderend onheil en tijdig daartoe maatregelen te kunnen treffen. In deze visie bestaat een SOC uit goede mensen, ondersteund met goede hulpmiddelen, en heeft zij een preventieve, detectieve en correctieve taak.

Zoals Paans stelt zijn SOC's noodzakelijk binnen het overheidsdomein, maar zijn deze in feite een verlengstuk van de klassieke informatiebeveiligers van de afgelopen decennia. Ook 20 jaar geleden was informatiebeveiliging van belang. Het grote verschil met toen is dat er nu veel meer aanvallen plaatsvinden door veel grotere groepen verschillende aanvallers, onder andere doordat

de infrastructuren en informatiesystemen verder zijn opengezet naar de buitenwereld. Dit geldt zowel voor toegang voor burgers met de e-overheid, als voor veel meer externe toegang door eigen medewerkers in het kader van Het Nieuwe Werken en het mobiele werken. Door deze grotere toegankelijkheid is de kwetsbaarheid toegenomen en is er steeds meer behoefte aan een krachtige beveiliging.

3. Informatiebeveiliging binnen de Rijksoverheid

De geautomatiseerde gegevensverwerking van de overheid is ontsloten via diverse kanalen, zoals de e-wereld, de kantoorautomatisering en het Nieuwe Werken [PvIB2011]. Door de vele verbindingen tussen de buitenwereld en de applicaties en gegevensverzamelingen van de overheid worden de dreigingen van cybercriminaliteit en misbruik steeds groter, ingenieuzer en complexer [AIVD2012].

Regelmatig vinden incidenten plaats, die door de media worden uitvergroot. Zo noopte een lek in programmeeromgeving Ruby on Rails overheidsorganisatie Logius ertoe om DigiD offline te halen [CW2013]. In 2011 is het systeem, waarmee SSL-certificaten voor overheidsdiensten als DigiD en de belastingdienst worden gemaakt, gekraakt [TW2011]. In 2012 besmette het Dorifel virus computers van tientallen gemeenten waardoor office-bestanden niet meer leesbaar waren [BB2012]. Dit soort incidenten prikkelt de politiek, die daarna druk uitoefent op senior management binnen de overheidsorganisaties. Veel bestuurders zijn hiermee overvallen, en missen persoonlijk de kennis en kunde om de juiste maatregelen te kunnen overzien. Hierdoor begint men vaak aan grote projecten om van alles te beveiligingen, zonder een helder doel voor ogen te hebben, en laat men zich overspoelen met toevallig aangeboden tooling. Het begrip cyberaanvallen blijft generiek en vaag, en het wordt niet concreet waartegen de organisaties zich moeten beschermen. Dit leidt tot inefficiënte investeringen.

De Rijksoverheid besteedt daarom in toenemende mate aandacht aan de standaardisering en centrale aansturing van informatiebeveiliging, inclusief privacybescherming. De Rijksoverheid wordt hierbij directiever, om senior management binnen de organisaties een richting te wijzen. In dit kader worden onder andere de ‘Baseline Informatiebeveiliging Rijksdienst (BIR)’ [BIR2012] en het ‘Tactische Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG)’ [BIG2012] uitgerold en de verplichting opgelegd om Chief Information Security Officers (CISO’s) aan te stellen.

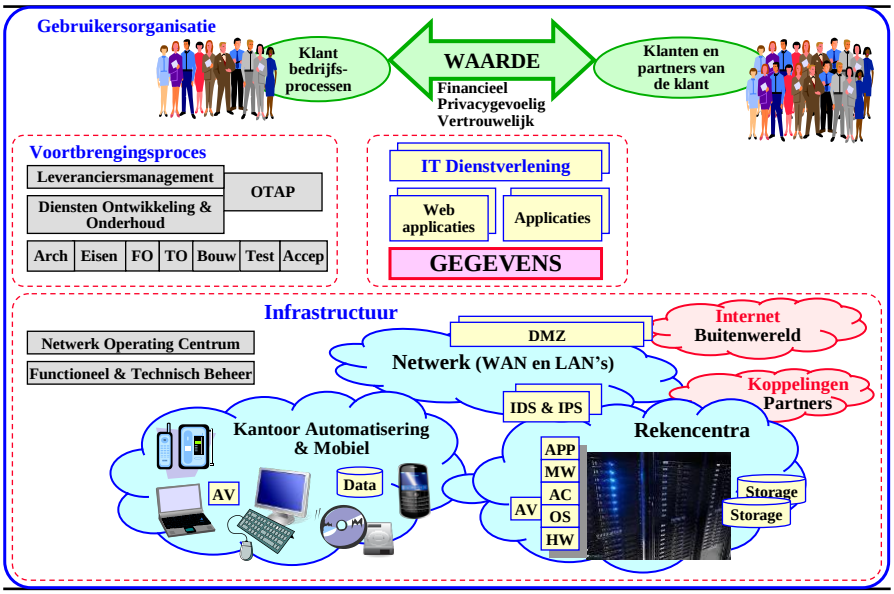
3.1. Het Object

Het is belangrijk om in kaart hebben welk object kan worden aangevallen en waartegen een organisatie zich moet beschermen. Dit zijn de zogenaamde ‘te beschermen belangen’.

Centraal bij een Rijksonderdeel staan de bedrijfsprocessen. Daarbij worden interne en externe gebruikers bediend, oftewel de Klant van de Klant. Dit is bijvoorbeeld een burger welke klant is van de belastingdienst. Daarbij worden gegevens met een bepaalde waarde uitgewisseld, dit kunnen financiële transacties zijn, privacygevoelige informatie, vertrouwelijke informatie etc. Deze informatiestromen kunnen worden gezien als de ‘te beschermen belangen’.

De te beschermen belangen vertalen zich in gegevens welke via applicaties door de infrastructuur stromen. In het onderstaande figuur is het object geschetst waarin de verschillende componenten van een willekeurige IT omgeving in deze context worden geplaatst.

IT Diensten en hun context



Security Operations Center

Figuur 3

3.2. Gebruikersorganisatie

In de bovenstaande figuur zijn de 'te beschermen belangen' aangegeven als de 'waarde' die wordt uitgewisseld tussen de eindgebruikers. De gebruikers kunnen zowel interne medewerkers zijn, als medewerkers van bijvoorbeeld ketenpartners, of burgers. De te beschermen belangen zijn berichten die een bepaalde betekenis en een bepaald belang hebben, en soms extra procedurele, organisatorische of technische bescherming vereisen. Met name als de berichten financiële transacties bevatten, of privacygevoelig of vertrouwelijk zijn, mogen die niet ongeautoriseerd worden onthuld of ongeautoriseerd worden gemodificeerd.

In hoeverre een bericht waarde vertegenwoordigt, wordt bepaald door het bedrijfsproces waarbinnen dit bericht wordt gebruikt, en door de bij de berichtuitwisseling betrokken gebruikers. De vaststelling van de waarde ligt primair bij de gebruikersorganisatie.

3.3. De Waarde en IT-dienstverlening

De 'waarde' wordt via de (web)applicaties binnen de IT-dienstverlening verwerkt en opgeslagen in de gegevens. Informatiebeveiliging richt zich met name op het borgen van de functionaliteit van de applicaties en het beschermen van de gegevens, gericht op hun Beschikbaarheid, Integriteit en Vertrouwelijkheid (BIV). Om deze reden staan de 'gegevens' centraal in de figuur.

Belangen in het kader van cybersecurity kennen verschillende niveaus: persoonlijke belangen, organisatiebelangen, ketenbelangen en maatschappelijke belangen. Deze belangen vertegenwoordigen een bepaalde waarde. Cybersecurity vereist bescherming van deze waarde

[NSCS2012]. Om de waarde van het object uit te drukken, kan gebruik worden gemaakt van een risicoanalyse in combinatie met de BIV-classificatie, Beschikbaarheid, Integriteit en Vertrouwelijkheid (BIV). Informatiesystemen, bedrijfsprocessen en gegevens worden, om het beoogde niveau van beveiliging te kunnen vaststellen, in de regel geclassificeerd volgens de BIV-indeling, gebaseerd op:

- Beschikbaarheid: Beschikbaarheid betreft het waarborgen dat geautoriseerde gebruikers op de juiste momenten toegang hebben tot gegevens en aanverwante bedrijfsmiddelen zoals informatiesystemen, oftewel het zorgen voor een ongestoorde voortgang van de informatievoorziening;
- Integriteit: Integriteit betreft het waarborgen van de juistheid, tijdigheid, actualiteit en volledigheid van informatie en de verwerking daarvan.
  Een onderdeel van Integriteit betreft de onweerlegbaarheid (non-repudiation). Dit is de mate waarin kan worden aangetoond dat acties of gebeurtenissen hebben plaatsgevonden, zodat deze acties of gebeurtenissen later niet kunnen worden ontkend;
- Vertrouwelijkheid: Met vertrouwelijkheid wordt gedoeld op het waarborgen dat informatie alleen toegankelijk is voor degenen die hiertoe zijn geautoriseerd.

Een Business impact analyse (BIA) wordt binnen een organisatie gebruikt om de kritieke processen van de niet kritieke processen te scheiden.

BIR 14.1.2 ‘Bedrijfscontinuïteit en risicobeoordeling’ stelt dat gebeurtenissen die tot onderbreking van bedrijfsprocessen kunnen leiden, behoren te worden geïdentificeerd, tezamen met de waarschijnlijkheid en de gevolgen van dergelijke onderbrekingen en hun gevolgen voor de informatiebeveiliging. Hiertoe schrijft BIR een Business Impact Analyse (BIA) voor. Aan de hand van een risicoanalyse worden de waarschijnlijkheid en de gevolgen van de discontinuïteit in kaart gebracht in termen van tijd, schade en herstelperiode.

Aan de hand van een BIA moet de gebruikersorganisatie voor iedere applicatie en iedere gegevensverzameling de BIV vaststellen en voor ieder van deze aspecten het belang aangeven in de termen zoals ‘Hoog’, ‘Midden’ en ‘Laag’. Op basis van deze classificatie worden de vereiste maatregelen geselecteerd en ingericht.

3.4. Voortbrengingsproces

De (web)applicaties worden verkregen aan de hand van het voortbrengingsproces, via ‘make or buy’ beslissing. In de Make-or-Buy beslissing ligt onder andere een overweging van de kosten en focus op kerncompetenties ten grondslag, welke bepalend kunnen zijn in de beslissing om een bepaalde activiteit zelf uit te voeren of deze activiteit door een externe leverancier te laten uitvoeren [OU2011]. Hier is Leveranciersmanagement bij betrokken of een ontwikkelorganisatie. Men koopt pakketten of ontwikkelt maatwerkprogrammatuur en maakt daarbij gebruik van de OTAP-straat, die bestaat uit de Ontwikkel, Test, Acceptatie en Productie omgevingen.

Informatiebeveiliging heeft ook betrekking op het voortbrengingsproces, aangezien naast functionele eisen en kwaliteitseisen specifieke eisen voor informatiebeveiliging moeten worden meegenomen. Deze specifieke eisen volgen uit de te beschermen belangen en houden rekening met de te ondersteunen bedrijfsprocessen en gebruikers. Nieuwe applicaties moeten al direct worden

ontworpen om bestand te zijn tegen de cyberdreigingen en tegen misbruik. Daarnaast moeten specifieke beveiligingseisen worden meegenomen bij het onderhoud van programmatuur en bij nieuwe releases.

3.5. Infrastructuur

Het woord infrastructuur is samengesteld uit de woorden infra (onder) en structuur. Het omvat alle componenten die beschikbaar zijn "onder de structuur". In het XR. Magazine met als thema 'ICT-infrastructuur' wordt gesteld dat de IT infrastructuur de totale set is van de fundamentele bouwstenen en niet-functionele eigenschappen die het mogelijk maken applicaties te laten functioneren [XRM2011]. De applicaties worden verwerkt in de infrastructuur en de gegevens worden daar opgeslagen. Diverse afdelingen zijn betrokken bij het operationeel beheer van de infrastructuur, zoals Functioneel Beheer, Technisch Beheer, Netwerk Operating Center (NOC), Floor Management, Housing Management etc. Al deze afdelingen vervullen diverse taken met betrekking tot informatiebeveiliging.

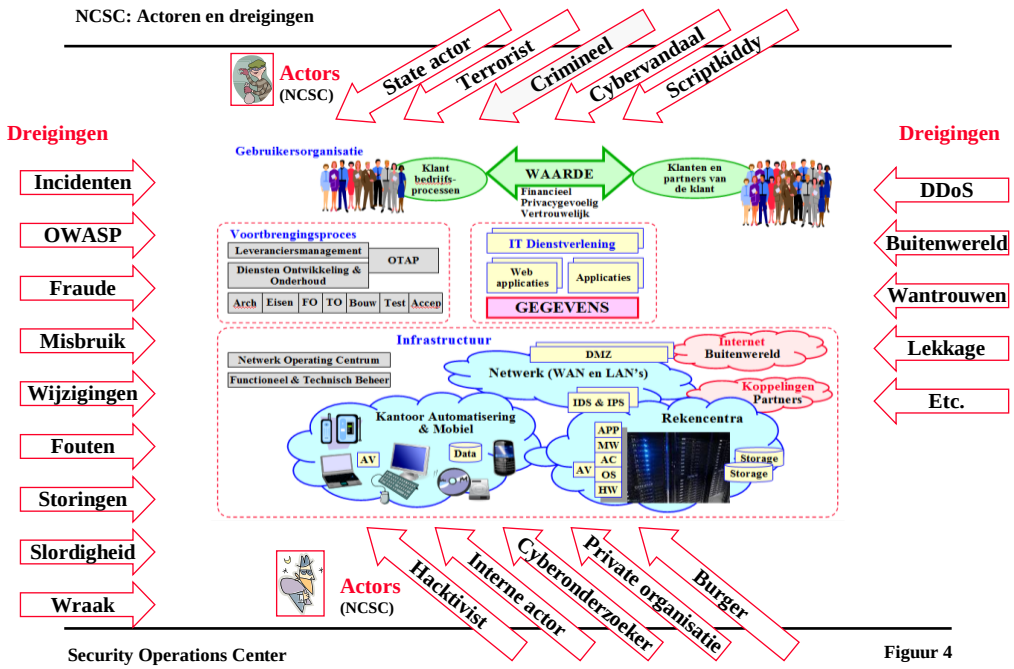
4. Literatuurstudie: Het Security Operations Center

Zoals reeds beschreven pretenderen veel organisaties te beschikken over een SOC, echter ontbreekt het aan consistentie tussen de onderlinge inrichting hiervan. Desalniettemin beschikken deze organisaties in hun ogen allen al over een effectief werkend SOC, dat kan worden ingezet als middel bij het tegengaan van cyberdreigingen en het verhogen van de weerbaarheid hiertegen. In de literatuur wordt er door verschillende auteurs invulling gegeven aan een effectief model of voorbeeld voor de inrichting van een SOC. In dit hoofdstuk is er aan de hand van een literatuurstudie onderzocht in hoeverre er kant en klare concepten bestaan voor het organiseren en inrichten van een SOC, en in hoeverre er synergie bestaat tussen de verschillende concepten. Hiertoe wordt de volgende deelvraag beantwoord:

> *Deelvraag 1: Is er vanuit de literatuur een model of een voorbeeld beschikbaar voor de inrichting van een effectief SOC of voor de optimalisatie van een bestaand SOC?*

4.1. NCSC: Actoren en bedreigingen

Een object kent verschillende dreigingen. NCSC beschrijft een groot aantal dreigingen welke op het object van toepassing kunnen zijn [NCSC2012]. Deze dreigingen zijn in het onderstaande figuur weergeven en geven een beeld wat allemaal op een object afkomt.



Figuur 4

Zonder dat het object inzichtelijk is voor een organisatie en de organisatie geen weet heeft van de waarde welke door haar omgeving stromen, kan een organisatie moeilijk gepaste maatregelen

nemen tegen de geschetste actoren en dreigingen. Het inzicht bij bedrijven ontbreekt waardoor er sprake is van beperkte weerbaarheid.

Weerbaarheid

Het NCSC stelt dat de aandacht voor cybercrime aanwezig is. De portefeuille voor cybersecurity en informatiebeveiliging wordt steeds vaker op strategisch niveau belegd, er ontstaat samenwerking tussen publiek en private bedrijven.

Echter daarbij stelt het NCSC ook dat organisaties de basismaatregelen, zoals patches en informatiebeveiligingsbeleid niet op orde zijn. Dit maakt bekende aanvalsmethode nog steeds effectief. Daarbij ontbreekt de juiste kennis, de middelen en het vermogen incidenten voldoende af te handelen. Deze conclusies van het NCSC komen overeen met de situatie welke is aangetroffen in de praktijk.

Een SOC wordt in deze scriptie gezien als het cruciale expertise centrum welke kan bijdragen aan de weerbaarheid van organisaties. Om toegevoegde waarde te leveren zoekt de scriptie diepgang in de inrichting van een professioneel SOC.

NCSC Factsheet 'De aanhouder wint'

In de factsheet 'De aanhouder wint' beschrijft het NCSC [NCSC2013] hoe organisaties zich kunnen wapenen tegen een Advanced Persistent Threat (APT). Een APT betreft een doelgerichte langdurige cyberaanval op met name kennisrijke landen en organisaties, veelal verricht door statelijke actoren en criminele organisaties. Voorbeelden van organisaties die zijn getroffen door een ATP betreffen NASA, Lockheed Martin en Aramco Overseas. De aanvallende partij is hierbij standvastig in zowel de pogingen om een organisatie binnen te dringen als ook om verscholen aanwezig te blijven binnen de ICT-infrastructuur. Het NCSC typeert het SOC als één van de middelen voor kennisrijke landen en organisaties om zich te wapenen tegen een dergelijke APT. Echter onthoudt het NSCS zich in deze factsheet van een eenduidige inrichting van een SOC, zoals blijkt uit de volgende passage uit de factsheet:

> *'Richt een toegewijd Security Intelligence (Operational) Center (SIC / SoC) of een CSIRT (APT) team op dat autonoom en met de juiste bevoegdheden en middelen kan optreden in geval van een APT-incident. Zorg dat dit team zo klein mogelijk is en goede directe contacten heeft met het hoger management. Zorg dat dit team ook de juiste managementtaal kan spreken en dat het management dit team vertrouwt en erkent'.*

4.2. PvIB model

Het PvIB bundelt in de expertbrief [PvIB2011] ervaringen van verschillende professionals en biedt een leidraad voor organisaties die een SOC overwegen in te richten. In deze expertbrief wordt tevergeefs geprobeerd handvatten te bieden bij de inrichting, taakverdeling en positionering van het SOC. In de expertbrief wordt gesteld dat ontwikkelingen, zoals 'Het nieuwe werken' en 'Cloud computing', leiden tot toenemende complexiteit van de IT-omgeving en tot gevolg heeft dat steeds meer organisaties behoefte hebben aan een SOC. De onderzoekers hebben

tijdens de verkennende literatuurstudie meerdere white papers bestudeerd en op basis hiervan geprobeerd inzichtelijk te maken op welke punten er overeenkomsten en verschillen bestaan tussen het PvIB model en de overige white papers.

4.3. Doelstellingen SOC

Er zijn verschillende doelstellingen die voor een organisatie als motivatie kunnen dienen bij het kiezen voor het oprichten van een SOC. Hieronder worden de belangrijkste doelen beschreven zoals deze binnen de PvIB expertbrief en overige white papers zijn geïdentificeerd.

Aantoonbaar beheersen van informatiebeveiliging door wet- en regelgeving

Het op aantoonbare wijze controle hebben over informatiebeveiliging binnen organisaties, wordt vanuit wet- en regelgeving in toenemende mate voorgeschreven en dient daarom dikwijls als een driver voor het oprichten van een SOC. In de white paper van IBM wordt gesteld dat de hedendaagse dynamische omgeving, steeds meer nieuwe eisen stelt op het gebied van wet- en regelgeving, welke zijn weerslag heeft op de organisatie van informatiebeveiliging binnen steeds meer organisaties [IBM2013]. In de expertbrief van het PvIB wordt aangegeven dat door interne controles en de bewaking van security incidenten uit te laten voeren door het SOC, deze als een waardevol instrument kan dienen om vanuit wet- en regelgeving te voldoen aan de plicht om het beheersen van informatiebeveiliging aantoonbaar te maken [PvIB2011]. In de white paper van HP wordt dit tevens bevestigd door aan te geven dat een operationeel SOC als een waardevol instrument kan dienen bij het aantoonbaar voldoen aan de vigerende wet- en regelgeving [HP2011].

Effectief uitvoeren van operationele security taken door bundeling van kennis

De steeds groter wordende wildgroei aan beveiligingsoplossingen, leidt ertoe dat specialistische kennis steeds meer versnipperd aanwezig is binnen organisaties. Daarbij is deze kennis schaars vertegenwoordigd op de arbeidsmarkt. McAfee bevestigt dit in hun white paper ‘Creating and maintaining a SOC’ door te stellen dat het een ware uitdaging is om geschikte SOC-medewerkers te vinden met de juiste kennis en vaardigheden op het gebied van informatiebeveiliging [McAfee2011]. Het concentreren van deze expertises binnen het SOC kan voor synergievoordeel zorgen, waardoor de kwaliteit kan worden verhoogd en de gevolgen van de schaarste in kennis kunnen worden beperkt.

Toepassen van functiescheiding

Een SOC kan bijdragen aan het principe van functiescheiding binnen organisaties. Zo kan het SOC de analyse op verdachte activiteiten volbrengen of de controle op de juiste werking van informatiebeveiliging uitvoeren. In de PvIB expertbrief wordt gesteld dat het oordeel van een onafhankelijke partij, zoals in dit geval het SOC, vaak kostbaarder is dan het oordeel van een verantwoordelijke IT-manager.

Incident- en risicobeheersing

Door te beschikken over kennis van alle security incidenten kan er aan de hand van analyses een accuraat beeld worden gevormd over mogelijke veranderende dreigingen en de daarbij horende risico's. Als deze informatie gefragmenteerd in de organisatie beschikbaar is, bemoeilijkt dit het verrichten van deze analyse. RSA stelt in de white paper 'Building an intelligence-driven security operations center' dat SOC's hun organisatie op holistische wijze moeten benaderen [RSA2013]. Een SOC kan op deze manier waardevol zijn bij het analyseren en aggregeren van security incidenten binnen verschillende afdelingen, die organisatiebreed van toepassing kunnen zijn.

Continuous monitoring

In de expertbrief van het PvIB wordt gesteld dat een SOC over het algemeen de plek in de organisatie is waar de operationele kennis rond informatiebeveiliging beschikbaar is [PvIB2011]. Het SOC dient daarvoor deze kennis actief bij te houden door het verkennen van de marktontwikkelingen op het gebied van informatiebeveiliging, maar dient ook bij te houden wat er intern in de organisatie aan beleid en richtlijnen wijzigt en hoe deze moeten worden geïnterpreteerd.

IBM geeft in de white paper 'Strategy considerations for building a security operations center' aan dat organisaties die niet beschikken over de meest actuele security intelligence, het risico lopen hun meest kostbare data onbewust te onderwerpen aan kwaadwillende cybercriminelen en dus niet beschikken over het vermogen om weerstand te kunnen bieden tegen opkomende bedreigingen [IBM2013]. IBM raadt daarom aan om een abonnement te nemen op verschillende mailing lists, die hun lezers periodiek op de hoogte houden van de laatste bedreigingen op het gebied van informatiebeveiliging en cybercrime. Aanvullend hierop is het voor een SOC ook raadzaam om zelf periodiek verschillende fora, websites en artikelen af te struinen. Hierdoor blijven de medewerkers van het SOC alerter op nieuwe bedreigingen en is het inventariseren van deze bedreigingen omvangrijker, aangezien dit zowel intern als extern gebeurt.

4.4. Inrichting van een SOC

Uit zowel de expertbrief van het PvIB [PvIB 2012], als de overige white papers werd vrij snel duidelijk dat er geen eenduidige manier is voor het inrichten van een SOC. Hieraan ten grondslag ligt het feit dat de taken, verantwoordelijkheden en bevoegdheden van een SOC erg uiteenlopend zijn en min of meer op basis van eigen inzichten en behoeften van de eigen organisatie worden bepaald. Dit leidt ertoe dat er geen eenduidige inrichting bestaat van een SOC. Hieronder worden een aantal aspecten beschreven die bepalend zijn voor de inrichting van een SOC. Tot slot worden de verschillende soorten SOC's behandeld die binnen de literatuurstudie zijn geïdentificeerd.

Positionering

Het takenpakket van een SOC is bepalend voor de plaatsing hiervan binnen een organisatie. In de PvIB expertbrief wordt gesteld dat uit de praktijk blijkt dat een SOC doorgaans in 'de lijn'

wordt geplaatst, waarbij het SOC de lijnorganisatie ondersteunt bij het verrichten van operationele security taken [PvIB2011]. McAfee stelt in de white paper 'creating and Maintaining a SOC' dat naast het takenpakket ook de behoeften van de klanten van het SOC bepalend kunnen zijn bij het positioneren van het SOC [McAfee2011]. Een SOC kan vanuit een bepaalde bedrijfskolom diensten verlenen aan andere bedrijfskolommen, binnen dezelfde organisatie. Hierbij is het maken van concrete afspraken belangrijk om mogelijke conflicterende belangen tussen bedrijfskolommen te voorkomen.

Competenties

In de PvIB expertbrief wordt aangegeven dat de competenties van medewerkers binnen een SOC direct zijn gelieerd aan de taken en verantwoordelijkheden die de medewerkers moeten uitvoeren. Zo geldt dat de competenties voor het uitvoeren van sleuteluitgifte zich beperken tot 'nauwkeurigheid' en 'klantvriendelijkheid'. Veel vakkennis op het gebied van informatiebeveiliging is hierbij niet nodig. Een SOC medewerker die verantwoordelijk is voor het bepalen van het risico van een security incident moet over compleet andere competenties beschikken. Hierbij kan onder andere worden gedacht aan 'analytisch vermogen', 'kennisgedreven' en 'organisatie sensitief'. Een belangrijke constatering binnen de expertgroep was dat het succes van een SOC binnen de organisatie grotendeels wordt bepaald door de professionaliteit, vakkundigheid en integriteit waarmee de taken worden uitgevoerd.

In de HP Enterprise Security Business white paper 'Building a succesful security operations center' wordt aangegeven dat het inzetten van medewerkers met de juiste vaardigheden en competenties en deze, vanwege het dynamische karakter van cyberdreigingen, te voorzien van permanente educatie bijdraagt aan een effectief werkend SOC [HP2011]. Daarnaast dient een SOC-medewerker over de volgende kerncompetenties te beschikken: een goede portie geduld, het vermogen om problemen te analyseren en te communiceren in tijden van stress. Echter blijft een meer concrete uitgediepte beschrijving, van de vaardigheden en competenties waarover een SOC-medewerker dient te beschikken, uit.

IBM benoemt in de white paper 'Strategy considerations for building a security operations center' de waarde van een adequate bemensing van een SOC. Eerder in de scriptie is door de auteurs aangegeven dat zowel het uitvoeren van cyberaanvallen als het verdedigen hiertegen, mensenwerk betreft [IBM2013]. Ondanks dat de SIEM-tooling security events identificeert, filtert en correleert, ligt er een sleutelrol weggelegd voor de SOC-medewerkers die deze data op de juiste manier moeten interpreteren. IBM geeft in haar white paper aan dat de SOC-medewerkers als ' het hart en ziel' van een SOC kunnen worden gezien. Zonder competente SOC-medewerkers en voldoende onderlinge communicatie, is het vrijwel onmogelijk om een effectief functionerend SOC te realiseren. IBM wordt in diens white paper niet concreet over de daadwerkelijke competenties waarover de medewerkers van een SOC behoren te beschikken.

Tooling

HP beschrijft in diens white paper dat één van de grootste uitdagingen het identificeren van significante security events is, uit een legio aan security tooling, deze vervolgens te correleren en terug te brengen naar een aantal dat is te overzien [HP2011]. Hierbij moeten analisten meerdere

malen inloggen en gebruik maken van de verschillende ondersteunende security tools, waardoor zij al snel door de spreekwoordelijke bomen het bos niet meer zien. Om dit proces efficiënter en effectiever te maken, adviseert HP dit te automatiseren door gebruik te maken van een zogenaamde Security Information and Event Management (SIEM) tooling. Een expliciete uitleg omtrent het inzetten en positioneren van deze tool komt in deze paper niet naar voren.

IBM beschrijft in diens paper het belang van het adequaat identificeren en monitoren van bedreigingen en vervolgens te bepalen op welke van deze bedreigingen actie moet worden ondernomen [IBM2013]. Met behulp van competente SOC-medewerkers, die worden ondersteund door de juiste SIEM tooling, kan het karakter van een SOC veranderen van reactief naar preventief. Zoals eerder beschreven, voorziet SIEM tooling in een technologisch middel waarvan een SOC gebruik kan maken bij het identificeren, correleren en prioriteren van bedreigingen. Concreet verzamelt de SIEM tooling een groot aantal logbestanden afkomstig van verscheidene objecten zoals Intrusion Preventing Systems (IPS), firewalls, routers en transformeert deze in praktisch toepasbare security intelligence. Uit de white paper blijkt dat het integreren van SIEM tooling binnen een SOC cruciaal is voor diens succes om cyberdreigingen tegen te gaan en de weerbaarheid en robuustheid van organisatie hiertegen te verhogen. Helaas blijft een praktisch toepasbare beschrijving van randvoorwaarden waaraan de inzet van SIEM tooling binnen een SOC dient te voldoen uit. De PvIB expertbrief wordt op dit punt niet concreet.

Verschillende soorten SOC's

De verantwoordelijkheden van een SOC zijn afhankelijk van het mandaat, de doelstellingen en de gekozen inrichting van het SOC. Periodieke controles op de implementatie van informatiebeveiliging kunnen op aanvraag door het SOC worden uitgevoerd. De verantwoordelijkheid om verdachte gebeurtenissen te identificeren en te beoordelen op risico´s kan tevens worden belegd bij het SOC. De verantwoordelijkheid om direct te handelen naar aanleiding van een bepaald security incident, valt ook onder de verantwoordelijkheid van het SOC. Als gevolg hiervan is het cruciaal om het SOC te voorzien van een mandaat om zelfstandig en op eigen initiatief te acteren op dergelijke gebeurtenissen, in het geval de belangen van de organisatie in het gevaar zijn. Uit de PvIB expertbrief en de overige white papers is gebleken dat een SOC op meerdere, uiteenlopende manieren kan worden ingericht. Onder andere de positionering, competenties en beschikbare tooling bepalen welk type SOC het beste kan worden toegepast. Hieronder wordt ingegaan op de verschillende soorten SOC's die zijn geïdentificeerd binnen de literatuurstudie:

- Het 'controle SOC' is voornamelijk controlerend van aard en voert hoofdzakelijk controles uit op de IT-omgeving om vast te stellen wat de actuele status is rond informatiebeveiliging. Tot het takenpakket van dit type SOC behoren onder andere: vulnerability scanning, compliancy testing en pentesting;
- Het 'monitorings SOC' concentreert zich vooral op het bewaken van de IT-omgeving en beschikt over het mandaat om op voortgekomen meldingen te acteren. Tot het takenpakket van dit type SOC behoren onder andere: monitoren van firewalls, IDS, virusscanners en SIEM oplossingen;
- Het 'operational SOC' richt zich hoofdzakelijk op operationele security werkzaamheden. Tot het takenpakket van dit type SOC behoren onder andere: key-management, access management en firewall beheer;

- Het 'maatwerk SOC', betreft een hybride vorm van de hiervoor genoemde SOC's. Het takenpakket van dit type SOC bestaat uit een combinatie van de takenpakketten van de overige SOC's.

4.5. Conclusie op basis van de literatuurstudie

Om antwoord te geven op de onderzoeksvraag: 'Is er vanuit de literatuur een model of een voorbeeld voor de inrichting van een SOC beschikbaar?', zijn er tijdens de verkenningsfase van dit onderzoek en bij het schrijven van dit hoofdstuk meerdere artikelen en papers bestudeerd. Ondanks dat meerdere auteurs dit onderwerp hebben behandeld en er diverse overeenkomsten zijn, wordt de literatuur niet concreet over een eenduidig model of voorbeeld voor de inrichting van een SOC. De taken, verantwoordelijkheden en bevoegdheden van een SOC zijn erg uiteenlopend en worden min of meer op basis van eigen inzichten en behoeften van de eigen organisatie bepaald. Zo biedt de literatuurstudie aan de hand van onder andere de expertbrief van het PvIB [PvIB 2011], de white paper van IBM 'Strategy considerations for building a security operations center' en de HP white paper 'Building a succesful security operations center' geen handvatten voor het concreet inrichten van een SOC. De expertbrief voorziet tevens niet in een eenduidige definitie van de activiteiten die een SOC dient uit te voeren. Ook worden er meerdere en uiteenlopende invullingen van een SOC beschreven. De taken, verantwoordelijkheden en bevoegdheden van een SOC worden min of meer op basis van eigen inzichten en behoeftes van een organisatie bepaald. Hierdoor ontstaat een diffuus beeld van de term SOC en belemmert dat de kennisuitwisseling en ontwikkeling van SOC's.

Derhalve zijn de auteurs van deze scriptie van mening dat er in de literatuur geen eenduidig model of voorbeeld voor de inrichting van een SOC voor komt. Deze absentie veroorzaakt verwarring. Deze verwarring belemmert de kennisuitwisseling en ontwikkeling van SOC's. Daarnaast bemoeilijkt dit ook de effectieve inrichting hiervan, terwijl het aantal organisaties die hier dringende behoefte aan heeft, gestaag blijft groeien.

5. Missie, doelstelling en scope van een SOC

In eerste instantie hebben wij een brede omschrijving gegeven van informatiebeveiliging waarbij de componenten van het object op generieke wijze zijn beschreven. Vervolgens is in het opvolgende hoofdstuk aandacht besteed aan de specifieke problematiek omtrent het SOC. Hierbij is een conclusie gegeven dat de literatuur niet komt tot een eenduidige oplossing maar iedere auteur specifiek voor zijn of haar eigen organisatie een oplossing beschrijft.

Wij zijn naar een hoger abstractieniveau teruggegaan. Het doel hiervan is om te kijken waar het SOC mogelijk een rol kan spelen binnen de organisatie. Vanuit deze integrale aanpak komen wij uiteindelijk tot een definitie en missie van het SOC.

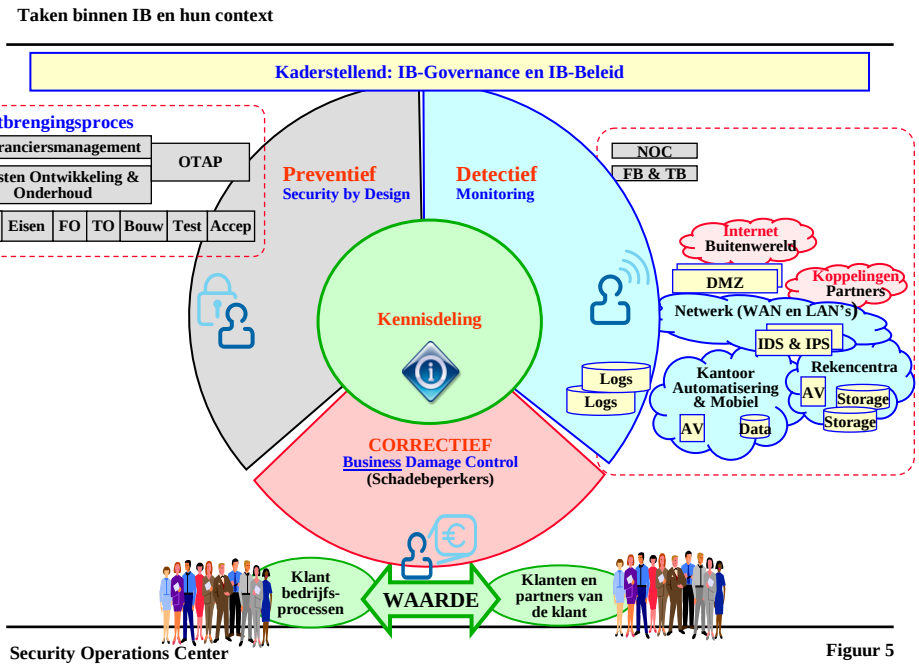
5.1. De taken van Informatiebeveiliging

Zoals John Hermans en Gerben Schreurs beschrijven in het artikel `Vijf denkfouten over cybersecurity [KPMG2012], is 100 % bescherming tegen cyberaanvallen en IT misbruik een illusie. Indien dit wordt onderkend kan vanuit een risicobenadering de juiste preventieve, detectieve en correctieve maatregelen worden opgesteld. Een denkfout welke hierbij wordt gemaakt is de oplossing te zoeken in de techniek. Hoewel de techniek essentieel is voor adequate beveiliging dient eerst een goed beleid, organisatie en procedures te worden ingericht. Techniek is pas te laatste stap. Hiervoor volgt de kenmerkende uitspraak: *'A Fool with Tool is still a Fool'*. De mens is en blijft verantwoordelijk voor vele incidenten en zonder de juiste competenties blijft deze uitspraak gelden.

Cyberdreigingen zijn niet altijd zo geavanceerd als door de bestuurders wordt gedacht. Er wordt soms ten onrechte paniek gezaaid door de media. Er wordt gedacht dat de hackers extreem intelligente middelen hebben om hun aanvallen uit te voeren. Als dit het geval is, waarom doen organisaties dan nog moeite om ons te beschermen tegen deze aanvallen? De beste vraag die bestuurders zich hierbij moeten afvragen is, wat maakt ons nou zo interessant om aan te vallen oftewel wat zijn de waarden van de organisatie en op welke systemen hebben deze betrekking?

Cybersecurity is van iedereen binnen een organisatie. Er wordt in het zelfde artikel gesteld dat cybersecurity vaak wordt belegd bij een groep experts maar dat de uitdaging juist ligt bij het integreren in de gehele organisatie.

Zoals wordt gesteld in de visie van KPMG zal effectieve informatiebeveiliging invloed moeten hebben op een samenhangend stelsel van preventieve, detectieve, correctieve en repressieve maatregelen. Dit samenhangend stelsel van maatregelen is in het onderstaande figuur uitgewerkt:



Figuur 5

Het samenhangend stelsel van maatregelen is geadresseerd en daarbij gekoppeld aan de componenten vanuit het object. De mapping van de componenten uit het object resulteert in drie hoofd aandachtsgebieden:

- Het voortbrengingsproces;
- De infrastructuur;
- De bedrijfsprocessen.

Het SOC kan een rol spelen binnen deze aandachtsgebieden. Het SOC is daarbij onderdeel van de totale informatiebeveiliging van de organisatie. De context van informatiebeveiliging wordt ook beschreven in dit hoofdstuk.

5.2. Hoofdtaken van een SOC

Er zijn drie hoofdtaken te onderscheiden bij de uitvoering van het bovengenoemde stelsel van maatregelen, namelijk sturing binnen het voortbrengingsproces, bewaking binnen de operationele omgeving en het ingrijpen in de bedrijfsprocessen.

Preventieve en detectieve maatregelen

Men moet zorgen dat zowel de voordeur als de achterdeur goed op slot zitten. Indien dit niet het geval is ontstaat het 'dweilen met de kraan open' effect. Hiertoe wordt getracht het voortbrengingsproces veilig te maken door het in voeren van Security by Design, namelijk Secure Service Development (SSD). SSD omvat onder andere betrokkenheid van consultants en architecten bij de BIA, de risicoanalyses, de Privacy Impact Analyses

(PIA's), het bijhouden van de architectuur voor informatiebeveiliging en de Attack Patterns, het participeren bij het vaststellen van specifieke beveiligingseisen, het toezien op code reviews, pentesten en scans etc.

Het onderwerp Security by Design is verder uitgewerkt in het boek 'Grip op secure software development (SSD)' van het Centrum voor Informatiebeveiliging en Privacybescherming (CIP) [CIP2014].

Binnen de infrastructuur voert men ook pentesten uit, naast observeren, continuous monitoring en scans. Daarnaast worden technische hulpmiddelen geïnstalleerd, zoals endpoint protection, IDS/IPS, firewalls, DMZ, PKI, certificaten en cryptografie. De doelstelling is de gegevens via een veilige applicatie te verwerken binnen een veilige infrastructuur en die veiligheid actief te bewaken. Het bewaken van de operationele omgeving van de IT is onderdeel van het SOC. Hiertoe beschikt het SOC over analisten, hulpmiddelen voor het observeren en analyseren, en kan pentesters inzetten. De primaire taak is de dreigingen tijdig te identificeren en daarop gepaste actie te ondernemen.

Correctieve en repressieve maatregelen

Bij een inbreuk op de informatiebeveiliging zijn niet alleen technische herstelmaatregelen nodig van beheerders, maar moet soms ook worden ingegrepen bij de gebruikers, zowel intern als extern. Hierbij kan worden gedacht aan integriteitskwesties zoals bekijken van ongewenst beeldmateriaal of aan identiteitsfraude bij de belastingdienst. Om deze reden ligt er een relatie tussen informatiebeveiliging binnen de eigen organisatie en beveiligingsfunctionarissen op de werkvloer, een Bureau Integriteit en Veiligheid, Beveiligingsambtenaren en functionarissen van het Openbaar Ministerie of Openbare Orde en Veiligheid, veiligheidsdiensten etc. Deze functionarissen hebben de taak elders in te grijpen en schade te beperken of te herstellen.

5.3. Context van Informatiebeveiliging

Informatiebeveiliging is alleen succesvol indien senior management dit uitdraagt en faciliteert. Dit houdt in dat er een CISO-rol moet zijn, levend en actueel beleid voor informatiebeveiliging (IB-beleid) en een IB-organisatie met voldoende omvang, competenties en middelen. Zolang niet aan deze randvoorwaarden is voldaan hoeft een organisatie niet te beginnen aan het inrichten van een SOC.

Kaderstellend voor informatiebeveiliging

De organisatie moet een functionaris hebben die informatiebeveiliging proactief aanstuurt. Over het algemeen is dat de CISO. Deze zorgt voor actueel IB-beleid en vooral dat het IB-beleid daadwerkelijk wordt uitgedragen en nageleefd. Hiertoe beschikt de CISO over middelen, inclusief de bevoegdheid audits te kunnen opleggen aan de organisatieonderdelen om naleving te laten verifieren.

Kennisdeling voor de Intelligence-functie

De informatie over dreigingen, IB-incidenten, kwetsbaarheden en oplossing moet worden gedeeld tussen de betrokkenen door bijvoorbeeld het bijhouden van een risicoregister, en worden gedeeld door het inregelen van verschillende processen en overlegstructuren. De analisten vernemen informatie over dreigingen en gebruiken dat voor het inrichten van hun analyses en scans, laten pentesters gericht zoeken op daaraan gerelateerde zwakheden, en lichten consultants in om passende maatregelen mee te nemen bij de specifieke beveiligingseisen bij het voortbrengingsproces. Business Damage Control ziet incidenten op de werkvloer en geeft dat door aan de analisten, die bewijsmateriaal kunnen verzamelen in de systemen en de beheerders kunnen ondersteunen met correctie of herstel etc.

Het NCSC draagt via samenwerking tussen bedrijfsleven, overheid en wetenschap bij aan het vergroten van de weerbaarheid van de Nederlandse samenleving in het digitale domein. Vanuit deze rol besteden zij aandacht aan het cyberdreigingsbeeld in Nederland. Vanuit deze analyse wordt getracht het dreigingsbeeld in kaart te brengen en daarbij handvatten te bieden zodat voor organisatie inzichtelijk wordt gemaakt waartegen men zich moet beschermen en wat hierbij de risico's zijn [NCSC2012].

Voor beveiliging is een holistische benadering nodig. Men moet de eigen objecten beschouwen binnen het overkoepelend kader van de dreigingen van buitenaf en van binnenuit, en de te beschermen belangen van de gebruikers centraal zetten.

Relatie met de gebruikersorganisatie en de bedrijfsprocessen

Analisten en consultants moeten weten wat de te beschermen belangen zijn. Die zijn voor veel instanties binnen de overheid verschillend. Zo gaat het bij de fiscale processen en sociale zekerheid om de onweerlegbaarheid van transacties door bedrijven en burgers, bij justitiële processen en opsporing om de vertrouwelijkheid en privacybescherming etc.

Ook de correctieve en repressieve maatregelen verschillen sterk per instantie. Bij de fiscale processen gaat het om schadeherstel, correcties of boetes. Bij integriteitzaken gaat het om het verzamelen van bewijsmateriaal en het treffen van personele sancties of overdracht aan Justitie etc.

Informatiebeveiliging kan alleen goed worden ingericht als er een nauwe band is met de gebruikersorganisatie, bijvoorbeeld met de Informatie Managers (IM's) en de business architecten, en met de functionarissen voor Business Damage Control.

Relatie met Functioneel en Technisch Beheer

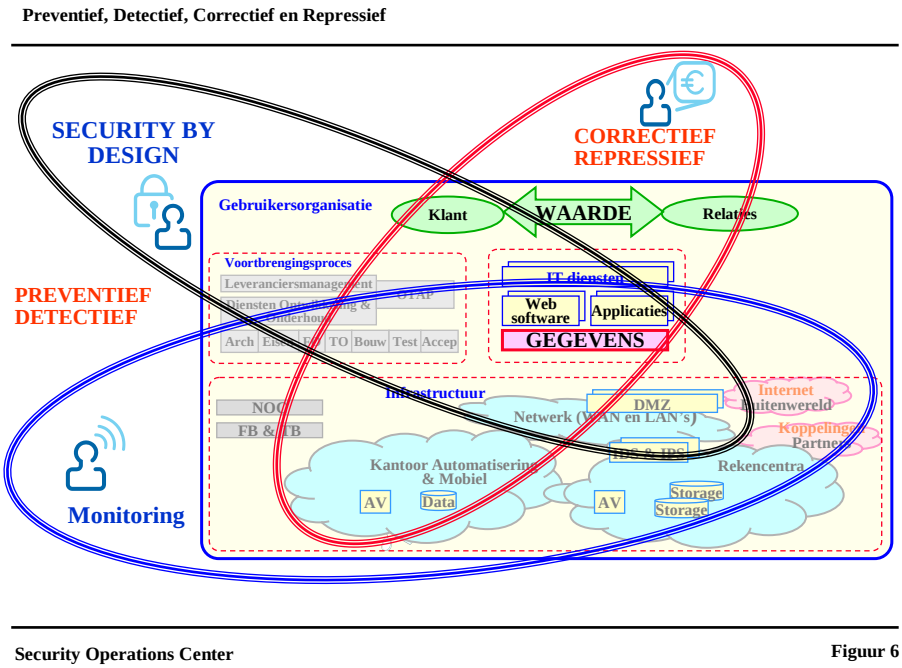
Ondanks het streven naar standaardisatie zijn alle applicatielandschappen binnen de overheid nog uniek, met name door de verschillende IV-behoeften van de verschillende instanties en de legacy-problematiek. De functionele en technische beheerders zorgen dat deze landschappen goed functioneren, en hebben hun processen aangepast aan de specifieke omgevingen. Hierbij is ieder applicatielandschap direct gekoppeld aan een bepaalde beheerorganisatie, welke alles weet van hoe de infrastructuur en applicaties in elkaar zitten en hoe die moeten worden bediend en

worden onderhouden. In het kader van Shared Service Centers is de relatie N:1, namelijk een aantal gebruikersorganisaties hebben hun eigen applicatielandschap ondergebracht bij één beheerorganisatie.

De specifieke kennis vanuit de beheerorganisatie is nodig om de verkeersstromen binnen zo een landschap te kunnen bewaken, te weten wat standaard verkeerspatronen zijn en anomalieën te kunnen detecteren. Daarnaast is deze kennis nodig bij het uitvoeren van scans en het adviseren over hardening en patches. Zo volstaat het vaak niet om een hardeningstemplate uit te rollen over de componenten, omdat dan blijkt dat legacy applicaties niet meer werken doordat zij niet gedocumenteerde functionaliteiten gebruiken. Alleen in samenwerking met de beheerders kunnen processen worden opgezet voor hardening en patches, waarbij de vereiste afwijkingen worden vastgesteld, worden gedocumenteerd en worden geborgd, in het kader van de continuïteit van de productie.

5.4. De overlap tussen preventief en detectief versus correctief en repressief

De relatie tussen de hierboven genoemde hoofdtaken binnen de informatiebeveiliging kan ruwweg worden weergegeven als:



Security by Design heeft een insteek vanuit de behoeften van de gebruikersorganisaties en de te beschermen belangen. De consultants en pentesters dragen bij een aan veilige applicatie en aan richtlijnen hoe die veilig kan worden verwerkt.

Het SOC kijkt vanuit de infrastructuur naar de applicaties en gegevensverzamelingen. Zij bewaken vanuit de techniek en zien vooral de verkeerstromen en IB-incidenten, veelal zonder een direct zicht te hebben op hoe de functionaliteit en gegevens worden gebruikt door de gebruikersorganisatie.

Business Damage Control werkt vooral vanaf de werkvloer bij de gebruikersorganisaties en heeft vaak een direct contact met de gebruikers.

De geschetste overlap geeft aan dat een set van preventieve, detectieve en correctieve maatregelen het totale object afdekt. Dit in aanvulling met een goed gepositioneerde IB-organisatie.

5.5. Conclusie

Conform de visie van KPMG stellen wij hiertoe dat het SOC integraal deel uit maakt van informatiebeveiliging. Hierbij hanteren wij de volgende definitie:

> *Een SOC is een groep competente medewerkers welke vanuit een integraal stelsel van maatregelen, gewenste bescherming biedt tegen cyberdreigingen en IT-misbruik.*

Hiertoe biedt het SOC diensten, informatie, advies en ondersteuning aan de gebruikersorganisaties en beheerorganisaties. Hierbij voeren zij een drietal hoofdtaken uit: sturing binnen het voortbrengingsproces, bewaking binnen de operationele omgeving en het ingrijpen in de bedrijfsprocessen.

6. De Meetmethode

De expertbrief van het PvIB over SOC's [PvIB2012] stelt dat taken van het SOC sterk uiteen kunnen lopen. In deze expertbrief wordt geen eenduidig takenpakket gedefinieerd. Iedere medeauteur aan dit stuk geeft een eigen definitie van taken, die naar zijn of haar mening de potentie hebben binnen het SOC te vallen. Daarbij ontstaan op gefragmenteerde wijze security taken, die mogelijk, al dan niet virtueel, binnen een SOC kunnen worden ondergebracht.

KPMG volgt een andere aanpak, namelijk een integrale benadering van informatiebeveiliging waar het SOC een logisch onderdeel van uitmaakt [KPMG 2012], [CBP 2013]. KPMG gaat uit van een samenhangend stelsel van preventieve, detectieve, correctieve en repressieve maatregelen. Deze kunnen bij diverse organisatieonderdelen worden belegd, maar moeten wel een samenhangende structuur blijven behouden.

Uit ons literatuuronderzoek blijkt dat er geen eenduidig beeld bestaat van een SOC. Iedere auteur beschrijft een eigen variant, soms vanuit een integraal perspectief, of soms als een geïsoleerde entiteit. Ook de taakverdeling varieert heel sterk.

> *In het kader van deze scriptie hebben wij de benadering van KPMG gevolgd, namelijk door het gehele stelsel als uitgangspunt te nemen. Hiervan is een deelverzameling van het stelsel relevant voor het SOC, waarbij een deel van die deelbenadering door het SOC zelf wordt uitgevoerd en de rest van deze deelverzameling kan worden gezien als randvoorwaardelijk en faciliterend. De grens tussen deze twee delen kan variëren.*

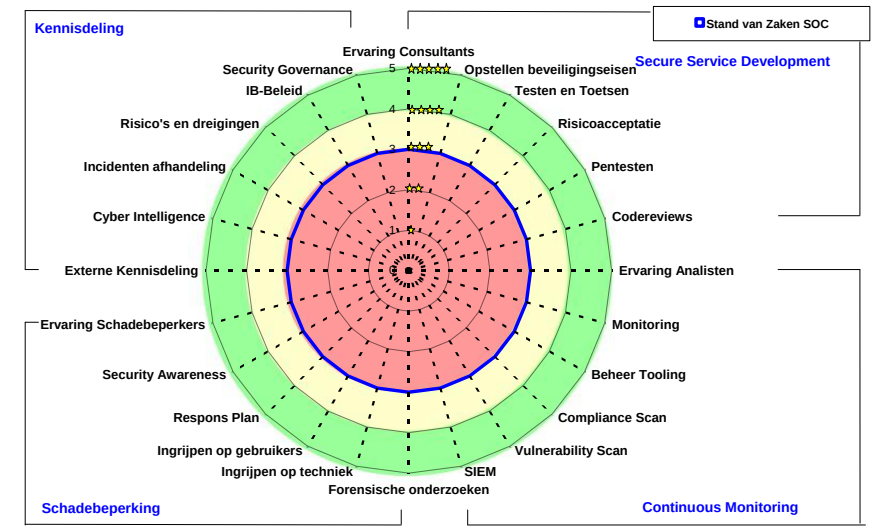
De naar onze mening relevante groepen van maatregelen die zijn gerelateerd aan een SOC hebben wij verdeeld over vier domeinen, die voor onze modelvorming van belang zijn. Dit zijn:

- Secure Service Development: De maatregelen die nodig zijn om een veilige (web)applicatie te verkrijgen;
- Continuous Monitoring: De maatregelen die nodig zijn om aanvallen vroegtijdig te ontdekken en snel actie te kunnen nemen;
- Schadebeperking: De maatregelen die nodig zijn om een aanval te stoppen en de schade zoveel mogelijk te beperken;
- Kennisdeling: De maatregelen die nodig zijn om alle betrokkenen te laten samenwerken.

Deze relevante groepen maatregelen hebben wij als assen afgebeeld in een spider diagram. Iedere as moet zijn ingevuld door de organisatie, anders kan een SOC niet effectief opereren. Een ketting is zo sterk als zijn zwakste schakel. Dit houdt niet in dat iedere as binnen het SOC valt. Maar de as moet wel ergens binnen de organisatie zijn belegd, anders vallen er gaten in de verdedigingslinie.

De voor het model van belang zijnde assen zijn:

Het Model



Security Operations Center **Figuur 7**

Iedere as representeert een groep van maatregelen en geeft hun volwassenheidsniveau aan. Hierbij is de waarde:

- Niveau 5: Gewenste situatie. Hier moet men niet de ideale situatie onder verstaan, maar het ambitieniveau van senior management gebaseerd op hun afweging van het accepteren van risico's versus de kosten van mitigerende maatregelen;
- Niveau 4: Voldoende;
- Niveau 3: Suboptimaal. Het functioneert wel, maar niet met de gewenste effectiviteit;
- Niveau 2: Zorgelijk;
- Niveau 1: Hoog risico of niet aanwezig.

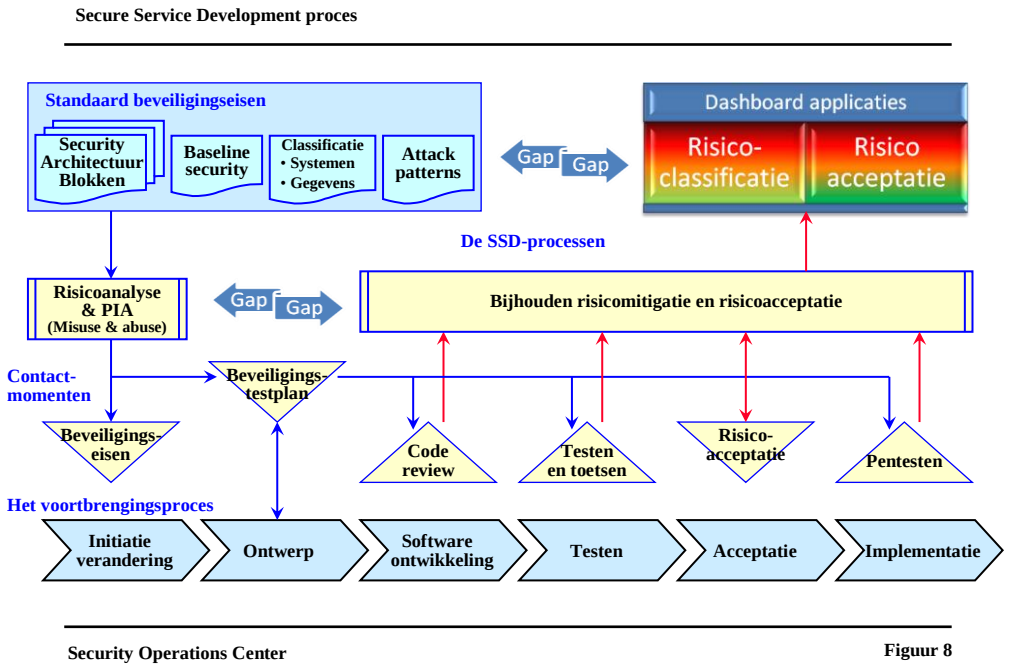
Door te werken met numerieke waarden op de assen wordt het mogelijk verschillende SOC's en hun omgevingen met elkaar te vergelijken.

Hieronder is per domein de relevantie van iedere as toegelicht.

6.1. Secure Service Development

Op het iBestuur Congres 2014 is het boek 'Grip op Secure Software Development (SSD)' gepresenteerd door Marcel Koers van UWV en Rob van der Veer van de Software Improvement Group (SIG) [CIP2014]. Deze methode beschrijft hoe grip te krijgen op de ontwikkeling van goed beveiligde software. In deze scriptie wordt naast software ook de hardware en de te leveren dienstverlening meegenomen, waarbij wij de bredere term Secure Service Development (SSD) hanteren. Naar onze mening zijn de in dit boek beschreven uitgangspunten voor SSD namelijk breder toepasbaar dan alleen voor software.

Hoewel het ontwikkelproces los staat van de detectieve functie van een SOC, bestaan er contactmomenten waarbij een SOC adviserende of controlerende taken kan leveren die bijdragen aan het veilig ontwikkelen van software en hardware. Deze contactmoment zijn beschreven in het boek en door ons als assen opgenomen in het meetmodel. De contactmomenten zijn:



Figuur 8

SSD is een uitbreiding op het bestaande voortbrengingsproces. De fase voor het opstellen van de functionele eisen en kwaliteitseisen wordt uitgebreid met een proces voor het opstellen van de specifieke beveiligingseisen voor het op te leveren product. Hiervoor is een context nodig, namelijk een voorafgaande risicoanalyse en Privacy Impact Analyse (PIA). Deze analyses worden gebaseerd op de Security Architectuur, de baseline Security, Attack Patterns en de BIV-classificatie voor het product. Hierbij staat BIV voor Beschikbaarheid, Integriteit en Vertrouwelijkheid. Deze BIV-classificatie volgt uit een Business Impact Analyse (BIA).

Uit de risicoanalyse volgt tevens het testplan voor de beveiligingsaspecten. Aan de hand van dit testplan worden code reviews, testen en pentesten uitgevoerd. Soms zijn beveiligingsmaatregelen niet op een bedrijfseconomische wijze te realiseren, waarvoor SSD een proces van risicoacceptatie beschrijft.

Op diverse punten in dit traject kan een SOC toegevoegde waarde leveren. Hieronder lopen wij langs de relevante assen:

Ervaring Consultants

Voor de ondersteuning van SSD zijn twee verschillende typen consultants nodig. Enerzijds zijn er ervaren architecten en projectleiders nodig, die de business door en door begrijpen, inclusief de voor deze business relevante dreigingen. Op basis van hun ervaring dragen zij bij aan het formuleren van de requirements, misuse cases, abuse cases etc. Zij weten de risico's op hun waarde in te schatten en ontwerpen de vereiste maatregelen op een pragmatische wijze, daarbij gebruik makend van hun expertise en ervaring.

Anderzijds zijn er gedreven IT-ers nodig in de rollen van code reviewers en pentesters. Zij hebben minder kennis nodig van de specifieke business, maar veel meer kennis van de techniek en de OWASP-aspecten. Zij moeten op de hoogte zijn van de actuele aanvalsmethoden van hackers, de cyberdreigingen, de risico's van misbruik via de IT etc. In feite zijn deze code reviewers en pentesters in vele omgevingen in te zetten, zowel binnen het ontwikkelproces als binnen een operationele omgeving.

Opstellen van de specifieke beveiligingseisen

Op basis van een risicoanalyse worden de specifieke beveiligingseisen opgesteld voor het op te leveren product. Het SOC of een beveiligingsadviseur vanuit de organisatie moet hierbij worden betrokken. Bij dit contactmoment wordt gekeken hoe de software wordt gebruikt of mogelijk kan worden misbruikt. Bij projecten worden de Project Start Architectuur (PSA) en de hierin opgenomen risicoparagraaf geëvalueerd. Hierbij wordt onder andere aandacht besteed aan de waarde en kwetsbaarheid van de gegevens. De BIV-classificatie voor het product en de gegevens bepaalt uiteindelijk welke maatregelen nodig zijn.

Code Review

Om beveiligingsrisico's van software te bepalen kan de broncode worden onderzocht via een zogenaamde code review. Deze methode vraagt om hele specifieke kennis en is tijdrovend. Gezien de kosten die hiermee gemoeid gaan is het verstandig de Business Impact Analyse (BIA) te laten bepalen in hoeverre een code review zinvol is. Mede door de specifieke kennis welke nodig is om code te controleren bestaat de kans deze taak bij het SOC te beleggen. Het doel van een code review is het vinden en oplossen van fouten in de software, die door de ontwikkelaars over het hoofd zijn gezien. Dit kan handmatig of middels analyse tools.

Testen en Toetsen

Vanuit de risicoanalyse en de vooraf definieerde 'misuse and abuse cases' wordt het testplan opgesteld. Middels het testplan wordt gecontroleerd of de services voldoen aan vooraf gedefinieerde beveiligingseisen. In het testplan wordt los van IB ook gekeken naar aspecten als functionaliteit en kwaliteit. Het SOC kan op verschillende manieren ondersteunen door bijvoorbeeld advies te leveren bij het opstellen van het testplan of erop toezien dat er voldoende testmaatregelen zijn getroffen.

Risicoacceptatie

In het geval een service of de gevraagde beveiligingsmensen niet voldoet aan de vooraf gedefinieerde beveiligingseisen, moet door de opdrachtgever een keuze worden gemaakt: De opdrachtgever accepteert het risico omdat het risico niet materieel is of de opdrachtgever besluit dat de service moet worden aangepast. Deze taak zal niet door het SOC worden uitgevoerd omdat de opdrachtgever verantwoordelijk is voor het accepteren van een risico. Wel ziet het SOC toe op het proces dat risico's daadwerkelijk zijn geaccepteerd en in hoeverre de acceptatie valide is en geen risico vormt voor de rest van de organisatie. Vanuit de lijn wordt wel advies gevraagd over bepaald risico's van het SOC.

Penetratietesten

Een penetratietest (pentest) is een test waarbij door gebruik van kwetsbaarheden wordt getracht een beveiligingssysteem te omzeilen of te doorbreken om inzicht te krijgen in de effectiviteit van dat systeem en om verbeterpunten te definiëren. Een pentest kan handmatig plaatsvinden, met gebruik van softwareprogramma's, of het kan geautomatiseerd plaatsvinden met tools als Nessus. Een pentest kan zowel als onderdeel worden uitgevoerd van het voortbrengingsproces maar kan ook worden uitgevoerd als het systeem in productie is om de status te checken van het systeem.

Zoals het GovCERT omschrijft in de white paper pentesten doe je zo [GOV2010], zijn pentesten niet zonder risico en vragen de pentesten om specifieke expertise. Het is voor de hand liggend dat deze expertise in een SOC te vinden is of extern wordt ingekocht.

6.2. Continuous Monitoring

Een SOC bewaakt de verkeersstromen en detecteert anomalieën. Hierbij worden de grote volumes aan signalen verzameld en geanalyseerd via filtering en het leggen van correlaties, met het doel de werkelijk relevante signalen te kunnen herkennen. Dit kan worden uitgevoerd door beheerders met beheertooling als IDS/IPS waarbij handmatig de logs worden bekeken. Gezien de verkeerstromen en de grote volumes aan log-gegevens welke kunnen oplopen tot honderden Gigabytes per dag, wordt gebruik gemaakt van security tooling.

Ervaring Analisten

Beveiliging is mensenwerk. De kennis achter de techniek zit bij de analisten. Tooling maakt het werk van de analisten efficiënter en effectiever maar zonder de juiste kennis is een tool niet doeltreffend. De analisten leveren uiteindelijk de input om rulesets te verbeteren en incidenten te signaleren.

Monitoring

Voordat wordt gekeken met welke technische hulpmiddelen de omgeving wordt gemonitord is het belangrijk om vast te stellen dat wat er wordt gemonitord relevant is. NIST omschrijft in een publicatie over Information Security Continuous Monitoring [NIST2011] dat monitoring van IB gaat over het in kaart brengen van kwetsbaarheden en dreigingen waardoor een organisatie op risico gebaseerde beslissingen kan nemen. Hiervoor is de eerste stap om vast te stellen welke kritische systemen moeten worden gemonitord. Het kan zijn dat een bedrijf slechts op de webapplicaties in de DMZ de monitoring goed heeft ingeregeld maar hiermee wel 80% van de gegevensstromen in kaart weet te brengen. Deze as heeft daarmee als doel in kaart te brengen in hoeverre de organisatie weet wat er zich af speelt want: ‘Meten is Weten’.

Naast vast te stellen wat moet worden gemonitord, is de analyse van de output van belang. Hoewel tooling ondersteunend kan zijn moet analyse plaatsvinden om de rulesets te verbeteren. Bevindingen en mogelijke verbeteringen kunnen leiden tot aanpassingen, bijvoorbeeld naar aanleiding van vernieuwde dreigingen. Zo ontstaat er een proces dat continu wordt verbeterd.

Beheertooling

In een beheerorganisatie bestaan diverse voorbeelden van operationele security taken. Anti Virus (AV), Intrusion Detectie en Preventie Systemen (IDS/IPS), Firewall beheer, Keymanagement zoals beheer van de PKI etc. De expertbrief van het PvIB koppelt aan deze categorie een bepaald type SOC, namelijk het Operational SOC [PvIB2011]. Hoewel deze aspecten niet dedicated security taken zijn kan de logging mogelijke verdachte gebeurtenissen en security incidenten ondervangen. Het regulier beheer van de systemen zelf is vaak elders in een organisatie belegd.

Compliance scans

Compliance scanning en vulnerability scanning liggen dicht bij elkaar. Het verschil hierin is dat bij een compliance scan wordt getoetst aan een vooraf gedefinieerde policy, zoals wet- en regelgeving, en bij een vulnerability scan wordt getoetst aan bekende kwetsbaarheden. Indien er geen kwetsbaarheden aanwezig zijn wil dat dus nog niet zegen dat het systeem voldoet aan de vooraf gedefinieerde policy [NESS2014]. Het grote voordeel dat te behalen is met het in kaart brengen van de compliance van systemen is dat de risico’s worden geïdentificeerd en de overall security wordt verbeterd. Het is ook gewenst dat de compliance structureel wordt gemeten.

Vulnerability Scans

Een vulnerability scan gaat uit van een whitebox methode en test dus op bekende kwetsbaarheden. Pinewood omschrijft in hun datasheet [PINE2013] dat de vulnerability scan de geautomatiseerde voorbereiding is op de penetratietest. De penetratie test is de handmatige validatie op deze gesignaleerde kwetsbaarheden. Ook is bij deze vorm van scanning een structurele vorm gewenst.

SIEM

Security Information and Event Monitoring (SIEM) wordt gezien als de tool welke in het SOC benodigd moet zijn. Een SIEM-systeem verzamelt (log)gegevens van diverse systemen. Door correlatie van deze gegevens wordt bruikbare informatie gegeneerd op het gebied van security incidenten. De uitdaging van een SIEM is om van de grote hoeveelheid data, honderden GB per dag, een bruikbaar signaal te genereren.

6.3. Schadebeperking

100% beveiliging is niet te realiseren. Indien de preventieve en detectieve maatregelen niet effectief zijn gebleken moet worden nagedacht over correctieve maatregelen. Dit domein heeft als doel de schade te beperken.

Ervaring Schadebeperkers

De ervaring van schadebeperkers wordt mede bepaald door de relatie welke met het SOC aanwezig is. Omdat de taken van schadebeperkers niet volledig technisch zijn georiënteerd, vertrouwen zij voor een groot deel op de kennis van een SOC. De wisselwerking tussen beide partijen resulteert in een goede visie op informatiebeveiliging en op wat risico's in de business zijn.

Respons Plan

Elke applicatie- of systeemeigenaar weet wat de waarde of classificatie van zijn systeem is. Daarom is het belangrijk om vooraf een plan op te stellen met daarin de acties die moeten worden uitgevoerd in het geval er een security calamiteit voordoet. Dit plan moet onder andere inzicht geven in welke systemen als eerste beschikbaar moeten zijn in het geval er sprake is van beperkte capaciteit.

Ingrijpen op techniek

Vaak lijkt het eenvoudig om de techniek te beheersen ten tijde van een security incident maar in werkelijkheid is dit vaak complex. Hierbij speelt het mandaat van een SOC een belangrijke rol. Indien het SOC een dreiging signaleert maar niet in staat is in te grijpen dan is het SOC weinig effectief. Zo spreekt het GvIB in een expertbrief over het stekkermandaat, oftewel wie trekt de stekker eruit op het moment dat dat nodig is [GvIB2006].

Relatie met de beheerafdeling speelt een cruciale rol. Beheerders hebben de kennis van het specifieke beheerdomein en zitten aan de knoppen. Een combinatie van kennis van zowel de beheerder als een medewerker van bijvoorbeeld het SOC kan efficiënt werken bij het oplossen van een incident.

Ingrijpen op gebruikers

Bij een inbreuk op de informatiebeveiliging zijn niet alleen technische herstelmaatregelen nodig van beheerders, maar moet soms ook worden ingegrepen bij de gebruikers. Het SOC signaleert en zal soms de gebruiker welke bewust of onbewust een incident veroorzaakt moeten stoppen. Bij structurele overtredingen dient de gebruiker te worden aangesproken.

Security Awareness

Schadebeperking kent ook een preventieve kant. Als iedere medewerker een hoog security bewustzijn heeft, zal dit sterk effect hebben op het laten dalen van de security incidenten. Echter blijkt het een grote uitdaging om medewerkers bewust te maken van de gevolgen van ongewenste handelingen. Het SOC kan een belangrijke taak spelen bij het verhogen van de security awareness binnen een organisatie door campagnes, presentaties en workshops te geven.

Forensische onderzoeken

Forensische onderzoeken worden om verschillende redenen uitgevoerd. Een forensisch onderzoek wordt uitgevoerd in het geval er een incident heeft plaatsgevonden. Een computer kan worden geanalyseerd om meer te weten te komen over het soort virus of malware dat zich in de computer bevindt of er kan een analyse worden gedaan naar bijvoorbeeld een mailbox of andere systemen om te zien hoe een gebruiker misbruik heeft weten te maken.

6.4. Kennisdeling

Informatie over dreigingen, IB-incidenten, kwetsbaarheden en mogelijke oplossingen moeten worden gedeeld tussen de betrokkenen. Dit kan door risicoregisters bij te houden of verschillende processen en overlegstructuren in te regelen. De analisten vernemen informatie over dreigingen en gebruiken die voor het inrichten van hun analyses en scans, laten pentesters gericht zoeken op daaraan gerelateerde zwakheden, en lichten consultants in om passende maatregelen mee te nemen bij de specifieke beveiligingseisen tijdens het voortbrengingsproces. Business Damage Control ziet incidenten op de werkvloer en geeft dat door aan de analisten, die bewijsmateriaal kunnen verzamelen in de systemen en de beheerders kunnen ondersteunen met correctie of herstel etc.

IB Governance

Governance is een set van verantwoordelijkheden en praktijken uitgevoerd door hoger management met als doel het versterken van de strategische richting, zorg dragen dat doelen worden gehaald, dat risicomanagement wordt toegepast en dat middelen op een verantwoorde wijze worden gebruikt[ITGI2006]. Het is belangrijk dat security commitment krijgt vanuit management, er

personen verantwoordelijk kunnen worden gesteld, en dat de security doelstelling bijdragen aan de business doelstellingen.

IB Beleid

Er dient een actueel IB-beleid aanwezig te zijn. Een IB-beleid heeft als doel om een raamwerk te bieden voor beleidsuitgangspunten. Hiertoe wordt op basis van risico's een evenwichtig stelsel van onderlinge samenhangende maatregelen ontwikkeld met als doel bescherming te bieden tegen interne en externe bedreigingen.

Risico's en dreigingen

Risico's moeten centraal worden bijgehouden. Risico's veranderen continu maar moeten wel in hun actuele vorm bekend zijn bij de verschillende organisatieonderdelen. Risico's kunnen bijvoorbeeld worden meegenomen bij het ontwikkelen van applicaties, maar ook bij het uitvoeren van projecten en zeker ook bij het gehele monitoringproces. Risico's kunnen worden ontdekt op verschillende plaatsen binnen de organisatie.

Incidenten afhandeling ISMS

Het SOC moet security incidenten centraal bijhouden. Hiervoor dient te zijn gedefinieerd wat een security incident is. Het bijhouden van incidenten op een centrale plek verhoogt het inzicht in mogelijke risico's, doordat analyses beter kunnen worden uitgevoerd. Daarbij is de afhandeling van een incident en de bewaking hiervan ook van belang. Conform ITIL is er sprake van incidenten en problemen. Management commitment is hierbij van belang zodat escalatie mogelijk is als incidenten en problemen blijven liggen.

Cyber Intelligence

Naast tools die zich richten op de interne omgeving is het belangrijk om dreigingen buiten de omgeving te signaleren om zo het totale dreigingsbeeld in kaart te brengen. Om op de hoogte te blijven van de meest actuele bedreigingen dienen SOC medewerkers verschillende fora en Social Media af te struinen. Social media leert namelijk erg veel over dreigingen maar het gebruik zelf kent ook de nodige dreiging [Trend2012]. Zoals eerder vermeld is het belangrijk aangesloten te zijn bij verschillende informatiebronnen zoals het NCSC. Het gaat erom een vertaling te maken van welke dreigingen daadwerkelijk impact hebben op de waarde van de organisatie.

Externe Kennisdeling

Intern is het belangrijk de verschillende output te verzamelen en te delen met de gehele organisatie maar extern is ook winst te behalen. Partijen als het NCSC verzamelen relevante informatie over dreigingen. Het is daarom verstandig aan te haken bij een dergelijke organisatie. Afhankelijk van de waarde is het soms nodig om met andere instanties als het AIVD, MIVD, Team Cybercrime Politie etc. nauwe contacten te onderhouden.

7. Hypothetische Praktijkuitwerkingen

Binnen het Rijk zijn verschillende SOC's in ontwikkeling of reeds operationeel. Via veldonderzoek is getracht de volgende operationele vraag te beantwoorden, als onderdeel van de tweede deelvraag:

> *Hoe zien SOC's er uit in de praktijk en is hieruit een generieke verschijningsvorm af te leiden en een decompositie van de functionaliteit?*

Voor iedere SOC hadden de oprichters een intentie. Wij hebben deze intenties ingedeeld naar de onderstaande mogelijke verschijningsvormen van een SOC. Daarnaast gaan wij in dit hoofdstuk in op de daarmee samenhangende specifieke meetpatronen.

In het navolgende hoofdstuk voeren wij de decompositie uit van de elementaire basisfuncties.

7.1. Bij het veldonderzoek onderkende verschijningsvormen van SOC's

SOC's zijn vrijwel altijd gepositioneerd binnen een technische IT-afdeling van een organisatie. Gezien de sterk technisch gerichte werkzaamheden is dit een voor de hand liggende positionering. Zoals beschreven in het voorgaande hoofdstuk, is het van belang dat een SOC invloed kan uitoefenen op het gehele stelsel van preventieve, detectieve, correctieve en repressieve maatregelen gerelateerd aan het werkgebied van het SOC.

Tijdens het veldonderzoek zijn er grofweg vier verschijningsvormen van SOC's naar voren gekomen.

- **Integraal SOC:**
  Een 'integraal SOC' is een kenniscentrum, bestaande uit een aantal competente en gedreven medewerkers, die zich met zowel het voortbrengingsproces als met beheer,infrastructuur en schadebeperking bezighoudt. Dit type SOC is geplaatst binnen de IT-organisatie en voelt zich integraal verantwoordelijk voor veel zaken die betrekking hebben op informatiebeveiliging;

- **Technisch gericht SOC:**
  Vaak zijn SOC's dichtbij of binnen het beheergedeelte van de IT-organisatie gepositioneerd en hebben daarbij voornamelijk interactie met de functionele en technische beheerders. Dit type SOC heet in onze indeling een 'technisch gericht SOC'. Zij worden niet betrokken bij het voortbrengingsproces en hebben een beperkte, veelal ad hoc relatie met de schadebeperkers die actief zijn in de business;

- **Intelligence SOC:**
  Er zijn SOC's die het analysewerk en de pentesten in eigen beheer uitvoeren en de monitoring (deels) uitbesteden aan een andere interne afdeling of een marktpartij. Zo een 'Intelligence SOC' komt bijvoorbeeld voor in situaties waarbij de infrastructuur, servers, bestu-

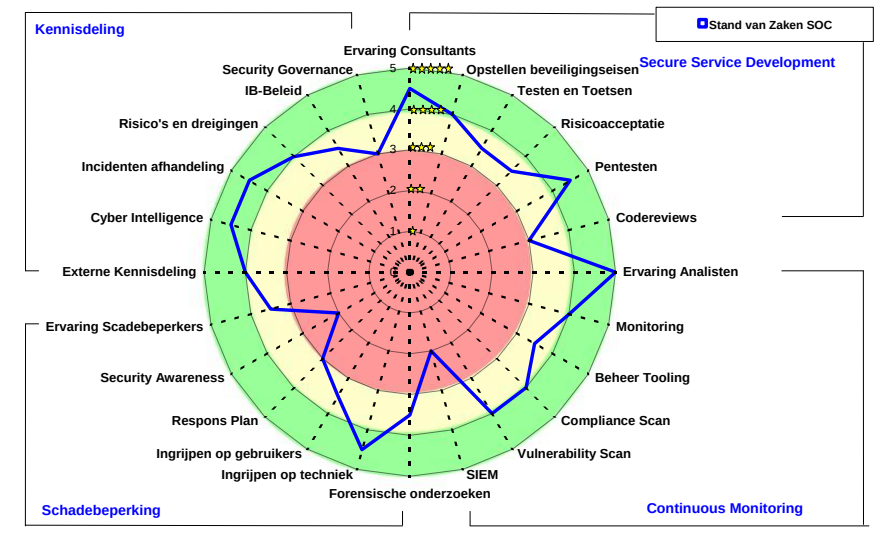
ringssystemen en middleware zijn uitbesteed. Hierbij is het de bedoeling van de opdrachtgever dat de leverancier de monitoring, filtering en selectie verzorgt en samen met de opdrachtgever de serieuze alerts en events meer diepgaand analyseert.

- **In de lijn geïntegreerde SOC-functie:**
  Soms is er wel deels SOC-functionaliteit, maar is deze niet benoemd als een entiteit. Dan wordt security niet dedicated belegd, maar is er bijvoorbeeld voor gekozen om security taken binnen de bestaande lijn te beleggen. Er zijn geen aparte security functies. Het uitgangspunt is dat alle medewerkers bewust bezig zijn met security. Er zijn wel specialisten bijvoorbeeld op het gebied van netwerken welke een sterkte security achtergrond hebben, maar zij voeren hun taken uit vanuit een netwerkbeheerders functie. De tooling zorgt op de achtergrond voor signalen welke in de lijn van incidenten wordt afgehandeld.

7.2. Integraal SOC

Voor het toelichten van onze meetmethode gaan wij uit van een hypothetische situatie. Rijksdienst ABC beschikt al jaren over een goed functionerend SOC. Dit is een Integraal SOC, dat naast Continuous Monitoring ook actief participeert bij Security by Design. Onze metingen leveren het volgende karakteristieke meetpatroon op:

Integraal SOC



Security Operations Center **Figuur 9**

Bij de hypothetische Rijksdienst ABC is de kennisdeling goed geregeld. De processen van het SOC zijn geïntegreerd in de bestaande IT-processen waardoor het SOC zicht heeft op het primaire bedrijfsproces. Dreigingen en incidenten worden vanuit het SOC gemonitord. Deze geïntegreerde aanpak zorgt ervoor dat het SOC op adequate wijze zicht houdt op de risico's.

De Rijksdienst stuurt zelf het bouwen en onderhouden van applicaties aan. Hierdoor behoudt het SOC grip gedurende het ontwikkelproces. In het kwadrant Secure Service Development is te zien dat er veel aandacht wordt besteed aan de expertise van de consultants, het opstellen van beveiligingseisen en het uitvoeren van pentesten. Deze scores duiden op een goede participatie van het SOC tijdens het voortbrengingsproces.

Het SOC is een aantal jaren operationeel. Zoals is te zien in het kwadrant Continuous Monitoring, heeft men inmiddels de beschikking over ervaren analisten en worden zowel monitoring als scanning op een professionele wijze aangepakt. De analisten kennen gradaties van juniors tot seniors waardoor de continuïteit van kennis is geborgd. Met SIEM heeft men slechte ervaringen. Er was een SIEM geïnstalleerd, maar deze bleek in de praktijk weinig toegevoegde waarde te leveren. Doordat hackers geen vast aanvalspatroon hebben, is het moeilijk de juiste rulesets te ontwikkelen. Het bleek efficiënter om zelf met queries in de loginformatie te zoeken, indien specifiek onderzoek naar dreigingen of incidenten nodig was. Daarom was besloten de SIEM tool af te schaffen.

Bij de Rijksdienst ABC is het SOC dicht bij de beheerorganisatie gepositioneerd. In het kwadrant Schadebeperking is aangegeven dat bij incidenten snel kan worden ingegrepen op de techniek of bij specifieke gebruikers. Dit wordt gerealiseerd door security als gezamenlijke verantwoordelijkheid te behandelen en goede relaties te onderhouden met de beheerorganisaties en gebruikersorganisaties. Een risico bij een integraal SOC is dat security awareness in de gebruikersorganisatie beperkt is omdat alle kennis rondom security vrijwel rondom het SOC is gegroepeerd.

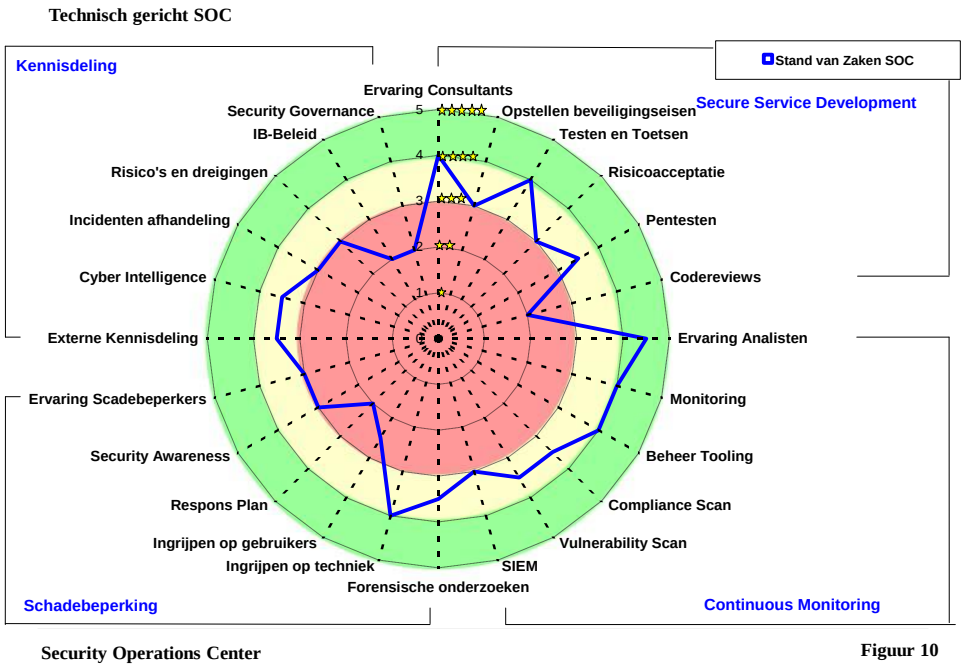
7.2.1. Conclusie Integraal SOC

Doordat een integraal SOC al een aantal jaren operationeel is, zijn er in de loop der tijd bewuste keuzes gemaakt om bepaalde taken wel of niet uit te voeren. De activiteiten die binnen de gekozen scope liggen hebben inmiddels een voldoende volwassenheidsniveau bereikt.

Een integraal SOC kan alleen succesvol zijn als de IT in eigen beheer wordt uitgevoerd voor één gebruikersorganisatie. Doordat er sprake is van korte afstanden en een gemeenschappelijk belang, is het SOC in staat efficiënt te opereren binnen alle kwadranten.

7.3. Technisch gericht SOC

Bij een andere hypothetische Rijksdienst 123 bestaat er aan de top weinig aandacht voor informatiebeveiliging, maar is men vooral bezig met het primaire bedrijfsproces. Er is een SOC operationeel, maar deze is geïnitieerd vanuit de technische invalshoek.



Figuur 10

Het gebrek aan aandacht vanuit de top blijkt duidelijk uit het kwadrant Kennisdeling. De processen rondom informatiebeveiliging worden nauwelijks aangestuurd en zijn daardoor gefragmenteerd geïmplementeerd. Door deze fragmentatie worden de betrokken medewerkers nauwelijks gestimuleerd om hun kennis te delen.

De Rijksdienst 123 kent een strikte scheiding tussen Ontwikkeling en Beheer. Zoals is te zien in het kwadrant Secure Service Development, beschikt Ontwikkeling over ervaren consultants. Deze consultants participeren bij het testen en toetsen van verschillende aspecten als Project Start Architecturen (PSA's), testplannen, abuse cases, pentesten etc. Het Technisch gericht SOC kent de ontwikkelorganisatie en geeft gedegen advies bij het proces voor risicoacceptatie. Doordat er geen integrale aansturing bestaat, worden taken vooral op ad-hoc basis uitgevoerd, bijvoorbeeld op aanvraag van een projectleider of lijnmanager. Het ontbreken van een gestructureerd proces brengt tal van risico's met zich mee. Zo bestaat er een risico dat applicaties die tijdens het voortbrengingsproces in onvoldoende mate zijn getest alsnog in productie worden genomen.

Ook binnen het kwadrant Continuous Monitoring beschikt men over ervaren analisten, die dit werk al vele jaren uitvoeren. Zij zitten midden tussen de technisch beheerders en zijn belast met allerlei security-gerelateerde taken. De lijntjes zijn kort en zij geven daadwerkelijk sturing aan

alles wat met security heeft te maken. De analisten hebben hun ervaring opgebouwd in een tijd dat er nog maar een beperkt instrumentarium beschikbaar was. Nu er meer instrumenten worden geïnstalleerd, verhoogt dat de efficiëntie van Continuous Monitoring. Alleen staat de SIEM nog in de kinderschoenen.

Uit het kwadrant Schadebeperking volgt dat de focus sterk op de techniek en het technisch ingrijpen ligt. De business staat op afstand, waardoor het lastig is grip te krijgen op het gedrag van de gebruikers. Door het gebrek aan sturing vanuit de top is er geen BIA uitgevoerd en beschikt men niet over prioriteitenlijsten in het kader van Incident en Emergency Response Plannen.

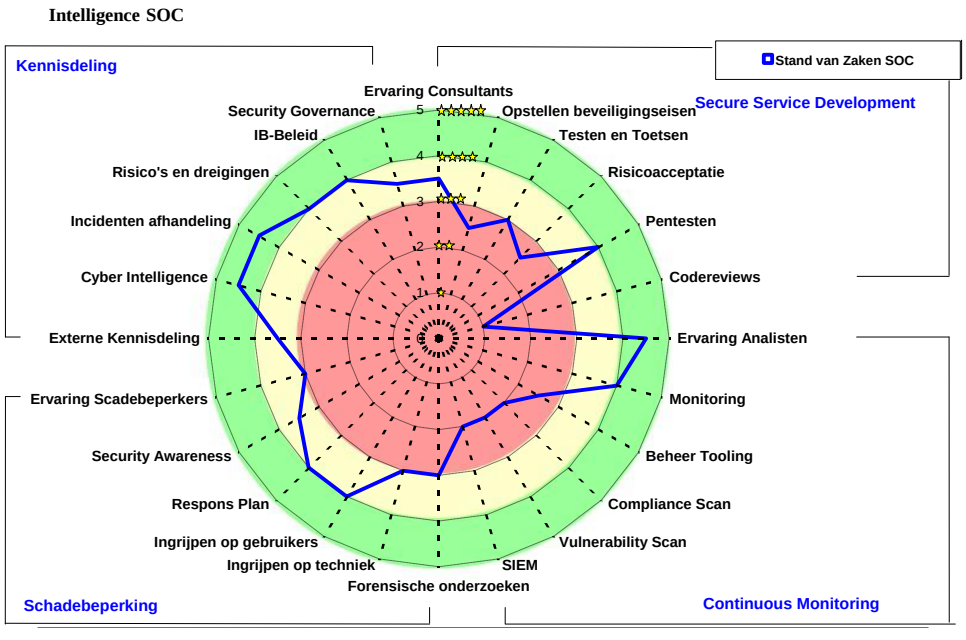
7.3.1. Conclusie Technisch gericht SOC

Een technisch gericht SOC kan prima functioneren, zeker als er analisten werkzaam zijn die dit werk al vele jaren doen. Het wel of niet succesvol zijn hangt sterk af van de competenties en persoonlijkheden van die analisten.

Zo een technisch gericht SOC is echter maar een deel van het verhaal. Als zaken als commitment bij hoger management, het informatiebeveiligingsbeleid, de CISO functie etc. niet zijn ingericht, is dat een beperking voor de effectiviteit van de overall informatiebeveiliging. Men heeft dan wel een goed instrument, namelijk het SOC, maar geen effectieve integrale beveiliging.

7.4. Intelligence SOC

Een Intelligence SOC is in feite een variant op een Computer Emergency Response Team (CERT), waarbij uitvoerende taken zijn belegd bij andere afdelingen of zijn uitbesteed.



Figuur 11

Bij het Intelligence SOC van de Rijksdienst 999 ziet men hoge scores in het kwadrant Kennisdeling, aangezien dat de primaire taak is van dit type SOC. Dit houdt in dat een groep experts continu de focus legt op de vertaling van dreigingen van buitenaf naar specifieke risico's voor de gebruikersorganisatie. Vanuit dit type SOC worden de resultaten van het analyseproces gedeeld met andere processen binnen de organisatie die raakvlakken hebben met informatiebeveiliging.

Het SOC levert bijvoorbeeld binnen het kwadrant Secure Service Development ervaren consultants en pentesters, maar bemoeit zich inhoudelijk niet met het voortbrengingsproces.

Het kwadrant Continuous Monitoring scoort relatief laag. De werkzaamheden binnen dit kwadrant zijn uitbesteed aan een leverancier. Deze doet de monitoring op een professionele wijze, maar ontbeert kennis over de bedrijfsprocessen van de gebruikers. Daardoor is niet bekend wat de specifieke risico's zijn en wordt mogelijk niet naar de juiste signalen gekeken. De context voor de interpretatie ontbreekt, waardoor de effectiviteit de mist in gaat.

Het Intelligence SOC toont overeenkomsten met het integrale SOC, maar mist de directe interactie met de beheerorganisatie doordat de monitoring is uitbesteed. Hierdoor is er veel minder interactie met de beheerders en heeft dit type SOC veel minder grip op de operationele beheerprocessen.

Het Intelligence SOC kent wel een nauwe interactie met de business. Mede hierdoor wordt het gewenste volwassenheidsniveau bereikt bij het kwadrant Schadebeperking.

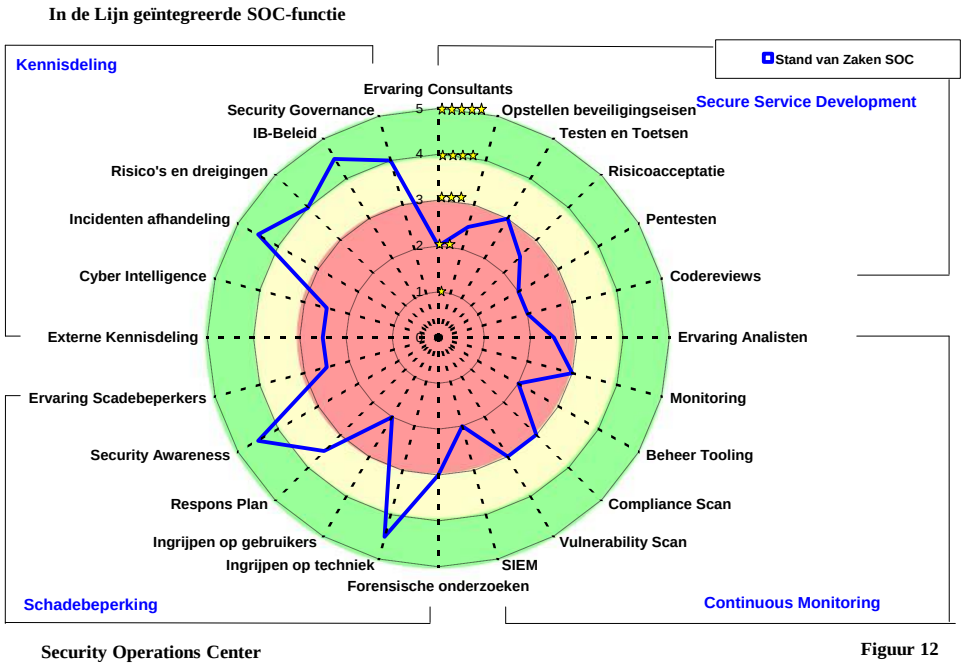
7.4.1. Conclusie Intelligence SOC

Het Intelligence SOC heeft een duidelijk inzicht in de risico's vanuit de business en is bij calamiteiten in staat het belang van de gebruikers centraal te plaatsen. De gebruikersorganisatie ziet de toegevoegde waarde van het Intelligence SOC.

Het Intelligence SOC heeft het echter veel moeilijker om iets te verbeteren bij de operationele beheerprocessen, aangezien er minder wordt samengewerkt met de beheerders.

7.5. In de lijn geïntegreerde SOC-functie

Bij de Rijksdienst XYZ is security belegd binnen de reguliere taken van lijnmanagement. Hierbij is het beleid dat alle managers en medewerkers zich bewust zijn van en verantwoordelijk zijn voor security, en deze verantwoordelijkheid vertalen naar hun dagelijkse handelen. Het SOC is hierbij een kleine uitvoerende organisatie, veelal gericht op het uitvoeren van technische metingen, ter ondersteuning van de taken van lijnmanagement. De meetprocessen zijn zo ingericht dat deze signalen opleveren die door de lijn kunnen worden afgehandeld. Het aantal dedicated security functies is hierbij beperkt, doordat security een collectieve verantwoordelijkheid is. Wij noemen deze aanpak een 'in de lijn geïntegreerde SOC-functie'. Het meetpatroon ziet er als volgt uit:



Figuur 12

In dit meetpatroon zien wij een sterke nadruk op de kwadranten Kennisdeling en Schadebeperking. De governance is binnen deze organisatie goed ingeregeld, wat duidt op aandacht voor security vanuit management. Door deze 'tone at the top' is er sprake van een hoog security bewustzijn onder de gebruikers. De lijn wordt conform een gedegen ingericht proces ondersteund. Dit heeft als voordeel dat incidenten, risico's en dreigingen centraal worden bijgehouden.

Binnen het kwadrant Secure Service Development levert het SOC geen enkele ondersteuning. Het opstellen van beveiligingseisen, het uitvoeren van testen en toetsen, het opdracht geven aan pentesters etc. is nu een collectieve verantwoordelijkheid van management. Maar als niemand daarvoor specifiek wordt aangewezen, is er weinig synergie bij deze activiteiten en is het een open vraag of die altijd consequent worden uitgevoerd.

Het kwadrant Continuous Monitoring valt binnen het verantwoordelijkheidsgebied van het SOC, maar er is onvoldoende aandacht en expertise om de monitoring adequaat en effectief in te regelen. Dit komt mede omdat de aansturende taak hiertoe niet specifiek bij één manager is belegd, maar bij het collectief.

7.5.1. Conclusie in de lijn geïntegreerde SOC-functie

De filosofie achter deze verschijningsvorm is interessant, maar blijkt gezien de complexiteit van een SOC niet effectief. Een SOC werkt alleen goed als iemand er expliciet voor verantwoordelijk is en zorgt dat alle taken op een verantwoorde wijze worden ingevuld, binnen de context van een volledig stelsel van maatregelen voor informatiebeveiliging.

7.6. Conclusie voor de verschijningsvormen

De meetmethode bevindt zich nog in een experimenteel stadium. Wij hebben deze methode ontwikkeld, gebruikt tijdens de interviews om een beeld te krijgen van de sterke en zwakke punten van ieder verschijningsvorm van een SOC, en de assen iteratief verbeterd op basis van voortschrijdend inzicht.

De indeling van de assen in vier kwadranten blijkt nuttig te zijn om snel een visueel beeld te krijgen over de verschijningsvorm van het SOC en hun focus.

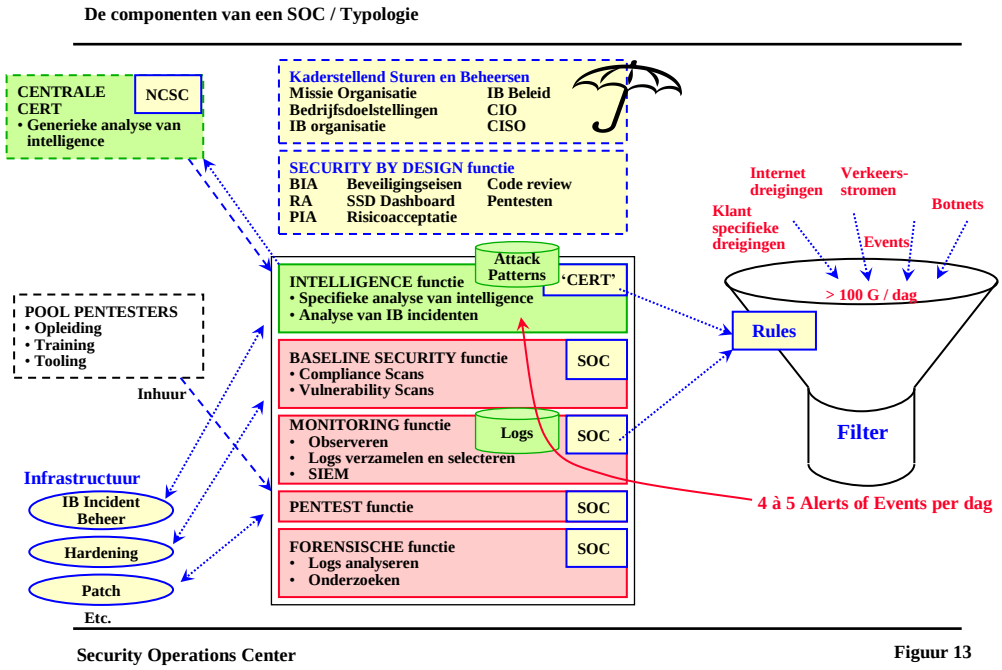
Bij de metingen in de praktijk herkenden wij snel de verschijningsvormen van de bezochte SOC's, met elk specifieke sterke en zwakke punten binnen een kwadrant. Echter is de waarde van de assen binnen deze verschijningsvormen fluctuerend. De fluctuaties geven aan dat er andere bepalende factoren zijn binnen een SOC, die de volledigheid van het takenpakket sterk beïnvloeden.

Dit leidde tot nader onderzoek, namelijk het uitvoeren van een decompositie van de elementaire basisfuncties binnen een SOC. Dit zijn in feite de bouwblokken waaruit het SOC is opgebouwd. In het volgende hoofdstuk gaan wij in op deze analyse.

8. De typologie van een SOC: de elementaire basisfuncties

Dit hoofdstuk beschrijft het model voor een SOC, bestaande uit vijf elementaire basisfuncties. Deze decompositie is van belang om mogelijk samenwerkingsverbanden per basisfunctie uit te kunnen werken.

Een SOC functioneert alleen binnen een bepaalde context. De vereiste bovenliggende structuur is op de onderstaande figuur ingetekend als een paraplu 'IB Sturen en Beheersen', met de CISO, IB-beleid etc., en Security by Design.



Figuur 13

De vijf basisfuncties van het SOC zijn hieronder uitgewerkt.

8.1. Intelligence-functie

Een SOC heeft een kern van ervaren analisten nodig, die zich richten op de specifieke dreigingen en beveiligingsincidenten die relevant zijn voor de gebruikersorganisatie. Zij analyseren en geven richtlijnen aan de andere functies binnen het SOC, aan de beheerders, aan de schadebeperkers binnen de gebruikersorganisaties en aan degenen die werkzaam zijn binnen het voortbrengingsproces. Tevens bepalen deze analisten hoe de rules van de SIEM moeten worden ingesteld, welke scans moeten worden gedraaid, welke pentesten moeten worden uitgevoerd etc.

De Intelligence-functie is de kern van het SOC. De opzet van deze functie vertoont overeenkomsten met een Computer Emergency Response Team (CERT), dat zich ook bezighoudt met drei-

gingen en het analyseren van incidenten. De naam CERT kan echter niet formeel worden gehanteerd, omdat dit een gedeponeerd handelsmerk is van het CERT/CC van de Carnegie Mellon University.

8.2. Baseline Security-functie

Een SOC ziet toe op de technische aspecten van de uitrol policy zoals de BIR, het proces van hardening van de technische componenten, het proces voor het aanbrengen van patches en de onderhoudsniveaus. Hiertoe worden naast preventieve instructies aan beheerders scans uitgevoerd om de compliance en kwetsbaarheden vast te stellen.

Het SOC draagt bij aan het opstellen van de Baseline Security, namelijk het stelsel van maatregelen voor informatiebeveiliging en privacybescherming. Deze Baseline Security is afgeleid van de security architectuur van de organisatie en de classificatie voor BIV voor de systemen en gegevens, die volgt uit de BIA. Via risicoanalyses en PIA's wordt bepaald welke maatregelen absoluut van belang zijn. Nadat die maatregelen door de beheerders zijn geïmplementeerd, worden deze met scans gecontroleerd. Afwijkingen worden gerapporteerd aan de beheerders en aan de Intelligence-functie. Deze ziet er op toe dat de afwijkingen worden opgelost.

8.3. Monitoring-functie

Een SOC bewaakt de verkeersstromen en probeert anomalieën te detecteren. Hierbij worden de grote volumes aan signalen verzameld en geanalyseerd via filtering en het leggen van correlaties, met het doel de werkelijk relevante signalen te kunnen herkennen.

Dagelijks genereren de netwerken en systemen grote volumes aan loggegevens, waarbij volumes van 100 tot 200 Gigabyte niet ongebruikelijk zijn. Het kernprobleem bij het gebruik van een SIEM is de rulesets zo in te regelen dat de werkelijk belangrijke alerts of events worden gefilterd uit deze omvangrijke stroom. Slechts enkele alerts of events per dag zijn kandidaat voor het initiëren van een verder onderzoek.

Op dit vlak hebben de onderzoekers in de private sector voorbeelden gezien waarbij SOC's meer grip hebben gekregen op het proces van selecteren en filteren. De effectiviteit van dit proces wordt grotendeels bepaald door de competenties en gedrevenheid van de betrokken analisten, oftewel dit is mensenwerk waarvoor (zeer) goede mensen nodig zijn. Die goede analisten zijn schaars.

8.4. Pentest-functie

Zowel in de productieomgeving als bij het voortbrengingsproces worden pentesten uitgevoerd, met name gericht op de door de Intelligence-functie aangegeven aandachtspunten. Het doel is robuustheid te creëren.

De pentesten in de productieomgeving zijn bedoeld als een noodzakelijk aanvulling op de Baseline Security en de scans. Via de scans worden maatregelen routinematig nagelopen en afwijkingen op de instellingen gesignaleerd, maar kan men geen sluipwegen ontdekken. Via de pentesten

wordt gecontroleerd of er omwegen zijn naar belangrijke functionaliteit of gegevens, die door kwaadwillende kunnen worden misbruikt. Populair gesproken, via de scan wordt gekeken of de voordeur dicht is, bij de pentest wordt er flink aan gerammeld om te kijken of hij niet uit de schoot springt bij een flinke schop en of men niet via de regenpijp naar een open raam kan klauteren.

Pentesten hebben enige verwantschap met technische IT-audits, waarbij technisch geschoolde IT-auditors diep in de infrastructuur speuren naar technische zwakheden.

8.5. Forensische functie

Het SOC assisteert forensische onderzoekers bij het verzamelen en analyseren van bewijsmateriaal.

Veelal ligt de leiding van dit soort onderzoeken bij functionarissen die een formele opsporingsbevoegdheid hebben. De medewerkers van het SOC zijn uitvoerend op het technische vlak. Hieronder vallen bijvoorbeeld activiteiten zoals het veilig stellen van computers en storage, en het analyseren van harde schijven, log bestanden, mail etc., waarbij veel aandacht nodig is voor een zorgvuldige ‘chain of custody’ voor het bewijsmateriaal.

Bij de meeste SOC’s is het forensische werk een parttime nevenfunctie, die wordt uitgevoerd door medewerkers die binnen de andere basisfuncties werkzaam zijn.

8.6. Andere varianten

Deze vijf basisfuncties vormen de typologie van het SOC. Voor iedere basisfunctie gelden specifieke randvoorwaarden, die invloed hebben op mogelijke of vereiste samenwerkingsverbanden met andere betrokken partijen.

Naast de bovenstaande basisfuncties wordt een SOC soms uitgebreid met andere taken zoals het:

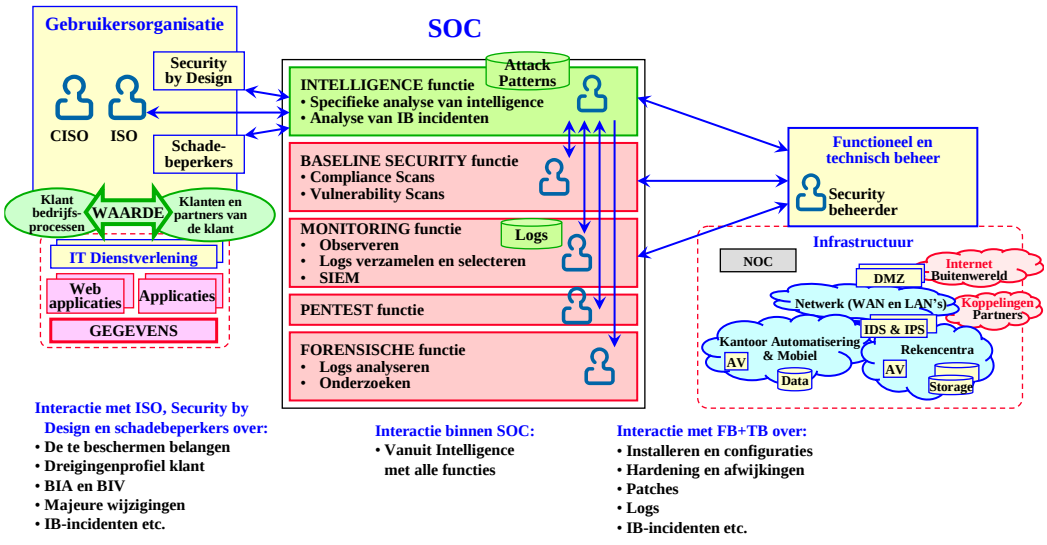
- Bewaken voor de beveiliging van SCADA computers en Industrial Controls Systems (ICS) voor procesautomatisering. Hierbij is ook een relatie met de vitale infrastructuur, zoals energievoorziening, bruggen sluizen etc. [TREN2013];
- Controleren op te ‘hoge bevoegdheden’;
- Adviseren over IB-vraagstukken;
- Beheren van het ontheffingsproces voor baselines;
- Beheren van endpoint protection, PKI, certificaten en cryptografie etc.;
- Beoordelen van wijzigingsverzoeken.

De diversiteit aan functies die binnen de verschillende SOC’s worden opgenomen maakt een vergelijking van de bestaande SOC’s gecompliceerd. Met name ter bevordering van de vergelijkbaarheid van SOC’s is in dit rapport een standaardmodel ontwikkeld voor de basisfuncties.

9. Verankering van de interacties van SOC

Een SOC functioneert binnen een bepaalde context. Voor ieder van de vijf basisfuncties wordt hieronder de relatie met de gebruikersorganisatie en de beheerorganisatie behandeld. Hierbij worden de ondeelbare relaties geïdentificeerd, namelijk die relaties die onmisbaar zijn voor het functioneren van het SOC. Deze worden de 'verankeringen' genoemd.

Ondeelbare relaties: Verankering van een SOC



Security Operations Center **Figuur 14**

Bij het definiëren van de mogelijke kansen voor gezamenlijke dienstverlening of centralisatie van een SOC kunnen de verankeringen als belemmeringen worden beschouwd. Als een van de SOC-functies wordt verhuisd naar een ander SOC, mogen de ondeelbare relaties namelijk niet worden verbroken.

9.1. Verankering van de Intelligence-functie

De Intelligence-functie richt zich enerzijds op de specifieke IT-dienstverlening aan een specifieke gebruikersorganisatie en de dreigingen voor hun bedrijfsprocessen. Er moet een sterke band zijn met de betreffende gebruikersorganisatie, en het SOC moet goed inzicht hebben in hun te beschermen belangen en de voor hen relevante dreigingen. Die zullen voor verschillende instanties geheel verschillend zijn.

In de bovenstaande figuur is een relatie ingetekend met de CISO van die organisatie, eventueel gedelegeerd aan een Information Security Officer (ISO) binnen de gebruikersorganisatie. Deze ISO treedt op als liaison en schakelt met de Intelligence-functie over het specifieke dreigingenprofiel voor de gebruikers, afhankelijk van hun bedrijfsdoelstellingen en omgeving, de BIA en BIV classificatie, majeure wijzigingen in het IT-gebruik, IB-incidenten etc.

De Intelligence-functie richt zich anderzijds op bepaalde domeinen met hun eigen functioneel en technisch beheer. In dit kader is samenwerking alleen mogelijk als er een nauwe band kan worden opgebouwd met de betreffende beheerorganisatie. Het begrip 'nauwe band' moet heel strikt worden gelezen, de relatie werkt alleen als de SOC-medewerker fysiek in de directe omgeving van de beheerders zit en bij hen in en uit kan lopen. Bij druk bezette beheerders heeft het geen zin per telefoon of email na te vragen waarom er ergens ongebruikelijk verkeer loopt of voor te stellen een beheerhandeling uit te voeren. Daarop komt of geen reactie, of het gebeurt met een forse vertraging.

De Intelligence-functie kent hierdoor twee verankeringen, namelijk de sterke band met de gebruikersorganisatie en de nauwe band met de beheerorganisatie.

9.2. Verankering van de Baseline Security-functie en Monitoring-functie

De Baseline Security en Monitoring-functies hebben niet of nauwelijks een relatie met de gebruikersorganisatie. Zij zijn echter wel nauw gekoppeld aan de activiteiten van de functionele en technische beheerders en aan de te bewaken infrastructuur.

De beheerders moeten voor de medewerkers van het SOC handelingen uitvoeren, zoals het installeren van de benodigde scansoftware, het installeren van agents en collectors op servers en componenten, paden door het netwerk beschikbaar maken etc. Daarnaast moeten de beheerders specifieke vragen kunnen beantwoorden om de meetresultaten te kunnen interpreteren. Zonder kennis van de specifieke infrastructuur en configuraties, verkeersstromen, applicaties en beheerhandelingen zitten de analisten 'in het donker te staren'.

Om deze twee basisfuncties succesvol uit te kunnen voeren is een directe interactie nodig, of een hiërarchische relatie waarbij beheerders direct kunnen worden betrokken. In de praktijk zullen de Baseline Security en Monitoring-functies vooral succesvol zijn als dit deel van het SOC in de directe omgeving van de beheerders is gepositioneerd.

De Baseline Security en Monitoring-functies kennen hierdoor één verankering, namelijk de nauwe band met de beheerorganisatie.

9.3. Verankering van de Pentest-functie

Het uitvoeren van pentesten of technische IT-audits is een relatief routinematige activiteit, waarvoor geen of slechts een beperkte kennis nodig is van de specifieke kenmerken van de gebruikersorganisatie. De specifieke kennis van de bedrijfsprocessen zit vooral bij de opdrachtgever, die de uit te voeren testen en audits omschrijft, conform de behoefte van de specifieke omgeving en de randvoorwaarden, en gericht op de gebruikte technologieën. Veelal zal de Intelligence-functie optreden als opdrachtgever.

Voor de competenties van de in te zetten pentesters kan een generiek profiel worden gehanteerd per te beschouwen type van platform, met uitzondering voor onderzoeken in omgevingen waar wordt gewerkt met procesautomatisering, zoals SCADA.

De pentesten of technische IT-audits kennen geen verankering, maar wel een diversiteit in profilering afhankelijk van de te beschouwen technologieën.

9.4. Verankering van de Forensische functie

De door de Forensische functie uit te voeren activiteiten zijn sterk gekoppeld aan de specifieke gebruikersorganisatie, hun bedrijfsprocessen en de voor hen relevante dreigingen. Veelal worden hiervoor SOC-medewerkers ingezet die een hoofdtaak hebben binnen de Intelligence, Baseline Security of Monitoring-functies. Zij worden vooral uitvoerend ingezet door een Bureau Integriteit of andere onderzoekers, omdat zij specifieke kennis hebben van de infrastructuur en weten waar zij het vereiste bewijsmateriaal kunnen vinden en hoe zij dat moeten interpreteren.

De Forensische functie kent vooral een verticale verankering, namelijk een directe relatie met de andere functies binnen het SOC. Hiermee is er een indirecte verankering in de richting van de gebruikersorganisatie en de beheerorganisatie.

9.5. Relatie met datacenters

In het kader van de Compacte Rijksdienst streeft de overheid naar consolidaties van het aantal datacenters.

Zoals hierboven omschreven, richt een SOC zich op een specifieke gebruikersorganisatie en een specifieke beheerorganisatie. In de moderne opzet zijn de grote datacenters verdeeld in vele suites en omgevingen, die worden beheerd door vele verschillende beheerorganisaties. Daardoor kan een datacenter niet als een te beschermen entiteit worden gezien vanuit het oogpunt van een SOC, maar als een verzameling van losse omgevingen. Daarnaast maken veel beheerorganisaties gebruik van (delen) van verschillende datacenters, onder andere in het kader van het streven naar continuïteit van de dienstverlening. Er is hierbij sprake van een N:M mapping tussen beheerorganisaties en datacenters. Het datacenter wordt in deze context slechts gezien als een ondergeschikt middel, namelijk als een van de componenten van de beheerde infrastructuur.

> *Een SOC gekoppeld aan een specifiek datacenter zal niet tot het gewenste doel leiden, omdat informatiebeveiliging is gekoppeld aan een beheerorganisatie en vele van deze beheerorganisaties ieder een deel van het datacenter gebruiken. Een uitzondering hierop is een datacenter dat alleen door één specifieke beheerorganisatie wordt gebruikt of per keten van informatie wordt ingericht.*

10. Mogelijkheden tot samenwerking van SOC's binnen de overheid

De derde deelvraag luidt:

> *Kan een SOC dusdanig worden ingericht dat deze ook diensten kan leveren aan meerdere gebruikersorganisaties en beheerorganisaties binnen de overheid?*

Op basis van het in dit rapport gepresenteerde model met de vijf basisfuncties en de identificatie van de verankeringen, kan per basisfunctie de mogelijkheid tot samenwerking of gezamenlijke dienstverlening worden verkend.

10.1. Mogelijke werkvormen voor een SOC

Om een effectief SOC op te zetten binnen de overheid zijn een aantal werkvormen gedefinieerd:

- Ieder Shared Service Center of losse beheerorganisatie zet een eigen SOC op. Dit zijn 'decentrale SOC's'. Hierbij is het mogelijk gezamenlijk best practices te ontwikkelen, kennis te delen of via het marktprincipe aan elkaar diensten te leveren;
- Binnen een keten wordt een SOC opgezet, dat werkzaam is voor de ketenpartners. Dit is een 'Ketengericht SOC';
- De grote Ministeries zetten ieder een eigen 'Departementaal SOC' op, of enkele Ministeries gezamenlijk een '(Multi)departementaal SOC';
- Er komt één fysiek Rijks SOC, dat diensten levert aan alle Shared Service Center en losse beheerorganisaties.

Hieronder wordt voor iedere optie de voor- en nadelen besproken, gevolgd door een advies.

10.2. Een decentrale aanpak voor SOC's

Op dit moment is het woord 'SOC' een hype. Vele instanties hebben hiervan gehoord en willen zelf een SOC. Op enkele uitzonderingen na, slagen deze instanties er tot nu toe niet in een SOC op te zetten dat effectief en efficiënt hun robuustheid verhoogt tegen cyberaanvallen en IT-misbruik. Het verschil tussen het wel of het niet succesvol zijn zit vooral in de personen die beschikbaar zijn om als de drijvende kracht(en) achter het SOC te fungeren, de vaardigheden van de in te zetten analisten en de attitude van senior management.

De enkele SOC's die als succesvol kunnen worden gezien zijn langere tijd geleden gestart en beschikken inmiddels over de juiste leidinggevenden en medewerkers met de vereiste competenties en vaardigheden. Zij hebben een langzaam groeipad gevolgd naar volwassenheid.

De overige SOC's in opbouw worden geconfronteerd met een schaarsheid aan geschikte medewerkers of met senior management die haar prioriteiten bij andere zaken legt dan bij het SOC. Daarnaast is het inrichten van een SOC een complex gebeuren, omdat dit gebeurt op het koppelvlak van de bedrijfsprocessen en de harde IT, en tevens een kostbare operatie.

> *Wij zijn van mening dat weinig instanties binnen de overheid succesvol zullen zijn in het opzetten van nieuwe effectief en efficiënt opererende SOC's, met name door de*

schaarsheid aan competenties en door de huidige prioriteitsstelling bij senior management in het kader van de lopende bezuinigingsprogramma's.

Indien men kiest voor decentrale SOC's, worden hieronder twee mogelijke vormen van samenwerking besproken, inclusief enkele door de geïnterviewden genoemde belemmeringen.

10.2.1. Het delen van best practices, kennis en vaardigheden

Decentrale SOC's hebben vergelijkbare behoeften aan methoden en hulpmiddelen om effectief te kunnen opereren. Dit betreft onder andere het omgaan met de legacy problematiek bij hardening en patches, het uitvoeren van de scan, het verwerken van de grote bulk aan signalen, het filteren en analyseren etc.

Onder regie van een centrale instantie kan een onderzoeksprogramma worden ontwikkeld, waarbij bepaalde decentrale SOC's onderzoeksvragen krijgen toegewezen. De resultaten van hun onderzoek worden daarna gedeeld met de overige instanties in de vorm van best practices. Een nadeel van deze aanpak is dat men voor de voortgang afhankelijk is van decentrale managers en medewerkers, waarbij er geen zekerheid is dat dit tot bruikbare resultaten leidt.

Tijdens de interviews is de behoefte uitgesproken voor een centraal punt binnen de overheid waar op operationeel niveau preventief informatie wordt verzameld en geanalyseerd, en de conclusies van de analyses worden uitgewisseld met andere instanties. Momenteel heeft men het gevoel dat iedereen 'het wiel moet uitvinden' voor het inrichten van het analyseproces.

Een voor de hand liggend gebied om samen te werken betreft de pentesten en technische IT-audits. Hiervoor worden al medewerkers ingehuurd van andere instanties, of bij commerciële partijen. Veel instanties kijken namelijk op tegen de kosten om deze vaardigheden binnen hun eigen organisatie op te bouwen en te onderhouden.

10.2.2. Het leveren van diensten van een decentrale SOC aan een ander SOC

De samenwerking tussen decentrale SOC's is op dit moment beperkt tot incidentele uitwisseling van ervaringen, onder andere via NCSC en CIP. Tijdens het veldonderzoek is de wens tot intensievere samenwerking uitgesproken en het leveren van diensten over en weer, maar zijn de volgende belemmeringen genoemd:

- **Politieke en bestuurlijke verantwoordelijkheid:**
  Op dit moment wordt de IT nog aangestuurd door individuele partijen binnen de overheid. Overheidsinstanties onder een Ministerie zijn nog terughoudend een verantwoordelijkheid op zich te nemen om bij te dragen aan het verbeteren van de informatiebeveiliging binnen een domein dat onder een ander Ministerie valt;

- **Gebrek aan visie:**
  De BIR en BIG richten zich op individuele organisaties. Er is geen Rijksbrede visie en geen Rijksbreed beleid op welke wijze individuele instanties moeten samenwerken. Op dit vlak valt een afwachtende houding waar te nemen bij die instanties;

- **Consolidatie datacenters:**
  Het Programma Consolidatie Datacenters (PCDC) is onderdeel van het Uitvoeringsprogramma voor een Compacte Rijksdienst. Een aantal partijen geven aan dat een goed functionerend SOC kan worden gezien als een concurrentievoordeel bij de selectie van Rijksdatacenters. Kennisdeling kan dan worden gezien als het helpen van de concurrent;

- **Financiële verrekening:**
  Een operationeel SOC is kostbaar. Als vuistregel kan men uitgaan van tussen de € 1,5 en 2 miljoen per jaar. Voor de meeste instanties geldt dat informatiebeveiliging niet integraal wordt gebudgetteerd, maar onderdeel is van begrotingen voor afdelingen, projecten etc. Dit impliceert, zeker in deze tijd van bezuinigingen, dat het niet eenvoudig is budgetten beschikbaar te stellen om SOC-diensten in te kopen;

- **Portfolio:**
  Er is nog geen portfolio beschikbaar voor de diensten die een SOC zou kunnen leveren aan andere instanties, met een prijsstelling. De inmiddels operationele SOC's functioneren alleen binnen hun eigen omgeving, en de overige SOC's zijn nog in opbouw. Hierdoor is er nog geen markt van vraag en aanbod binnen de overheid.

Op dit moment fungeert NCSC als centraal meldpunt voor beveiligingsincidenten en communiceert met verschillende instanties in het geval van een virusuitbraak of een calamiteit. Deze informatie-uitwisseling is vooral incident gedreven. Er is geen rechtstreekse uitwisseling van informatie en geen kennisdeling op het gebied van dreigingen, intelligence etc. tussen de verschillende SOC's.

10.3. Een aanpak per relevante keten: Het Ketengerichte SOC

De overheid kent een aantal ketens tussen overheidsinstanties, agentschappen, ZBO's etc., gericht op een bepaald type dienstverlening aan de burgers.

Het is mogelijk functies van SOC's te combineren per keten. Hierbij richt men zich op samenwerking tussen gebruikersorganisaties die verwante bedrijfsprocessen hebben of binnen dezelfde keten opereren. Het gaat hierbij voornamelijk om de aard van de gegevens.

> *Wij zijn van mening dat een ketengerichte aanpak voor een SOC mogelijkheden tot succes biedt. Daarbij moet men wel de verankering borgen naar voor het SOC nieuwe gebruikersorganisaties en beheerorganisatie.*

Op de borging van de verankering wordt verder ingegaan in de volgende sectie.

10.4. Een aanpak per relevant Ministerie: Het (Multi)Departementale SOC

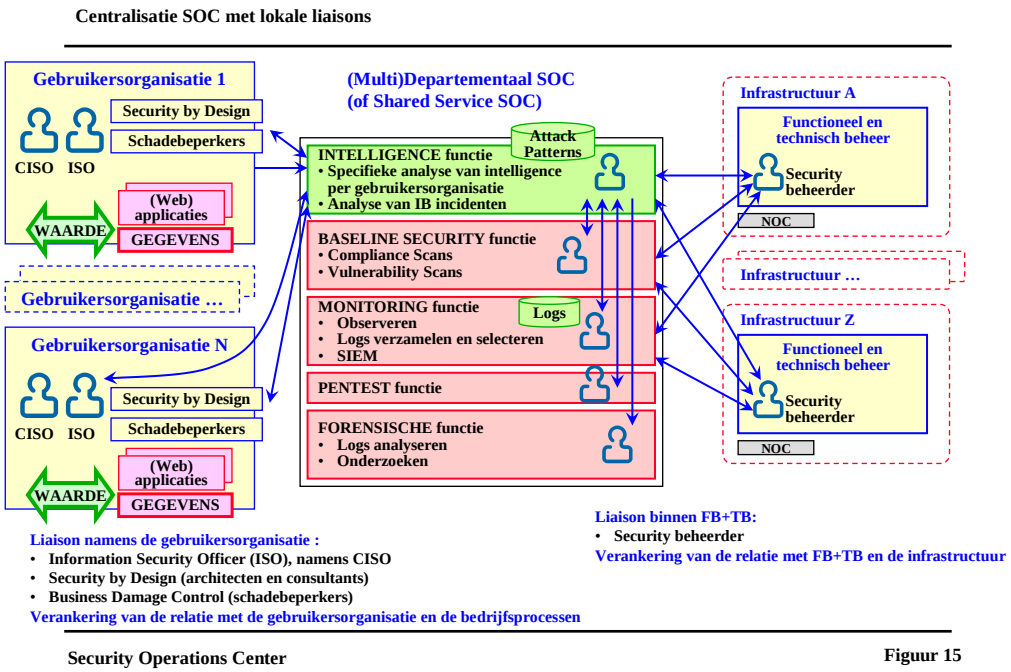
Sommige Ministeries beheren grote delen van de ketens. Een alternatief voor decentrale of ketengerichte SOC's kan zijn een SOC in te richten voor de daartoe in aanmerking komende Ministeries. Hierbij is het ook mogelijk dat enkele Ministeries samenwerken. Zo een (Multi)Departementaal SOC moet dan alle instanties ondersteunen die onder de verantwoordelijkheid van het Ministerie of de samenwerkende Ministeries vallen en de bijbehorende relevante delen van de ketens. Hierbij komt de financiering uit departementale middelen.

> *Wij zijn van mening dat een (Multi)Departementaal SOC een hogere mate van slagingskans heeft dan een nieuw in te richten decentraal SOC of een nieuw in te richten ketengericht SOC, met name omdat een kerndepartement over meer middelen beschikt, een sterker mandaat kan geven en veelal een stabieler beleid kan voeren dan lagere instanties.*

Via het centraliseren van de SOC-functies binnen enkele SOC's bundelt men de reeds aanwezige competenties en creëert men zo enkele krachtige centra waar nieuwe analisten kunnen worden opgeleid en waar methoden en technieken kunnen worden ontwikkeld.

De (Multi)Departementale SOC's vormen gezamenlijk het virtueel Rijks SOC, waarbij via mandatering hiërarchische relaties worden ingericht met de participerende partijen. Zowel door mandatering als door het beschikbaar stellen van centrale middelen van Ministeries elimineert men de huidige lokale vrijblijvendheid bij het wel of niet implementeren van (delen) van de BIR en is men niet meer afhankelijk van de attitude van senior management binnen de individuele instanties.

Zo een (Multi)Departementaal SOC heeft de volgende vorm:



Figuur 15

Bij een centralisatie van functies van het SOC is het van essentieel belang de verankering te borgen met de doelgroepen waarvoor het SOC werkzaam is.

10.4.1. De gebruikersorganisaties, bedrijfsprocessen en de te beschermen belangen

De gebruikersorganisaties zijn gebonden aan het BIR. Dit impliceert dat zij hun informatiebeveiliging hebben ingericht, beschikken over een CISO of daaraan gelijkwaardige rol, BIA's en risicoanalyses uitvoeren etc. Voor de verankering van de relatie met het SOC komt de CISO in aanmerking of, bij grotere instanties, een Information Security Officer (ISO), die in de nabijheid van de CISO is gepositioneerd. Deze ISO treedt op als vooruitgeschoven post voor het SOC en acteert als een vast aanspreekpunt binnen de Intelligence-functie.

In het kader van de BIA's en risicoanalyses zijn de architecten en consultants betrokken bij Security by Design en zo goed op de hoogte van de te beschermen belangen en de vereiste maatregelen voor informatiebeveiliging. Binnen deze groep wordt ook een vast aanspreekpunt aangewezen voor de Intelligence-functie.

De derde partij die relevant is binnen de gebruikersorganisatie zijn de schadebeperkers, die bezig zijn met Business Damage Control, en natuurlijk met Damage Prevention. Een of meer van hen acteren ook als aanspreekpunt.

Aan de kant van het SOC is er een kernteam bij de Intelligence-functie, waarbij een van de analisten optreedt in een 'account rol' voor de betreffende instantie. Via deze relatie tussen de gebruikersorganisatie en de relatiebedienende analist wordt overlegd over het specifieke dreigingenprofiel van de instantie, de BIA's en BIV classificaties, majeure wijzigingen in de bedrijfsprocessen of het applicatielandschap, IB-incidenten etc.

De Intelligence-functie bouwt initieel een beeld op van de instantie met het specifieke dreigingenprofiel, hun te beschermen belangen etc., en onderhoudt dit beeld. Daarnaast bouwt het SOC een relatie op met de bovengenoemde aanspreekpunten, om een toegevoegde waarde te leveren aan de bescherming van de bedrijfsprocessen, de gebruikers en de daar van belang zijnde waarden.

10.4.2. Functioneel en Technisch Beheer, en de infrastructuur

De beheerorganisaties binnen het Rijk zijn ook gebonden aan het BIR. Dit impliceert dat zij hun processen hebben geformaliseerd en dat die aanstuurbaar zijn. Voor de verankering van de relatie met het SOC komt een gespecialiseerde Security Beheerder in aanmerking, die op de werkvloer zit bij de functionele en technische beheerders.

De Security Beheerder treedt ook op als een vooruitgeschoven post van het SOC, met een vast aanspreekpunt in de vorm van een relatiebedienende analist binnen de Intelligence-functie. Via deze relatie wordt overlegd over het installeren van programmatuur voor de scans en monitoring, configuraties, het proces voor hardening en afwijkingen, het proces en de prioriteitsstelling voor patches, het vullen en kopiëren van logs, IB-incidenten etc.

De Intelligence-functie bouwt initieel de techniek op die nodig is voor het bewaken en monitoren van de infrastructuur, samen met Functioneel en Technisch Beheer. Nadat de verkeerstromen voor de scans en monitoring lopen, verloopt het dagelijks contact via de Security Beheerder.

10.4.3. Alternatief voor de verankering via vaste aanspreekpunten

Bij het opstellen van het model voor een SOC is een afweging gemaakt tussen een relatiebedienende analist ter plaatse bij de gebruikersorganisatie en de beheerorganisatie, versus vaste aanspreekpunten zoals een ISO, een Security Beheerder etc. Het voordeel van een analist ter plaatse is de nauwe band met de overige analisten binnen de Intelligence-functie. Het nadeel is dat deze analist dan in feite twee werkplekken heeft, namelijk bij de centrale Intelligence-functie en ter plaatse. Zo een gekunstelde constructie brengt het risico met zich mee dat de analist in de praktijk slecht op een van de twee werkplekken daadwerkelijk actief is en het andere deel van zijn functie niet of deels invult.

Om een heldere rolbeschrijving te krijgen is daarom gekozen voor de relatie via de ISO, Security by Design, schadebeperkers en de Security Beheerder, die fulltime opereren binnen hun eigen organisatie. Daarbij zijn zij verantwoordelijk voor de relatie met het SOC en hebben daar hun vaste aanspreekpunt. Vanuit organisatorisch oogpunt heeft zo een relatie meer kans van slagen dan het alternatief van een pendelende analist.

10.5. Een fysiek Rijks SOC

Gezien de schaarsheid aan analisten zijn er argumenten om één fysiek Rijks SOC te overwegen. Dit heeft voordelen in het kader van centralisatie van het opleiden en trainen van analisten, en het ontwikkelen van methoden en technieken.

Gezien de complexe opbouw en grote omvang van de Rijksoverheid versus het zelfstandige optreden van de Ministeries bestaat het risico dat zo een Rijks SOC onvoldoende grip zal krijgen op de gebruikersorganisaties. Hierbij zal met name de 'span of control' van de analisten binnen de Intelligence-functie een beperking kunnen zijn.

Tijdens de interviews en besprekingen in het kader van dit onderzoek is het alternatief van een Rijks SOC besproken. Daarbij bleek niet echt een draagvlak voor een mega-aanpak.

> *Wij zijn van mening dat één centraal fysiek Rijks SOC bij de huidige inrichting van IT bij de overheid nog een brug te ver is. Zo een Rijks SOC zou voordelen hebben op het vlak van efficiëntie, maar zal naar verwachting niet of nauwelijks in staat zijn om alle banden op te bouwen met alle Rijksdiensten, Diensten, Agentschappen, ZBO's etc. Bij de overwegingen voor centralisatie moet men de 'span of control' van de analisten binnen het SOC nauwlettend bewaken.*

10.6. Mogelijke scenario's voor schaalvergroting

Op basis van de bovenstaande afwegingen, kunnen scenario's worden opgesteld voor SOC-functies die meer dan een gebruikersorganisatie en meer dan een beheerorganisatie bedienen. De scenario's gelden voor het Ketengerichte SOC en het (Multi)Departementale SOC, die beide kunnen worden gezien als een Shared Service SOC.

10.6.1. Centralisatie van de Intelligence-functie

De Intelligence-functie van het SOC bestaat uit een kerngroep van competente analisten, die relaties onderhouden met informatiebronnen zoals NCSC etc., bezig zijn met dreigingsbeelden, analyses van dreigingen en IB-incidenten, en sturing geven aan de scans, monitoring, pentesten en technische IT-audits.

Deze analisten doen dit voor alle aangesloten doelgroepen. Voor een deel is hun werk generiek, gericht op de algemene bedreigingen en de standaardmaatregelen voor beveiliging, en voor een deel specifiek voor een of meer bepaalde doelgroepen. Voor het specifieke deel worden ook de relatiebedienende analisten ingezet, die een directe band hebben met de betreffende doelgroep. Hierbij wordt de verankering van de relatie benut, namelijk de ISO of de Security Beheerder die fulltime binnen de doelgroep aanwezig is.

10.6.2. Centralisatie van de Baseline Security-functie

De Baseline Security-functie kan geheel worden gecentraliseerd, als de programmatuur voor scans wordt gestandaardiseerd. Dit heeft een kostenbesparend effect, aangezien licenties via schaalvergroting goedkoper worden en de vereiste vaardigheden worden gebundeld.

Er wordt gebruik gemaakt van de lokale Security Beheerders voor het onderhoud van de lokale programmatuur voor de scans, wijzigingen en het verkrijgen van nadere informatie als de interpretatie van de uitkomsten van de scans dat vereisen.

10.6.3. Centralisatie van de Monitoring-functie

De Monitoring-functie betreft met name het doorlopend kopiëren van logs via eigen programmatuur, zoals agents, of rechtstreeks. Bij de inrichting moet worden gezorgd voor netwerkpaden met voldoende bandbreedte en voldoende centrale opslagruimte.

Het centraal uitvoeren van deze functie leidt ook tot besparingen op licenties en menskracht, ten opzichte van een decentrale opzet. Hierbij wordt ook gebruik gemaakt van de lokale Security Beheerder voor ondersteuning. Met betrekking tot de kosten van opslagruimte zal centralisatie deze kosten niet verhogen, aangezien het volume aan log informatie bij centrale of decentrale opslag hetzelfde blijft.

Centralisatie heeft als voordeel dat bij het correleren van logs en IB-incidenten men een breder beeld heeft, namelijk over alle aangesloten instanties heen.

10.7. Financiering van de dagelijkse werkzaamheden van het SOC

Met de hierboven gekozen opzet voor het Ketengerichte SOC en het (Multi)Departementale SOC moet de financiering van de dagelijkse werkzaamheden zo eenvoudig mogelijk worden ingericht.

De lokale ISO en Security beheerder worden betaald door de betreffende organisatie, en de kosten voor de centrale analisten, licenties en apparatuur komen uit centrale middelen. Met een eigen budget is het SOC in staat de juiste deskundigen aan te trekken en een eigen opleidings- en trainingsprogramma op te zetten, en haar werkzaamheden in te plannen onafhankelijk van de attitudes van management binnen de verschillende aangesloten instanties.

10.8. 7x24 beschikbaarheid van het SOC

Het onderzoek heeft geef duidelijkheid gegeven over de behoefte van de Rijksoverheid aan 7x24 uur beschikbaarheid van een SOC of SIEM-functionaliteit. Geen enkele instantie heeft dit ingericht.

De argumenten tegen 7x24 uur bewaking door een SOC zijn:

- Op dit moment worden weinig cyberaanvallen realtime gedetecteerd, mogelijk doordat de Rijksoverheid weinig wordt aangevallen of doordat men de meetinstrumenten mist om zulke aanvallen te zien en te herkennen. Hierdoor zal een nacht- of weekenddienst saai zijn;
- Onderzoeken naar IT-misbruik vinden bijna altijd achteraf plaats. Dergelijke onderzoeken worden geïnitieerd door signalen vanuit de gebruikersorganisatie of de schadebeperkers, of door het achteraf signaleren van ongebruikelijke verkeersstromen of vastgelegde activiteiten. Deze werkzaamheden kunnen prima tijdens kantoortijd worden uitgevoerd;
- Voor het herkennen van een DDoS-aanval is geen permanente bewaking nodig door een SOC. Zodra er een DDoS-aanval plaatsvindt wordt die snel gemeld door de getroffen gebruikers en burgers via het reguliere incidentkanaal. Via dit kanaal worden daarna de medewerkers van het SOC en de beheerders opgeroepen om de draaiboeken voor de DDoS-tegenmaatregelen te activeren;
- Het SOC heeft niet de taak nieuwe vormen van virussen en malware te identificeren. Die informatie krijgt het SOC aangeleverd via de leveranciers en NCSC. Het treffen van lokale maatregelen is vrijwel nooit zo tijdkritisch dat dit niet kan wachten tot een volgende werkdag;
- Veel medewerkers van de overheid werken vooral tijdens kantooruren. Een massale virusuitbraak buiten werktijd is weinig waarschijnlijk, omdat dan de werkstations binnen de kantoren toch niet worden gebruikt. Als er een virusuitbraak plaatsvindt op mobiele apparatuur, wordt die door de getroffen gebruikers snel gemeld via het reguliere incidentkanaal;
- Er zijn nog geen ‘gouden rulesets’ voor een SIEM, die automatisch relevante alerts en events tonen aan het SOC. Met de huidige aanpak van analyseren en spitten door logs en waarnemingen van vastgelegde verkeersstromen kan de bewakende functie prima tijdens kantooruren worden vervuld.

Een afweging van wel of niet 7x24 uur moet men baseren op een dreigingsanalyse. Per dreiging wordt dan bepaald of die buiten kantoortijd schade kan veroorzaken voor de overheid of burgers. Uit zo een analyse volgen de eisen voor de beschikbaarheid van het SOC.

Vooralsnog volstaan alle geïnterviewde instanties met een SOC nog men met consignatiediensten, waarbij een of meer medewerkers van het SOC oproepbaar zijn.

10.9. Praktisch probleem bij Logging en Monitoring

Het blijkt dat de analysewerkzaamheden van een SOC in de praktijk worden bemoeilijkt door de gigantische stroom aan loginformatie. Uit de meeste interviews blijkt dat analisten moeite hebben met de volumes en het zoeken van de speld in de hooiberg, of beter gezegd de relevante speld tussen de grote aantallen niet-relevante spelden.

Men wordt hierbij geconfronteerd met een oud probleem uit de IT, namelijk dat de logmechanismen indertijd zijn ontwikkeld door IT-ers als een hulpmiddel voor henzelf om fouten te kunnen opsporen en onderhoud uit te kunnen voeren. Deze logs waren nimmer bedoeld als hulpmiddel voor beveiliging. Hierdoor staan voor het analyseren van cyberaanvallen en IT-misbruik niet de juiste gegevens in een hanteerbaar formaat in de logs, maar wel heel veel technische details waar de analisten weinig tot niets aan hebben. Door deze reden is de aanpak met SIEM in feite nergens werkelijk succesvol.

Als de overheid SOC's op een bredere schaal zou willen inzetten dan vandaag, is het nodig onderzoek uit te voeren naar de wijze van logging op de IT-componenten binnen het overheidsdomein en te bepalen welke informatie aanvullend moet worden verzameld en welke informatie geen nut heeft. Door al direct op de verzamelpunten, namelijk de servers en netwerkcomponenten, te selecteren en loginformatie te verrijken beperkt men de hoeveelheid loginformatie en verhoogt men de kans op succesvolle analysewerkzaamheden.

11. Evaluatie van het groeiproces van ons model

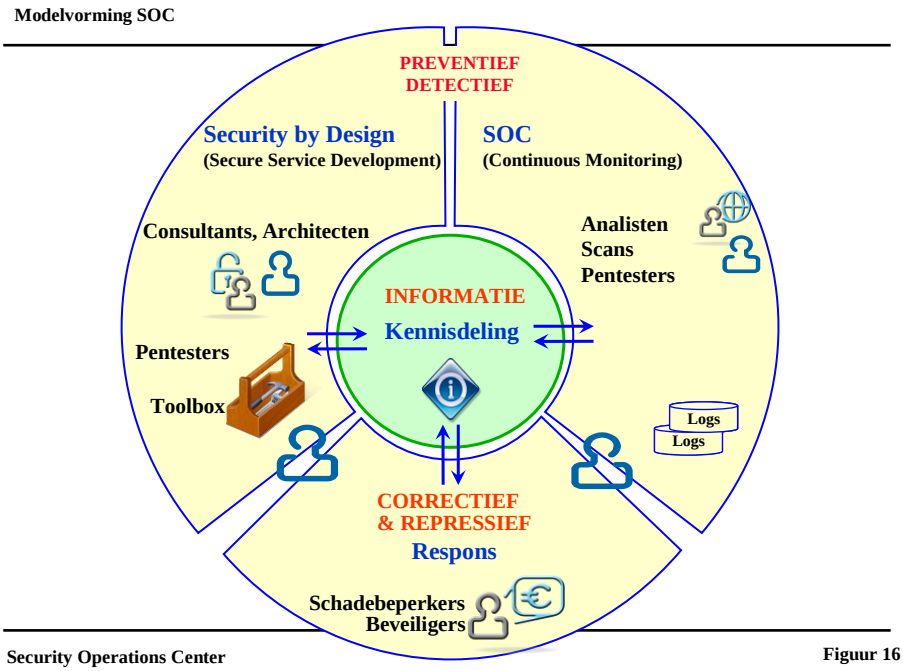
In de scriptie is getracht een model te ontwikkelen welke breed toepasbaar is. Draagvlak van de professionals is hierbij een succesfactor. In dit hoofdstuk wordt beschreven hoe het proces van het ontwikkelde model is verlopen. Hiermee wordt de volgende deelvraag beantwoord.

Wat is de professionele opinie van vakgenoten over het ontwikkelde model?

Wij zijn dit onderzoek begonnen tijdens een opdracht voor de inrichting van een integraal SOC bij een Rijksdienst. Dit SOC participeert in zowel het leveren van adviesdiensten en Security by Design voor het voortbrengingsproces als het uitvoeren van Continuous Monitoring voor de operationele omgeving. Wij veronderstelden dat een integraal SOC overal zou kunnen worden geïmplementeerd. Het aspect 'integraal' bleek niet te landen bij veel betrokkenen. Er bleef een forse kloof bestaan tussen de consultants voor het voortbrengingsproces en de analisten en beheerders die bezig zijn met Continuous Monitoring. Ook bij andere organisaties blijken Ontwikkeling en Beheer twee gescheiden werelden te zijn, die zich niet gemakkelijk laten combineren.

11.1. Gestart op een verkeerd spoor

In ons eerste ontwerp hebben wij de volgende taken geïntegreerd in het SOC:



Figuur 16

In dit ontwerp voor een integraal SOC staat een team van IT-beveiligingsexperts centraal, dat de coördinatie verzorgt voor een groot aantal IB-kwesties en proactieve en reactieve IB-diensten

levert. Dit is in feite een IB-supermarkt die de organisatiebrede informatiebeveiliging voor haar rekening neemt.

De proactieve IB-diensten zijn gericht op het voorkomen van incidenten door het vervaardigen van veilige applicaties via een veilig voortbrengingsproces, die worden verwerkt in een veilige omgeving. Dit omvat onder andere ook bewustwording, training, het bewaken van de configuraties en het inrichten van technische beveiligingsmaatregelen.

De reactieve IB-diensten zijn gericht op het bewaken van de operationele omgeving, het afhandelen van incidenten, het minimaliseren van de hieruit voortkomende schade en het analyseren van eventuele oorzaken.

Dit integrale ontwerp was veel te optimistisch. Wij veronderstelden, naar nu blijkt ten onrechte, dat het SOC verantwoordelijk kan zijn voor organisatiebrede informatiebeveiliging. Dit past niet bij de expertise van veel medewerkers van een SOC en wordt ook niet geaccepteerd door de lijn. De lijn heeft altijd een verantwoordelijkheid op het gebied van informatiebeveiliging want je bent zo sterk als je zwakste schakel.

Een variant op de integrale aanpak is integratie van informatiebeveiliging in het voortbrengingsproces en de operationele procedures, waarbij gebruikt wordt gemaakt van de medewerkers van het SOC ter ondersteuning van deze processen. De beveiliging zit dan niet zozeer in het SOC als wel in de integrale aanpak van informatiebeveiliging binnen de organisatie. Hierbij is de expertise ondersteunend.

Dit is ook conform de visie van KPMG, waarbij IB vanuit een preventief, detectief en correctief perspectief moet worden aangepakt. In de KPMG-visie maakt het SOC een integraal onderdeel uit van de andere IB gerelateerde gebieden. Zonder een juiste positionering is een SOC niet effectief. Deze visie heeft ons geholpen om tot het besluit te komen dat een ‘integraal SOC’ als een zelfstandige entiteit een doodlopende weg is. Wij hebben deze ontwerpplannen gearchiveerd als ‘op dit moment nog een brug te ver’.

11.2. Een hernieuwde poging

Wij zijn teruggegaan naar de tekentafel en hebben een blanco vel gepakt. Daarbij is het SOC gepositioneerd ten opzichte van de verschillende IB-verantwoordelijkheidsgebieden binnen een organisatie en is een decompositie uitgevoerd, op basis van onze waarnemingen bij een tiental bestaande SOC’s binnen en buiten de overheid. Wij hebben gekeken welke functies daar worden uitgevoerd en hoe het SOC de diverse IB-processen kan ondersteunen.

Dit heeft geleid tot het identificeren van de elementaire basisfuncties van een SOC, zoals echte SOC’s die leveren. Het zo ontwikkelde model geeft een duidelijke basis die voor elke organisatie toepasbaar is. De daadwerkelijke invulling van specifieke taken hebben wij buiten ons model gelaten, omdat iedere organisatie zelf wil en zal bepalen hoe zij een bepaalde basiscomponent inrichten. De meerwaarde is voornamelijk gevonden in de relatie en verankering van de basisfuncties met de betreffende IB-verantwoordelijkheidsgebieden.

Door de decompositie en de identificatie van de elementaire basisfuncties bleek dat het complexe probleem opeens veel eenvoudiger werd. Met de integrale aanpak liep van alles door elkaar heen en kwamen wij niet tot een ontwerp dat acceptabel was voor zowel Ontwikkeling als voor Beheer. Door terug te gaan naar vijf elementaire basisfuncties voor een SOC, die ieder kunnen worden gekoppeld aan bepaalde IB-verantwoordelijkheidsgebieden, kregen wij draagvlak. Het lijnmanagement herkende nu de verschillende taken van het SOC en zag de toegevoegde waarde daarvan in.

11.3. De ontvangen feedback

Onze eerste poging met een integraal SOC is in feite een mislukking geworden. Het lukte niet om Ontwikkeling en Beheer op een lijn te krijgen. Dit theoretische model is indertijd wel besproken met een aantal vakgenoten, die op zich gecharmeerd waren van de integrale benadering en daar voordelen in zagen. Echter, de theorie paste niet bij de praktijk.

De tweede poging leidde tot veel meer draagvlak. Het model met de decompositie en de vijf elementaire basisfuncties was herkenbaar voor de werkvloer en de stakeholders van het SOC. Dit model is gepresenteerd voor diverse commissies en werkgroepen, en is besproken met diverse leidinggevenden en medewerkers binnen het vakgebied informatiebeveiliging.

Dit model loste allerlei praktische problemen op. Als voorbeeld, in de integrale aanpak gingen wij uit van pentesters die fysiek zijn gepositioneerd binnen Security by Design en binnen Continuous Monitoring. Dit was verwarrend omdat hierbij pentesters als personen werden ingetekend in bepaalde vakken. In het nieuwe model hebben wij de handeling ‘uitvoeren van een pentest’ ingetekend in deze beide vakken en de pentester als persoon buiten het model gezet. In de praktijk kunnen uren worden ingehuurd voor het uitvoeren van deze handelingen, of kan de persoon in een bepaald vak zitten en kan zijn expertise worden gebruikt in een ander vak. Het ontkoppelen van handelingen en personen maakte het model organisatieonafhankelijk toepasbaar.

11.4. Adviezen voor verder onderzoek

Het meetmodel wordt vooralsnog door vakgenoten gezien als een beschrijvend model en biedt nog niet de mogelijkheid kwantitatief de effectiviteit van een SOC te meten of uit te drukken. Het advies is om een diepgaande analyse te doen en mogelijke KPI’s af te leiden voor de bestaande assen. Als een SOC meetbaar wordt gemaakt kan er vanuit de organisatie sturing plaatsvinden. Via deze KPI’s kan concreet worden vastgesteld of het SOC daadwerkelijk effectief opereert. De onderzoekers zien dit als een nuttige uitbreiding en stellen voor dit op te pakken als een mogelijke vervolgstudie.

12. Conclusies

Op grond van de bovenstaande uiteenzetting kunnen wij nu antwoord geven op de geformuleerde deelvragen. De deelvragen hebben een inventariserend, analyserend en beschouwend karakter.

12.1. Deelvraag 1: Literatuurstudie naar een model

In de literatuur zijn een groot aantal white papers te vinden over SOC's. Deze artikelen zijn voorbeelden van een eigen implementatie of zijn opgesteld vanuit een commercieel uitgangspunt. In het inventariserende onderzoeksonderdeel is antwoord gegeven op de volgende deelvraag:

> *Is er vanuit de literatuur een model of een voorbeeld beschikbaar voor de inrichting van een effectief SOC of voor de optimalisatie van een bestaand SOC?*

Het woord SOC is een modewoord geworden. Allerlei organisaties die zich bedreigd voelen door cyberaanvallen en IT-misbruik denken dat het inrichten van een SOC de ultieme oplossing is. Zij zien het SOC dan als '*Haarlemmerolie*', namelijk een oplossing voor alles, en zoeken die oplossing veelal in de techniek. Men schaft te snel dure meetinstrumenten aan, zoekt er wat mensen bij die er enig verstand van lijken te hebben, en verklaart het SOC voor geopend en operationeel actief. Als wij dan vragen wat de missie en het werkgebied van het SOC is, zijn de antwoorden vaak vaag. Dan blijkt dat die organisaties geen duidelijk beeld hebben van hun eigen risico's, de voor hen van belang zijnde dreigingen en geen integrale aanpak hebben om hun risico's te mitigeren. Het geheel hangt een beetje als los zand aan elkaar, doordat vrijwel geen enkele organisatie werkt vanuit een gestructureerde Business Impact Analyse (BIA) voor hun primaire proces en de daarbinnen gebruikte informatiesystemen en gegevensverzamelingen.

Het probleem van deze organisaties is dat de literatuur geen eenduidig model biedt van een SOC. De taken, verantwoordelijkheden en bevoegdheden van de in de literatuur beschreven SOC's zijn erg uiteenlopend en worden min of meer op basis van eigen inzichten en behoeften van de eigen organisatie bepaald [PvIB2012]. Hierbij ontbreekt het aan een wetenschappelijke basis. De literatuur wordt niet concreet over welke taken wel of niet bij een SOC kunnen of moeten worden belegd. White papers van toonaangevende leveranciers zoals HP, RSA, McAfee IBM gaan elk uit van hun eigen specifieke inrichting, die allemaal totaal verschillend zijn. Doordat er geen synergie bestaat over de invulling van een SOC, ontstaan op gefragmenteerde en bijna willekeurige wijze security taken die mogelijk binnen een SOC kunnen worden ondergebracht. Er is sprake van een diffuus beeld van de term SOC.

In realiteit hebben de meeste bestaande SOC's een beperkt werk- en verantwoordelijkheidsgebied, en functioneren goed binnen hun eigen specifieke omgeving met de door hen tot volwassenheid gebrachte meetmethoden en hun eigen ervaren analisten en security experts. Zij zijn echter geen model voor de inrichting van een nieuwe SOC binnen een andere organisatie. Het antwoord op de eerste deelvraag is:

Vanuit de literatuur is er geen eenduidig model of voorbeeld, maar blijkt een forse pluriformiteit in inrichtingen van SOC's. Men kan bijna zeggen, het vliegt alle richtingen uit.

12.2. Deelvraag 2: Veldonderzoek voor daadwerkelijke realisaties

Naast de literatuurstudie hebben wij gelijktijdig veldonderzoek uitgevoerd. Hierbij is een tiental SOC's bezocht binnen de overheid. Aan de hand van onze waarnemingen is getracht antwoord te geven op de volgende deelvraag:

Hoe zien SOC's er uit in de praktijk en is hieruit een generieke verschijningsvorm af te leiden en een decompositie van de functionaliteit?

Wij hebben het gehele stelsel van maatregelen voor informatiebeveiliging en privacybescherming als uitgangspunt genomen, dus gekozen voor een brede benadering, en daar vandaan geredeneerd naar een meetmodel. Onze doelstelling is een meetmodel te ontwikkelen dat toepasbaar is op elk type organisatie.

Conform de eerste helft van deelvraag 2 hebben wij aan de hand van de resultaten van ons veldonderzoek gezocht naar de meest gebruikelijke verschijningsvormen. Dit zijn:

- **Integraal SOC:**
  Als alle security taken bij het integrale SOC zijn belegd met een brede focus op zowel het voortbrengingsproces, beheer en infrastructuur, alsmede schadebeperking, is er sprake van een 'integraal SOC'. Dit type SOC is geplaatst binnen de IT-organisatie en is integraal verantwoordelijk voor veel zaken die betrekking hebben op informatiebeveiliging;

- **Technisch gericht SOC:**
  Een technisch gericht SOC legt de nadruk op de techniek en heeft daarbij een (zeer) goede relatie met de technische beheerders en tevens met een aantal functionele beheerders. Zij worden niet betrokken bij het voortbrengingsproces en hebben een beperkte kennis van bedrijfsprocessen, waardoor veelal een ad hoc relatie met de schadebeperkers bestaat;

- **Intelligence SOC:**
  De naam SOC wordt soms ook gebruikt voor een groep analisten die in feite werken als een Computer Emergency Response Team (CERT). Deze security experts acteren als het kenniscentrum van de organisatie met een sterke focus op cybersecurity. Naast deze groep, die men kan zien als een 'Intelligence SOC', bestaan binnen de organisatie nog diverse andere afdelingen die zich zelfstandig bezighouden met security. Dit type SOC staat verder af van de techniek doordat de techniek (deels) door die andere afdelingen wordt ingevuld. Het SOC vervult een functionele rol met nadruk op de analyse van de huidige dreigingen en hun mogelijke impact op de business;

- **In de lijn geïntegreerde SOC-functie:**
  Sommige organisaties hebben security belegd binnen de reguliere taken van lijnmanage-

ment. Hierbij is het beleid dat alle managers en medewerkers zich bewust zijn van en verantwoordelijk zijn voor security, en deze verantwoordelijkheid vertalen naar hun dagelijkse handelen. Het SOC is hierbij een kleine uitvoerende organisatie, veelal gericht op het uitvoeren van technische metingen, ter ondersteuning van de taken van lijnmanagement. De meetprocessen zijn zo ingericht dat deze signalen opleveren die door de lijn kunnen worden afgehandeld. Het aantal dedicated security functies is hierbij beperkt, doordat security een collectieve verantwoordelijkheid is. Wij noemen deze aanpak een 'in de lijn geïntegreerde SOC-functie'.

De verschijningsvorm geeft aan hoe het SOC is gepositioneerd binnen het stelsel van verantwoordelijkheden voor informatiebeveiliging, oftewel hoe past het SOC binnen het geheel. Hiermee is de eerste helft van deelvraag 2 beantwoord.

De tweede helft van deelvraag 2 betreft het uitvoeren van een decompositie, uitgaande van de daadwerkelijk bestaande verschijningsvormen. Welke taken van een SOC kan men zien als een elementaire basisfunctie? Aan de hand van ons veldonderzoek hebben wij vastgesteld welke taken in feite bij iedere vorm van een SOC zouden moeten worden uitgevoerd om de gewenste doelstelling te kunnen behalen, namelijk het realiseren van meer cyberrobuustheid. Voor ieder van de door ons onderkende basisfuncties worden hieronder tevens de ondeelbare relaties, de zogenaamde verankeringen, benoemd om het SOC binnen de gewenste context te kunnen laten functioneren. De onderkende bouwblokken van een SOC zijn:

- **Intelligence-functie:**
  Een SOC beschikt over een kern van ervaren analisten, die zich richten op de specifieke dreigingen en beveiligingsincidenten die relevant zijn voor de gebruikersorganisatie. Zij analyseren en geven richtlijnen aan de andere functies binnen het SOC, aan de beheerders, aan de schadebeperkers binnen de gebruikersorganisaties en aan degene die werkzaam zijn binnen het voortbrengingsproces. De Intelligence-functie kent twee verankeringen, namelijk een sterke band met de gebruikersorganisatie en een nauwe band met de beheerorganisatie;

- **Baseline Security-functie:**
  Een SOC ziet toe op de technische aspecten van de uitrol van de BIR, het proces van hardening van de technische componenten, het proces voor het aanbrengen van patches en de onderhoudsniveaus. Hiertoe worden naast preventieve instructies aan beheerders scans uitgevoerd om de compliance en kwetsbaarheden vast te stellen. De Baseline Security en Monitoring-functies kennen één verankering, namelijk de nauwe band met de beheerorganisatie;

- **Monitoring-functie:**
  Een SOC bewaakt de verkeersstromen en probeert anomalieën te detecteren. Hierbij worden de grote volumes aan signalen verzameld en geanalyseerd via filtering en het leggen van correlaties, met het doel de werkelijk relevante signalen te kunnen herkennen. De Monitoring-functie is verankerd met de Intelligence-functie binnen het SOC;

- **Pentest-functie:**
  Zowel in de productieomgeving als bij het voortbrengingsproces worden pentesten uitgevoerd, met name gericht op de door de Intelligence-functie aangegeven aandachtspunten.

Veelal zal de Intelligence-functie optreden als opdrachtgever. De pentesten of technische IT-audits kennen geen verankering, maar wel een diversiteit in profilering afhankelijk van de te beschouwen technologieën;

- **Forensische functie:**
  Het SOC assisteert forensische onderzoekers bij het verzamelen en analyseren van bewijsmateriaal. De door de Forensische functie uit te voeren activiteiten zijn sterk gekoppeld aan de specifieke gebruikersorganisatie, hun bedrijfsprocessen en de voor hen relevante dreigingen. De Forensische functie kent vooral een verticale verankering, namelijk een directe relatie met de andere functies binnen het SOC. Hiermee is er een indirecte verankering in de richt van de gebruikersorganisatie en de beheerorganisatie.

Als een organisatie een nieuw SOC wil inrichten, helpt deze decompositie. Iedere basisfunctie kan nu separaat worden ingevuld en worden gekoppeld om de daarbij benodigde verankering te realiseren. De keuze van staffing en competenties, plus de benodigde meet- en analyse-instrumenten, kan per basisfunctie worden opgepakt. De organisatie kan het inrichten nu veel efficiënter uitvoeren, door voor iedere basisfunctie doelstellingen te formuleren en die op een wijze te gaan invullen die voor hun eigen context het meest geschikt is.

De introductie hierboven van de elementaire basisfuncties maakt het ontwerp van een nieuw SOC overzichtelijk, omdat er nu gebruik wordt gemaakt van standaard bouwblokken.

Deze standaardisatie helpt tevens bij het optimaliseren van een bestaand SOC. Daarnaast kunnen nu best practices worden ontwikkeld per basisfunctie, zonder dat men een verwarrende discussie krijgt over wat een SOC nu precies inhoudt en hoe dit moet worden gepositioneerd. Die vragen staan los van het daadwerkelijk invullen van een basisfunctie.

12.3. Deelvraag 3: 'SOC as a Service'

Het veldonderzoek was gericht op het identificeren van bouwblokken. Deze worden samengevoegd tot één bouwwerk, namelijk het SOC. Aan de hand van theoretische beschouwingen is getracht antwoord te geven op de volgende deelvraag:

Kan een SOC dusdanig worden ingericht dat deze ook diensten kan leveren aan meerdere gebruikersorganisaties en beheerorganisaties binnen de overheid?

De mogelijkheid tot het leveren van diensten moet per bouwblok worden beschouwd. Voor ieder bouwblok zijn de benodigde verankeringen in kaart gebracht. Door deze verankeringen in te vullen via liaisons, kan een 'SOC as a Service' worden samengesteld dat diensten levert aan die organisaties die behoefte hebben aan meer weerbaarheid tegen cyber aanvallen. Hiermee vormt men het SOC om tot een Shared Service Center, of beter gezegd een Shared Service SOC. Dit is een gezamenlijke inspanning, die moet worden gefinancierd vanuit de deelnemende organisaties.

Tegenwoordig is er steeds minder een 1:1 relatie tussen gebruikersorganisaties en beheerorganisaties door de invoering van Shared Service Centers voor IT-dienstverlening. In feite is er sprake

van een N:M mapping tussen gebruikers en beheerders. In dit kader zijn in deze scriptie separaat de vereisten uitgewerkt voor de relatie met een gebruikersorganisatie versus de relatie met een beheerorganisatie, in de vorm van het inrichten van verschillende soorten van liaisonfuncties.

Als het SOC werkt voor een specifieke gebruikersorganisatie, moet er een nauwe band worden opgebouwd met een drietal liaisons, namelijk:

- De Chief Information Security Officer (CISO), of namens deze met een Information Security Officer (ISO);
- De architecten en consultants die zijn betrokken bij Security by Design, dus bij het voortbrengingsproces voor het realiseren van veilige (web)applicaties;
- Schadebeperkers in het kader van Business Damage Control.

Daarnaast kan het SOC werken met verschillende beheerorganisaties. Hiertoe moet binnen iedere beheerorganisatie een liaison worden ingericht. In de praktijk zou hiertoe een Security Beheerder kunnen worden aangesteld, die de brug vormt tussen de analisten en specialisten binnen het SOC en de technische en functionele beheerders binnen de specifieke beheerorganisatie.

> *De bedoeling van 'SOC as a Service' is dat door schaalvoordeel en het bundelen van kennis en expertise tegen zo laag mogelijke kosten het hoogst mogelijke beveiligingsniveau wordt verkregen. Daarbij wordt met de bouwblokken een bouwwerk gerealiseerd, dat leidt tot een optimaal overall resultaat om de overheid weerbaar te maken tegen cyberaanvallen en IT-misbruik.*

12.4. Deelvraag 4: Consultatie van vakgenoten

Na het concipiëren van onze eerste rapportages zijn het meetmodel en de daaruit volgende resultaten afgestemd met een aantal vakgenoten. Deze afstemming had de vorm van een validatie van ons model, en vormt daarmee het beschouwend onderdeel van ons onderzoek. Dit geeft antwoord op de vierde deelvraag:

> *Wat is de professionele opinie van vakgenoten over het ontwikkelde model?*

De resultaten zijn op verschillende momenten gepresenteerd, zoals tijdens workshops, bijeenkomsten van commissies van de Rijksoverheid, bijeenkomsten van werkgroepen zoals bij het Centrum voor Informatiebeveiliging en Privacybescherming (CIP), bilaterale besprekingen met experts etc. De tussenresultaten en eindresultaten zijn steeds in goede orde ontvangen en de meerwaarde van de decompositie in elementaire basisfuncties wordt onderschreven.

> *Het complexe vraagstuk met betrekking tot het ontwerpen en inrichten van SOC's is door de decompositie en het invoeren van standaard bouwblokken een stuk eenvoudiger geworden. Dit helpt management om nieuwe SOC's op te zetten of bestaande SOC's te optimaliseren.*

Het meetmodel wordt vooralsnog door vakgenoten gezien als een beschrijvend model en biedt nog niet de mogelijkheid kwantitatief de effectiviteit van een SOC te meten of uit te drukken.

Het advies is om een diepgaande analyse te doen en mogelijke KPI's af te leiden voor de bestaande assen. Als een SOC meetbaar wordt gemaakt kan er vanuit de organisatie sturing plaatsvinden. Via deze KPI's kan concreet worden vastgesteld of het SOC daadwerkelijk effectief opereert. De onderzoekers zien dit als een nuttige uitbreiding en stellen voor dit op te pakken als een mogelijke vervolgstudie.

12.5. Beantwoording van de onderzoeksvraag

De centrale onderzoeksvraag is:

> *Op welke wijze dient een SOC te worden georganiseerd en ingericht om de IT-dienstverlener en haar klanten binnen de overheid weerbaar te maken tegen cyberaanvallen en IT-misbruik?*

De organisatie dient een overkoepelend beleid te hebben voor informatiebeveiliging en privacybescherming, waarvan het SOC een herkenbaar en geïntegreerd onderdeel is. Per basisfunctie van het SOC bepaalt de organisatie de gewenste doelstellingen, staffing, competenties, meetinstrumenten, meetmethoden, rapportage- en escalatiepaden, etc.

Doordat het SOC wordt opgebouwd per basisfunctie, kan de aanpak modulair verlopen en kan tevens het SOC zo worden ingericht dat meerdere gebruikersorganisaties met hun eigen bedrijfsprocessen, en meerdere beheerorganisaties met hun eigen infrastructuren kunnen worden bediend. Binnen de Rijksoverheid kan men hierbij denken aan een (Multi)Departementaal SOC, dat voor een of meer Ministeries zorgt voor cybersecurity en het voorkomen van IT-misbruik.

Zo een (Multi)Departementale aanpak lost een aantal praktische problemen op, zoals de huidige schaarste aan expertise voor analisten, het nergens functioneren van een echte SIEM, het op vele plaatsen uitvinden van het wiel door allemaal verschillende SOC's te ontwikkelen etc. Door schaalvergroting en het schaalbaar maken van het SOC, krijgt men een verhoging van de effectiviteit en de efficiëntie.

12.6. Aandachtpunten voor de inrichting van een effectief SOC

Nu de onderzoeksvraag is beantwoord, willen wij de lezer nog een aantal boodschappen meegeven. Tijdens het onderzoek hebben wij een aantal ervaringen opgedaan, die mogelijk nuttig zijn om als randvoorwaarden mee te nemen bij een ontwerp of optimalisatie van een SOC:

- **De analisten:**
  Een cyberaanval is mensenwerk, en het verdedigen daartegen is ook mensenwerk. Daarom is de kwaliteit en de ervaring van de individuele analisten van vitaal belang voor de doeltreffendheid van een SOC, met name voor de Intelligence-functie. De vereiste vaardigheden zijn echter nog (zeer) schaars. De verwachting is dat er onvoldoende analisten op de markt zijn om alle momenteel voorziene decentrale SOC's adequaat te kunnen bemensen. Deze schaarsheid is een van de argumenten om te pleiten voor een meer gecentraliseerde aanpak van SOC's binnen de overheid;

- **Tooling:**
  Meetinstrumenten zijn van essentieel belang, want '*meten is weten*'. Goede meetinstrumenten zijn echter kostbaar. Door de huidige versnippering van programmatuur en licenties voor endpoint protection, scans en monitoring geeft de overheid nodeloos veel geld uit. Door trage lokale besluitvorming zijn er ook licenties waarvoor wel wordt betaald, maar die (nog) niet worden gebruikt of met een forse vertraging in gebruik zijn genomen. Standaardisatie kan tot een aanzienlijke reductie in kosten voor licenties en menskracht leiden voor de overheid;

- **SIEM:**
  Continuous Monitoring vereist het verzamelen van veel log-informatie, het selecteren en analyseren, en vooral het correleren van events. Hiervoor is een Security Information and Event Manager (SIEM) nodig. Wij komen tot de conclusie dat de juiste instrumenten en technieken hiervoor nog niet breed beschikbaar zijn, en het opzetten van de juiste rulesets nog steeds niet lukt. Op het gebied van scans en preventie zijn enkele succesvolle voorbeelden, maar bij geen enkele van de door ons bezochte organisaties is men er tot nu toe in geslaagd een doeltreffende SIEM op te zetten. Het ontwerpen van een goede methode voor een SIEM is iets wat centraal moet worden opgepakt binnen de overheid;

- **Informatiebeveiliging:**
  Een SOC is alleen effectief als een aantal essentiële onderdelen van informatiebeveiliging op orde is binnen de overheidsinstantie, zoals de governance voor informatiebeveiliging en privacybescherming, grip op het voortbrengingsproces, grip op de beheerprocessen en grip op de beheerprocessen, zoals voor hardening en patches. Het SOC is onderdeel van een groter geheel, en dat grotere geheel moet wel bestaan en werken, bij voorkeur conform de BIR;

- **Management Commitment:**
  Een belangrijke randvoorwaarde is de attitude van lokaal senior management. Worden er daadwerkelijk budgetten en menskracht beschikbaar gesteld, krijgen informatiebeveiliging en het SOC de formele status die daarvoor nodig is, of werkt men volgens 'BIR in Name Only (BiNO)'? Deze attitude verschilt per bezochte instantie.

Met betrekking tot het laatste punt geldt, dat als lokaal senior management geen prioriteit geeft aan het inrichten en financieren van een SOC, men er niet aan moet beginnen. Het opbouwen van een SOC heeft alleen zin als het SOC over een lange periode daadwerkelijk wordt gebruikt, mede gezien de forse investering en alle energie die gaat zitten in het opleiden en trainen van de expertise. Wij zien in de praktijk dat alleen de wat oudere SOC's stap voor stap effectief worden, door de daar opgebouwde ervaring, expertise en contactennetwerk. Het effectief krijgen van een SOC is een groeipad.

13. Dankwoord en reflectie

Graag spreken wij onze waardering uit voor de Rijksdiensten die ons opdrachten hebben gegeven voor de ontwikkeling van een SOC en het onderzoeken van de mogelijkheden tot samenwerking tussen SOC's en organisaties die behoefte hebben aan het gebruik van SOC-diensten. Wij willen met name het Ministerie van BZK, DGOBR/DIR, bedanken voor het feit dat wij een aantal onderzoeksresultaten vanuit de voor hen uitgevoerde opdracht mochten hergebruiken voor het samenstellen van deze scriptie.

Wij hebben voor ons onderzoek prima gebruik kunnen maken van alle input die wij hebben gekregen vanuit bestaande SOC's en vonden overal een warm onthaal. Men gaf ons echt inzicht in wat er in de keuken gebeurt. De door de SOC's getoonde details hebben gezorgd dat wij een model konden ontwerpen dat praktisch toepasbaar is binnen diverse omgevingen, omdat de hiervoor vereiste waarnemingen in de echte praktijk hebben plaatsgevonden.

Wij zijn zelf pas twee jaar actief binnen het vakgebied van IT-audit en zijn gestart vanuit een relatieve 'green field' positie. Door de diversiteit van het beroep komen er dagelijks complexe onderwerpen op je af, wat soms zorgt voor een forse dosis onzekerheid. Binnen onze opdrachtenportefeuille zijn wij in aanraking gekomen met de problematiek omtrent het SOC in verschillende contexten, hetgeen eerst voor ons een totaal nieuw onderwerp was. Door de actualiteit van dit onderwerp en de verwarring binnen het vakgebied over wat dit nu echt is, hebben wij besloten het SOC als scriptieonderwerp te kiezen. Wij zijn zelf blij verrast, dat wij in staat zijn geweest voldoende kennis op te bouwen om nu als serieuze gesprekspartners te worden beschouwd. Dit heeft wel de nodige inspanning gekost, ook buiten kantoortijd. De belangrijkste 'lesson learned' van dit onderzoek is dat het mogelijk is een junior IT-auditor, die zich echt vastbijt in een onderwerp, in korte tijd te laten doorgroeien tot een volwaardig gesprekspartner over een specifiek deelgebied. Dit geeft ons het vertrouwen om in de toekomst ook andere complexe problematiek aan te pakken.

De werkvorm welke is gehanteerd voor het uitvoeren van het onderzoek is een van de key factoren voor de afronding van deze scriptie. Er is veel in teamverband samengewerkt, met veel brainstorming en vele schetsen op het whiteboard, waarbij gebruik is gemaakt van de expertise van ervaren vakgenoten en collega's zoals onder andere Prof.dr.ir. Ronald Paans RE en Jerry Fasten BEc RE QSA CISA. Door de gezamenlijke inspanning en kruisbestuiving zijn ideeën gegenereerd, bekritiseerd, in de prullenbak gegooid, opnieuw geprobeerd en verrijkt, totdat het uiteindelijke resultaat erkenning kreeg van vakgenoten.

Onze bijzondere dank gaat uit naar Ronald Paans welke de ruimte en ondersteuning heeft gegeven om deze scriptie af te ronden.

14. Literatuur

14.1. Geraadpleegde bronnen

[AIVD2012] Algemene Inlichtingen- en Veiligheidsdienst, (2012). Jaarverslag.

[BB2012] Binnenlands Bestuur, (2012). Computer virus lijkt tot stilstand te komen: *http://www.binnenlandsbestuur.nl/digitaal/nieuws/computervirus-lijkt-tot-stilstand-te-komen.8382998.lynkx*.

[BIG2013] Kwaliteitsinstituut Nederlandse Gemeente, (2013). Tactisch Baseline Informatiebeveiliging Nederlandse Gemeente.

[BIR2012] Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (2012). Baseline Informatiebeveiliging Rijksdienst: *Tactische Normenkader*.

[BZK2013] Plasterk, R.H.A., (2013). Brief van de Minister van Binnenlandse Zaken en Koninkrijksrelaties, Nr 51.

[CBP2013] College Bescherming Persoonsgegevens, (2013). Beveiliging van persoonsgegevens.

[CIP2014] Reuijl, A., Koers, M., Paans, R., Veer van der, R., Roukens, R., Kok, C., Breeman, J., (2014). Centrum Informatiebeveiliging en Privacybescherming: *Grip op Secure Software Development.*

[CW2013] Redactie Computerworld, (2013). 38 grote IT-incidenten in 2013: *http://computerworld.nl/beveiliging/78462-38-grote-it-incidenten-in-2013-deel-1*.

[ENISA2006] European Union Agency for Network and Information Security, (2006). Een stapsgewijze aanpak voor het samenstellen van een CSIRT.

[GOV2010] GOVCERT.NL, Fox-IT, (2010). Pentesten doe je zo: *Een Handleiding voor opdrachtgevers.*

[GvIB2006] Tolido, R., Borsoi, P., Bronk, H., Elsinga, B., Greuter, R., Haftkamp, W., … Reijers, R. (2006). Genootschap van Informatie Beveiligers [GvIB]: *CERT in de organisatie.*

[HP2011] Hewlett- Packard Development Company, (2011). Building A Successful Security Operations Center: *ESP-BWP014-052809-09.*

[IBM2013] International Business Machines Corporation, (2013). Strategy considerations for building a security operations center: *Optimize your security intelligence to better safeguard your business from threats.*

[ITIG2006] IT Governance Institute, (2006). Information Security Governance: *Guidance for Boards of Directors and Executive Management 2nd Edition.*

[KPMG2013] Hermans, J., Schreurs, G. [KPMG] (2013). Vijf denkfouten over cybersecurity: *Een bestuurdersperspectief op cybersecurity.*

[McAfee2011] McAfee Creating and Maintaining a SOC, (2011): *The details behind successful Security Operations Centers.*

[NCSC2012] Nationaal Cyber Security Centrum, (2013). Cyber securitybeeld Nederland: *CSBN-3.*

[NCSC2013] Nationaal Cyber Security Centrum (2013). De aanhouder wint: *De wereld van Advanced Persistent Threats. Factsheet FS-2013-02C.*

[NIST2011] Dempsey, K., Chawla, N.S., Johnson, A., Jonston, R., Jones, A.C., Orebaugh, A., Stine, K. (2011). National Institute of Standards and Technology [NIST]: *Information Security.* 800-137.

[OU2011] Pruller, M. (2011). Open Universiteit: *De Make-or-Buy beslissing voor kleine Software Ontwikkelorganisaties.*

[PINE2013] Pinewood, (2013). Datasheet Penetratietest.

[PvIB2011] Rorive, K., Beerends, M., Bordewijk, L., Breedijk, F., Cimen, H., Cornelisse, J., Smulders, A., (2011). Platform voor Informatie Beveiliging, Expertbrief Security Operations Center: *Een inrichtingsadvies. ISSN 1872-4876, Jaargang 7 - Nr3.*

[RSA2013] RSA Technical Brief, (2013). Building an intelligence driven security operations center.

[SIEM2012] Dorigo, S., (2012). Radboud University Nijmegen: *Security Information and Event Management.*

[TNS2014] Tenable Network Security, (2014). Nessus Compliance Checks: *Auditing System Configurations and Content.*

[Trend2012] Trend Labs, (2012). You have one new friend request: *A guide to threats on Social Media.*

[Trend2013] Wilhoit, K., (2013). Trend Micro: *Who's really attacking your ICS Equipment?*.

[TW2011] Wokke, A., (2011). http://tweakers.net/nieuws/76558/overheid-mogelijk-digid-inloggegevens-gestolen-door-hack.html;

[XRM2011] Laan, S., (2011). XR Magazine Thema ICT-infrastructuur, editie 26.

[YIN2009] Yin, R.K., (2009). Case Study Research Design and Methods.

14.2. Seminars en conferenties

Wij hebben de volgende seminars bezocht:

- VUroRE Seminar: Fighting cybercrime, 30 oktober 2013 www.vurore.nl
- Het Periodiek Informatiebeveiliging Overleg (PIO), 21 januari 2014 www.cip-overheid.nl