PvIB Expertbrief – februari 2011
ISSN 1872-4876, jaargang 7 – Nr. 3

Februari 2011

Security Operations Center: Een inrichtingsadvies

Een Security Operations Center, kortweg SOC wordt steeds meer omarmd door organisaties voor het beleggen van security taken. Dit is gedreven vanuit de strenger wordende wet- en regelgeving, en ook vanuit het besef van efficiëntie bij het consolideren van specialistische operationele securityactiviteiten. Maar wanneer is een SOC een SOC? Welke taken worden binnen een SOC uitgevoerd en wat is de positionering van een SOC in de organisatie? Deze en meer vragen spelen bij het inrichten van een SOC.

In deze expertbrief hebben SOC deskundigen hun ervaringen gebundeld met het doel een lijdraad te bieden voor organisaties die overwegen een SOC in te stellen.

Kelvin Rorive

Mark Beerends

Lourens Bordewijk

Frank Breedijk

Haydar Cimen

Jethro Cornelissen

Remco Ruiter

Rob Schuurman

Andre Smulders

Pagina

http://www.pvib.nl/

✉ expertbrief@pvib.nl

2

ACHTERGROND

De aandacht voor informatiebeveiliging blijft maar groeien. Er wordt ingezien dat het goed beheersen van informatiebeveiliging randvoorwaardelijk is om de bedrijfsvoering van tegenwoordig te garanderen. Zo was vroeger een bedrijfsnetwerk een fysiek afgeschermde omgeving waar de controle op toegang tot het netwerk relatief eenvoudig was. Dit in tegenstelling tot de huidige situatie waar organisaties geconfronteerd worden met steeds complexere en heterogene IT omgevingen. Daarnaast worden bedrijven geconfronteerd met ontwikkelingen, zoals 'Het nieuwe werken' en 'Cloudcomputing'. Dit zijn containerbegrippen voor e-mail bekijken met de Ipad vanuit de trein, twitteren met collega's vanuit de auto en 'bedrijfsdata ergens opgeslagen op het Internet'.
Nieuwe ontwikkelingen en de toename in complexiteit van IT omgevingen hebben tot gevolg dat het beheersen van informatiebeveiliging en het naleven van regelgeving voor organisaties ook steeds complexer en omslachtiger wordt. Daarbovenop wordt steeds vaker door het bestuur en toezichthouders van organisaties geëist dat de complexe samenhang van security bedreigingen en maatregelen aantoonbaar worden beheerst.

In reactie op deze ontwikkelingen benoemen steeds meer organisaties een risicomanager, securitymanager of richten zij hiervoor een security afdeling op. De taken van een security afdeling kunnen bestaan uit zowel strategische, tactische als operationele security taken. Operationele taken kunnen bestaan uit de analyse van security logging, bewaken van de netwerk perimeter, uitgifte en beheer van elektronische sleutels, autorisatiebeheer of forensisch/cyber-security onderzoek.
Het uitvoeren van deze operationele activiteiten wordt in toenemende mate samengevoegd in één security afdeling, het zogenaamde Security Operations Center (SOC). Er zijn echter verschillende uitgangspunten en redenen waarom een organisatie kiest voor oprichting van een SOC. Al enkele jaren is ervaring opgedaan bij het uitvoeren van deze operationele security gerelateerde activiteiten vanuit een SOC. Er bestaat echter geen eenduidige definitie van de activiteiten die binnen een SOC uitgevoerd moeten worden. 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.

Deze expertbrief biedt organisaties handvatten bij het opzetten van een SOC.

Leeswijzer

Na de verantwoording van deze expertbrief in de totstandkoming wordt ingegaan op de doelstelling vaneen SOC. Vervolgens worden aspecten beschreven die van invloed zijn op de inrichtingen en positionering van een SOC. Uiteindelijk worden typeringen van een SOC beschreven.

Totstandkoming expertbrief

Deze expertbrief is tot stand gekomen vanuit de behoefte om kennis er ervaringen te bundelen rond het opzetten van een SOC en mogelijk te komen tot een eenduidige definitie van een SOC. Een aantal ervaren experts (SOC managers en adviseurs) met directe ervaring in relatie tot een SOC hebben belangeloos meegewerkt aan de totstandkoming van deze expertbrief.
In een expertsessie hebben de deelnemers op basis van de probleemstelling zoals hierna beschreven, gediscussieerd over o.a. de definitie van een SOC. Hierbij is gebruik gemaakt van de standaard PvIB aanpak voor expertsessies. Kortweg komt het erop neer dat op basis van door de experts aangeleverd referentiemateriaal een selectie is gemaakt van de belangrijkste onderwerpen in relatie tot de probleemstelling. Deze onderwerpen zijn vervolgens door de groep geclusterd en verder uitgediept. De resultaten van de expertsessie zijn verwerkt in deze expertbrief.

Doelgroep

Deze expertbrief heeft tot doel kennis er ervaring rond security operations centers op gestructureerde wijze te bundelen, zodat andere organisaties hier gebruik van kunnen maken bij de overweging, inrichting of het inkopen van een SOC. De expertbrief heeft een internationaal karakter.

Doelgroepen van deze expertbrief zijn:
- Verantwoordelijke voor security management;
- Manager SOC;
- IT auditors.

Probleemstelling

Het blijkt bij navraag bij meerdere managers dat de definities van een SOC zeer uiteenlopen. Het expertteam heeft daarom zichzelf de volgende hoofdvraag gesteld:

Wat is een Security Operations Center?

Detailvragen

Binnen de context van de hoofdvraag zijn de volgende detailvragen gedefinieerd die het expertteam belangrijk vond bij de beantwoording van de hoofdvraag:

- *Wat zijn de taken van een SOC, wat zou een SOC minimaal moeten doen en wat is handig om te doen?*
- *Op welk detail niveau zou een SOC moeten acteren?*
- *Welke verantwoordelijkheden zou een SOC moeten hebben?*
- *Kan een controlerende en adviserende functie in een SOC gecombineerd worden?*

4

AL EERDER GEHOORD?

Een Security Operations Center bestaat al lang. Een Particuliere Alarm Centrale (PAC) kan gezien worden als een soort SOC, maar dan gericht op hoofdzakelijk fysieke beveiliging. In een PAC wordt continue de beveiliging van gebouwen en terreinen bewaakt die zijn aangesloten. Een PAC heeft procedures voor het opvolgen van (automatische) meldingen of wanneer bij analyse een verdachte situatie wordt waargenomen. Omdat de bemanning van een PAC 24x7 aanwezig is, worden hier door klantorganisaties soms niet-beveiliging gerelateerde zaken belegd. Hierbij valt te denken aan opvolging van storingen in het gebouw, zoals de airco van de serverruimte. Hiermee kan vertroebeling van de primaire taak voor een PAC ontstaan.

Het bewakingsprincipe van beveiliging, zoals bij PAC's is al langere tijd bekend. Maar is een SOC gelijk aan een PAC of is een SOC gericht op informatiebeveiliging en een PAC op fysieke beveiliging? In ieder geval zijn de jarenlange ervaringen van een PAC bruikbaar bij het komen tot een definitie van een SOC in deze expertbrief.

DOELSTELLING SOC

Waarom is een SOC de laatste jaren in opkomst? Met welke doelstelling wordt een SOC ingesteld? Een SOC kan met een bepaalde doelstelling ingericht worden, gedreven vanuit bijvoorbeeld wetgeving. Maar ook met andere doelen kan een SOC ingesteld worden. In de volgende paragrafen zijn de belangrijkste doelen voor een SOC beschreven zoals deze binnen de expertgroep zijn geïdentificeerd.

Aantoonbaar beheersen van informatiebeveiliging door wet- en regelgeving
Vanuit wet- en regelgeving wordt in toenemende mate vereist om aantoonbaar controle te hebben over onder andere de informatiebeveiliging. Een SOC kan een waardevol onderdeel zijn bij het aantoonbaar beheersen van informatiebeveiliging door het uitvoeren van interne controles en het bewaken van security incidenten. Het aantoonbaar te beheersen van informatiebeveiliging vanuit wet- en regelgeving kan daarom een driver zijn voor het inrichten van een SOC.

Effectief uitvoeren van operationele security taken door bundeling van kennis
Door de toename van beveiligingsoplossingen, vaak verdeeld over een organisatie, is veel versnipperde specialistische kennis binnen de organisatie. Met beveiligingsoplossingen wordt gedacht aan firewalls, virusscanners, identity- en access management en vulnerability scanning. De gewenste expertise voor bediening en beheer van al deze beveiligingsoplossingen is niet ruim beschikbaar op de arbeidsmarkt. Door het bundelen van deze expertises in het SOC kan synergievoordeel worden behaald, de kwaliteit kan worden verhoogd en de gevolgen van de schaarste in kennis kunnen worden beperkt. Het verhogen van de effectiviteit door het bundelen van kennis kan daarom een doelstelling van een SOC zijn.

Toepassen van functiescheiding
Een SOC kan helpen bij de scheiding van verantwoordelijkheden (seperation of duties). Het gebruik van functiescheiding beperkt het risico dat informatie binnen een systeem of applicatie wordt gemanipuleerd.

Logging dient bijvoorbeeld op een veilige manier te worden verstuurd naar een aparte logserver. De analyse op verdachte activiteiten kan dan vervolgens worden uitgevoerd door de experts van een SOC.
Hetzelfde geldt voor het controleren op de juiste werking van informatiebeveiliging. Het oordeel van een onafhankelijke partij, zoals een security afdeling of internal audit is vaak waardevoller dan het oordeel van de verantwoordelijke IT manager. Een IT manager kan uiteraard een eigen onderzoek uitvoeren, maar deze dient wel gecontroleerd te worden door een partij (bijvoorbeeld het SOC) die onafhankelijker is.

Incident- en risicobeheersing
Het SOC kan een waardevolle rol spelen door betrokken te zijn bij security incident management. Door kennis te hebben van alle security incidenten kan een beter beeld gevormd worden over de mogelijk (veranderde) dreigingen en de daaraan gekoppelde risico's. Wanneer deze informatie op verschillende plekken in de organisatie beschikbaar is, is deze analyse lastiger uit te voeren.
Security incidenten kennen meerdere bronnen. De meest gebruikte bron is het incident management proces. Via dit ITIL gerelateerde proces kunnen security incidenten worden geïdentificeerd en worden gerapporteerd naar het SOC. Bovendien zou het SOC voor de incidentopvolging kunnen zorgen.
Bij grotere organisaties met meerdere zelfstandige eenheden kunnen meerdere incidentprocessen bestaan. Een SOC kan waardvol zijn bij het analyseren en aggregeren van security incidenten van de verschillende eenheden, om daar nieuwe dreigingen in te herkennen die organisatie breed van toepassing kunnen zijn.
Daarnaast zijn er externe bronnen zoals GOVCERT.NL of andere CERT achtige diensten die nieuwe dreigingen en analyse daarvan kunnen doorgeven aan het SOC.

ORGANISATIE ASPECTEN SOC

Een SOC kan op meerdere manieren ingericht worden. Van invloed daarop is een aantal organisatorische aspecten. Deze aspecten worden in de volgende paragrafen toegelicht.

24x7
Een organisatie is op Internet 24x7 aanwezig en open. Dus ook cyberaanvallen kunnen 24x7 plaatsvinden. Dit wil niet zeggen dat een cyberaanval in de nacht direct schadelijk is voor een organisatie, maar het is wel prettig om daarvan op de hoogte te zijn. Op deze manier kunnen maatregelen worden getroffen, voordat de productieve uren weer aanbreken.
Een SOC is vaak voorzien een monitoringfunctie. Daarbij is het inregelen van een 24x7 monitoring vrijwel altijd van belang. Tooling kan ondersteunen bij het geautomatiseerd herkennen van 'verdachte' gebeurtenissen en een medewerker met piketdienst alarmeren buiten kantoortijd of wanneer snelle interventie vereist is, wordt veelal gekozen voor 24x7 aanwezigheid van SOC medewerkers.
Een alternatief voor het inregelen van bewaking buiten kantooruren is het uitbesteden van bewaking naar commerciële diensten.

Positionering
De taken die een SOC moet uitvoeren zijn bepalend voor de plaats in de organisatie. Wanneer het SOC bijvoorbeeld de taak krijgt onafhankelijke analyses uit te voeren op activiteiten in de IT infrastructuur, dan is een gescheiden ophanging in de organisatie wenselijk. In de praktijk blijkt dat een SOC veelal in 'de lijn' wordt opgehangen, waarbij het SOC de lijnorganisatie ondersteunt bij het uitvoeren van operationele security taken. Afhankelijk van de taken die

het SOC toebedeeld krijgt, kunnen dit zeer gedetailleerde operationele handelingen zijn tot abstracte security risicoanalyses.
Een SOC kan vanuit een bepaalde bedrijfskolom diensten verlenen voor andere bedrijfskolommen binnen dezelfde organisatie. In deze situatie is het belangrijk om duidelijke afspraken te maken over mogelijk conflicterende belangen tussen de bedrijfskolommen, omdat het SOC dan zowel hiërarchisch als functioneel wordt aangestuurd.

Opdrachtgevers
Een mogelijk argument om een SOC in te richten kan zijn het aantoonbaar beheersen van informatiebeveiliging zoals bijvoorbeeld gesteld in het intern vastgestelde beveiligingsraamwerk. In deze beveiligingsraamwerken kan staan dat de organisatie verantwoordelijk is voor de structurele analyse van security logging. Het SOC voert keurig analyses uit op de loginformatie en rapportages die worden gemaakt. Hoge kosten worden gemaakt voor analysetools en arbeid bij het bedienen en beoordelen van de analyses. Technisch gesproken wordt daarmee voldaan aan de gestelde eisen uit het beveiligingsraamwerk. Maar doet de organisatie ook wat met de goedbedoelde rapportages? Voelt iemand zich verantwoordelijk om de rapportages op te volgen? Een dergelijke situatie kan ontstaan wanneer er geen opdrachtgever is voor bepaalde functies in het SOC. Het is van belang altijd een afnemer (opdrachtgever) te hebben voor de uitgevoerde taken binnen een SOC, ook al is het in het beveiligingsraamwerk of beleid vastgesteld dat het moet gebeuren.

Verantwoordelijkheid
De verantwoordelijkheid van een SOC is afhankelijk van het mandaat, doelstellingen en functies die het moet uitvoeren. De volgende categorieën van verantwoordelijkheden zijn geïdentificeerd:

- **Controleren, registreren, rapporteren en adviseren**
  Het SOC voert op aanvraag of periodiek controles uit op de implementatie van informatiebeveiliging. De verantwoordelijkheid in relatie tot deze taak is beperkt tot het kwalitatief samenvatten en rapporteren van de bevindingen van de controles.
  Een taak die ook binnen controleren en rapporteren valt is het uitvoeren van specifiek onderzoek naar security incidenten of integriteitsonderzoek. Vaak is het belangrijk dat de vertrouwelijkheid van de onderzochte informatie goed wordt beschermd.
  Ondersteunen en adviseren van de organisatie bij operationele security taken in de lijn of in projecten kan een verantwoordelijkheid zijn van het SOC. Hiertoe moet het SOC op de hoogte zijn van het interne beleid, richtlijnen en van de ontwikkelingen in de markt op het gebied van security.
  Wanneer een SOC wordt ingezet voor het uitvoeren van bijvoorbeeld uitgifte van elektronische certificaten of autorisaties, dan heeft het SOC ook de verantwoordelijk om een nauwkeurige transparante registratie bij te houden van de uitgifte.
- **Bewaken en beleggen**
  Op dit niveau kan een SOC de verantwoordelijkheid hebben om verdachte gebeurtenissen te identificeren en deze te beoordelen op risico's. Normaliter betekent dit dat een SOC een 24x7 dienstverlening moet inrichten. Bij de identificatie van bijvoorbeeld frauderisico's kan men er voor kiezen de opvolging te beleggen bij een speciale fraudeafdeling.
- **Opvolgen en handelen**
  Een grote verantwoordelijkheid is het direct handelen op basis van een gebeurtenis. Het SOC heeft dan een mandaat om zelf acties uit te voeren in het geval de belangen van de organisatie in gevaar zijn. Hierbij valt te denken aan het direct afsluiten van een webwinkel wanneer de klantendatabase is gekraakt.

Het is mogelijk om meerdere verantwoordelijkheden te combineren. Dit is vooral afhankelijk van de doelstellingen, functies en het mandaat van het SOC. Daarnaast is het belangrijk dat de verantwoordelijkheden van het SOC formeel worden afgestemd met de opdrachtgever, zeker als het gaat om het direct handelen op basis van een gebeurtenis.

COMPETENTIES

Competenties van medewerkers binnen een SOC zijn direct gelieerd aan de taken en verantwoordelijkheden die de medewerkers moeten uitvoeren. Over het algemeen geldt dat een SOC de plek in de organisatie is waar de operationele kennis rond informatiebeveiliging beschikbaar is. Het SOC dient daarvoor deze kennis actief bij te houden door het verkennen van de marktontwikkelingen op het gebied van informatiebeveiliging, maar ook wat er intern in de organisatie aan beleid en richtlijnen wijzigt en hoe deze geïnterpreteerd moeten worden.

De competenties voor het uitvoeren van sleuteluitgifte beperken zich tot ‘nauwkeurigheid’ en ‘klantvriendelijkheid’. Veel securitykennis is hierbij niet nodig. Een SOC medewerker die verantwoordelijk is voor het bepalen van het risico van een security incident moet geheel andere competenties hebben, alvorens eventuele corrigerende acties uit te voeren. Hierbij kan gedacht worden aan ‘analytisch vermogen’, ‘kennisgedreven’, ‘organisatie sensitief’ enz.

Een belangrijke vaststelling binnen de expertgroep was dat het succes van een SOC binnen de organisatie voor een belangrijke mate wordt bepaald door de professionaliteit, vakkundigheid en niet te vergeten integriteit waarmee de taken worden uitgevoerd. Hierdoor wordt het controlerende karakter van een SOC niet meer als bedreigend ervaren, maar juist ondersteunend aan het realiseren van de bedrijfsdoelen.

SOORTEN SOC

Vanuit de expertgroep is gebleken dat er meerdere en uiteenlopende invullingen zijn van een SOC. Ook werd vastgesteld dat er geen eenduidige inrichting of definitie voor een SOC beschikbaar is. Toch heeft de expertgroep groeperingen van mogelijke taken bepaald, waardoor vier typen SOC’s zijn onderkend. Vooral het soort organisatie, de volwassenheid van de organisatie en de positie van het SOC in de organisatie bepalen welk type SOC het beste toegepast kan worden. De volgende vier soorten zijn benoemd:

- **Controle SOC**
  Voert vooral controles uit op de omgeving om vast te stellen wat de actuele status is rond informatiebeveiliging. Taken kunnen zijn: vulnerability scanning, compliancy testing, pentesting, etc.
- **Monitoring SOC**
  Een monitoring SOC richt zich vooral op het bewaken van de omgeving en acteren op meldingen die ontstaan. Taken kunnen zijn: monitoren van firewalls, IDS, virusscanners, SIEM oplossingen, etc.
- **Operational SOC**
  Een operational SOC richt zich vooral op het uitvoeren van operationele Security taken, zoals key-management, access management, firewall beheer etc.
- **Maatwerk SOC**
  Een maatwerk SOC is volledig aangepast aan de situatie en bestaat uit een mix van taken die in een SOC belegd zouden kunnen worden.

In de onderstaande tabel zijn de verschillende soorten benoemd, met de daarbij horende SOC functies (zie bijlage A voor de definities).

	Controle SOC	Monitoring SOC	Operational SOC	Maatwerk SOC
Firewall loganalyse	✓	✓		
Firewall beheer			✓	✓
Intrusion detection and prevention (IDP) loganalyse		✓		
Intrusion detection and prevention (IDP) beheer			✓	✓
Vulnerability scan, Penetration testing	✓			
Compliancy management	✓			
Identity and Access management (IAM) beheer			✓	✓
Risico Assessment	✓			
Key Management			✓	✓
Digitale kluis			✓	✓
Cyber Intelligence		✓		✓
Forensics		✓		
Computer Emergency Response Team (CERT)		✓		
Data loss prevention (DLP)		✓		
Brand protection				✓
Security advies	✓	✓	✓	✓
Security Information and Event Management (SIEM)		✓		
Privileged user management			✓	
Fraud preventions				✓
Sabotage preventie				✓

De invulling is hooguit richting gevend, maar kan helpen bij het vaststellen van de primaire focus die een SOC moet hebben binnen de organisatie. Uiteraard kan een combinatie van typen SOC's ook gebruikt worden.

CONCLUSIE

De expertgroep is gestart met de vraag "*Wat is een SOC?*". Gedurende de expertsessie werd al snel duidelijk dat er geen eenduidige inrichting mogelijk is voor een SOC. De doelstellingen en werkzaamheden van een SOC liepen te veel uiteen. Elke organisatie had zijn eigen argumenten waarom hun SOC de specifieke taken moest uitvoeren. De werkgroep vond het daarom waardevol om deze argumenten te bundelen in deze expertbrief voor organisaties die zoekende zijn naar de juiste inrichting en positionering van een SOC. Tevens zijn vier soorten SOC's onderscheiden. Dit onderscheid kan organisaties helpen bij het aanbrengen van focus in de activiteiten die uitgevoerd kunnen worden door een SOC. Het

aanbrengen van focus voorkomt dat het SOC een ongedefinieerde samenvoeging wordt van securityfuncties, waardoor afspraken over kwaliteit lastiger gemaakt kunnen worden met de opdrachtgevers.

De detailvragen die de expertgroep zichzelf had opgelegd zijn voor het grootste deel beantwoord. De detailvraag "*Wat zijn de taken van een SOC, wat zou het minimaal moeten doen en wat is handig om te doen?"* is volledig beantwoord. Uit de lijst met functies die in deze expertbrief is opgenomen kunnen de taken voor een SOC afgeleid worden. Welke functies van belang zijn is afhankelijk van de doelstellingen die een SOC meekrijgt van de opdrachtgever(s).

Op de detailvraag "*Op welk detail niveau zou een SOC moeten acteren?"*is antwoord gegeven in de paragraaf 'positionering'. De detaillering van activiteiten binnen een SOC is afhankelijk van de doelstellingen, mandaat en functies die het SOC krijgt toebedeeld.

Op het gebied van verantwoordelijkheid, ter beantwoording van de detailvraag "*Welke verantwoordelijkheden zou een SOC moeten hebben?"* is ruimschoots stilgestaan in de paragraaf 'verantwoordelijkheid'. Uit deze paragraaf blijkt dat verantwoordelijkheid meerdere niveaus kent. De meest omvangrijke verantwoordelijkheid is het direct handelen door het SOC op basis van een gebeurtenis.

De detailvraag "*Kan een controlerende en adviserende functie in een SOC gecombineerd worden?"* is beantwoord in de paragraaf 'verantwoordelijkheid'. Het expertteam heeft aangegeven dat deze twee functies prima in een SOC kunnen worden gecombineerd. Het is belangrijk dat de functies en verantwoordelijkheden van het SOC formeel worden afgestemd met de opdrachtgever en dat de opdrachtgever zich bewust is van de mogelijke conflicterende belangen.

De slotconclusie is dat de taken die een SOC uitvoert van meerdere aspecten afhankelijk is die per organisatie verschillen. Er is dus geen eenduidige definitie van een SOC gevonden. Wel is er de afgelopen jaren veel kennis en ervaring opgebouwd die in deze expertbrief is gebundeld.

Interessant voor eventuele vervolgstudie is de vraag of er patronen zijn tussen branches en een type SOC. Zijn bij banken een ander soort SOC te herkennen dan bij de overheid? Daartoe zou een breder onderzoek (benchmarking) uitgevoerd moeten worden onder een grote populatie organisaties met een SOC.

10 Bijlage A: Operationele Security Functies

Uit de expertsessie is gebleken dat er vele verschillende invullingen zijn van een SOC. Deze bijlage omvat een opsomming van operationele security functies die door de groep zijn benoemd. De lijst is niet uitputtend. Afhankelijk van het type SOC en gehanteerde uitgangspunten kunnen deze operationele security functies bij een SOC ondergebracht worden. Zeker niet elk SOC voert deze functies uit!

Firewall log analyse of Firewall beheer

Firewall management is grofweg op te delen in twee functies:

- Analyse van de logfiles van firewalls en beoordelen of security incidenten zich voordoen.
- Beheer van volledige firewall omgeving. Dit betreft het functioneel en operationeel beheer van firewalls (updates software, hardware en OS, maar ook de filterregels). Het functioneel beheer is over het algemeen lastig te scheiden van operationeel beheer van firewalls. Het beheer wordt daardoor vaak door één partij gedaan. Dit kan het SOC zijn.

Intrusion Detection and Prevention (IDP)

IDP systemen dienen net zoals firewalls functioneel en operationeel beheerd te worden. Men kan ervoor kiezen om het bewaken/analyseren van IDP logging uit te laten voeren door het SOC. Mogelijke verdachte gebeurtenissen en security incidenten kunnen dan opgevolgd worden.
Wanneer gekozen wordt om het volledige beheer bij het SOC te beleggen wordt functiescheiding (t.o.v. reguliere beheersorganisatie) gerealiseerd en kan gebruik gemaakt worden van de algemene security kennis van het SOC bij het uitvoeren van de taak.

Vulnerability scan, Penetration testing

Een organisatie kan kiezen voor grofweg twee modellen voor vulnerability scanning:

- Een vulnerability scan op aanvraag van verantwoordelijke lijnmanager.
  In dit geval is het SOC een dienstverlenende partij naar de interne organisatie en voert een vulnerability scan uit, wanneer de organisatie of afdeling daarom vraagt. Desgewenst kan de opdrachtgever vragen het rapport door het SOC te laten analyseren.
- Structureel en periodiek het gehele domein scannen.
  Met deze optie heeft het SOC in opdracht van de (deel)organisatie de opdracht gekregen structureel en periodiek het gehele domein te scannen op kwetsbaarheden en daarover te rapporteren aan de betreffende verantwoordelijke manager.

Wanneer er is gekozen om de verantwoording van informatiebeveiliging zoveel mogelijk te beleggen bij de verantwoordelijke lijnmanager, dan zal optie 1 het beste aansluiten. De lijnmanager moet maar aantonen dat de

informatiebeveiliging goed is ingericht, waar een vulnerability scan bij kan helpen. Het is uiteraard minder effectief wanneer alle verantwoordelijke lijnmanagers een aparte opdracht geven voor het uitvoeren van een scan. Daarom is optie 2 interessanter voor een meer volwassen organisatie op het gebied van vulnerability scanning en informatiebeveiliging.

Compliancy management

Compliancy scanning is vergelijkbaar met vulnerability scanning. Het grote verschil is dat bij compliancy scanning vaak een toets wordt gedaan op basis van de corporate security policy gebaseerd op interne en/of externe regelgeving, terwijl bij vulnerability scanning een toets wordt uitgevoerd op basis van bekende kwetsbaarheden.
Verder gelden ook hier de twee varianten van dienstverlening die bij het SOC belegd kunnen worden:

- Het in opdracht van verantwoordelijke lijnmanager uitvoeren en deze daarmee ondersteunen in zijn risicomanagement verantwoordelijkheid;
- Het periodiek uitvoeren van compliancy scans om zo een structurele bijdrage te leveren in de handhaving van een corporate security policy.

Identity and Access Management (IAM)

Als een autorisatie aanvraag voor een bepaalde business applicatie is goedgekeurd door de eigenaar, dan kan het afhandelen van deze aanvraag prima belegd worden bij een SOC. Het SOC is dan geautoriseerd om een gebruiker te koppelen aan een vooraf gedefinieerde rol. In deze situatie is het verstandig functiescheiding te realiseren door het beheer van rollen te beleggen bij een aparte afdeling. Dit om te voorkomen dat één afdeling in staat is zowel rollen te creëren en gebruikers aan de rollen te koppelen.
Zowel het rolbeheer als het autorisatiebeheer kan bij het SOC worden belegd, de combinatie van beide is niet verstandig.
Het SOC controleert uiteraard eerst of de betreffende autorisatieaanvraag voldoet aan de eisen en autorisatiematrix. Het grote voordeel van deze werkwijze is dat op één plek bekend is wie welke autorisaties heeft. Bij wijzigen van functie of vertrek van een medewerker is snel inzichtelijk welke autorisaties aangepast of weggenomen moeten worden.

Risico Assessment

Het SOC kan op meerdere manieren risicoanalyses uitvoeren. De risico's kunnen worden gehaald uit de analyse van logging, het uitvoeren van vulnerability en compliancy scans en uit de analyse van security incidenten (ook vanuit interne of externe Certs).
Deze analyses zijn daarmee vooral gericht op operationele risico's, zoals de identificatie van verhoogde dreiging van interne of externe aanvallen.

Sleutel Management

Steeds meer cryprografische technologie wordt toegepast om de vertrouwelijkheid en integriteit van informatie te garanderen.

Verschillende oplossingen worden daartoe toegepast zoals PKI, SSL, lijn-encryptie enz. Deze oplossingen werken met elektronische sleutels (symmetrisch of asymmetrisch).
Rond elektronische sleutels zijn twee opties geïdentificeerd:

- **Sleutel guarding**
  Beheer van sleutels die nodig zijn in uitzonderlijke situaties, zoals het recoveren van versleutelde informatie waarbij de originele sleutel verloren is gegaan. Het SOC stelt elektronische sleutels beschikbaar op basis van een streng uitgevoerde procedure.
- **Sleutel uitgifte en beheer**
  Het SOC kan de uitgifte van sleutels voor medewerkers begeleiden, bijvoorbeeld de uitgifte van certificaten bij een PKI omgeving. Met deze functie is op één plek inzichtelijk welke elektronische sleutels er zijn aangevraagd en wie deze in gebruik heeft.

Digitale kluis

Een digitale kluis betreft een oplossing waarmee gevoelige informatie, zoals belangrijke documenten en/of privilleged accounts versleuteld kunnen worden opgeslagen in de infrastructuur.
Het is belangrijk om sterke authenticatie (b.v. 2-factor) in te zetten voor toegang tot deze digitale kluis. Het functioneel beheer (waaronder het uitgeven van digitale sleutels) van de oplossing voor de digitale kluis kan in zijn geheel worden belegd bij het SOC.

Cyber Intelligence

Het is voor een organisatie belangrijk om te kunnen anticiperen op dreigingen vanuit het Internet. Virussen en SPAM zijn twee voorbeelden van Internet dreigingen die tegenwoordig beter door organisaties worden beheerst. Maar steeds nieuwere en complexere dreigingen doen zich voor. Hoe moet een organisatie zich daarop voorbereiden? Het hebben van kennis van deze dreigingen vanuit internet kan belegd worden bij het SOC. Let hierbij op dat er geen overlap ontstaat met taken die mogelijk bij een CERT zijn belegd.

Maar ook aanvallen of georganiseerde criminaliteit gericht op de organisatie vanuit het Internet moeten zo snel mogelijk geïdentificeerd worden. Hulp van externe organisaties (zoals Govcert.nl, leveranciers of concurrerende organisaties) is daarbij waardevol. Het SOC kan de informatie uit deze bronnen organiseren en intern verspreiden naar de verantwoordelijke managers.

Het SOC kan ook ingezet worden om zelf dreigingen op Internet te onderzoeken (zoals berichtgevingen die bedreigen kunnen zijn voor de organisatie). Het SOC voert dan een soort Internet-recherche taak uit.

Forensics

Het SOC kan worden ingezet voor het uitvoeren van forensische IT-onderzoeken. Afhankelijk van de taken die het SOC uitvoert, heeft het SOC inzicht in veel security-informatie vanuit verschillende IT-systemen. Daarnaast kan het SOC een onafhankelijke functie hebben.
Het uitvoeren van een onderzoek naar mogelijk ongeautoriseerde handelingen van een medewerker zou bij het SOC kunnen worden belegd. Hierbij is het van belang dat het SOC beschikt over de competentie om de specifieke technische en juridische aspecten op een juiste wijze te kunnen afhandelen.

Computer Emergency Response Team (CERT)

Het SOC kan een waardevolle rol vervullen bij een CERT. Het SOC kan de taak vervullen van verantwoordelijke partij voor het uitvoeren van de CERT. Bij een omvangrijk security incident neemt het SOC dan de verantwoordelijkheid voor het beperken van de gevolgschade en het herstellen van de primaire bedrijfsprocessen. Omdat bij dergelijke incidenten meerdere disciplines betrokken moeten zijn waarbij ook grote bedrijfsbelangen meespelen, wordt een CERT vaak als losstaande entiteit ingericht waarbij het SOC vanuit operationeel security perspectief betrokken is.

Data Loss Prevention (DLP)

DLP is ten aanzien van taken voor het SOC sterk vergelijkbaar met firewall management. De analyse van logging van DLP kan als taak belegd worden bij het SOC, maar ook het volledige operationeel beheer van DLP.

Brand protection

Een minder gebruikelijke functie die bij het SOC belegd kan worden is het beschermen van de handelsmerken van een organisatie (brand protection). Het betreft hier het beheer van domeinnamen van de organisatie en diens varianten. De communicatieafdeling richt zich op de bescherming van overige uitingen (b.v. in de media) van het handelsmerk. Een afgeleide domeinnaam van de organisatie kan een bedreiging vormen voor de organisatie. Wanneer de domeinnaam ‘companyX’ is en iemand anders opent en website met de naam ‘companyX-nieuws’ en plaatst daar misleidende of andere onjuiste informatie op, dan kan dat tot omvangrijke schade leiden. Daarom moet daar snel en adequaat op gereageerd worden. Het SOC kan de rol invullen van het bewaken van de domeinnaam.
Daarnaast kan brand protection worden gebruikt om specifiek informatie te vinden over wat er door buitenstaanders over een bedrijf wordt gezegd, klachten, plannen voor aanvallen. Hiernaast kan eventueel via deze manier informatie worden gevonden over het bedrijf, waaruit blijkt dat medewerkers zich niet aan bedrijfsbeleid houden.
Deze vorm kan tevens verder uitgebreid worden naar brand intelligence, waar het verder kijkt naar bijvoorbeeld social media.

Security advies

Omdat het SOC een centrale operationele rol heeft in security is

het goed mogelijk om ook advies te geven rond security oplossingen en implementaties. Uiteraard dient het dubbele belang wat mogelijk ontstaat (advies en controle) goed beschouwd te worden. Maar over het algemeen is dit goed intern te organiseren.

Security Information and Event Management (SIEM)

Met een SIEM is het mogelijk op basis van logging uit IT componenten, maar ook uit security systemen (firewalls, IDS, enz.) en applicaties, verdachte of ongewenste patronen te herkennen en hierop te alarmeren. Het werken met SIEM wordt veel bij een SOC belegd, omdat een SOC onafhankelijk kan werken. Daarnaast heeft een SOC de juiste kennis om een complex systeem als SIEM te bedienen.

Privileged user management

Een SOC kan een rol spelen bij het bewaken van gevoelige accounts. Dit zijn accounts binnen een organisatie die een verhoogd risicoprofiel hebben. Activiteiten kunnen bestaan uit de gebruikerscontrole of de monitoring van uitgevoerde activiteiten door dit type accounts.

Fraud preventions

Door de complexiteit van de interacties tussen de verschillende systemen en bedrijfsapplicaties is er overzicht nodig om mogelijke fraudescenario's te kunnen detecteren. Een mogelijke aanpak hiervoor is om voor kritische applicaties security monitoring onder te brengen in een SOC met specialistische kennis. Denk bijvoorbeeld aan internet bankieren. Dit soort applicaties wordt door banken vaak zwaar en apart gemonitord.

Sabotage preventie

Naast fraude kan afhankelijk van het type organisatie ook sabotage een rol spelen. Denk hierbij aan bedrijven en organisaties die een rol spelen in de vitale infrastructuur.

BIJLAGE B: LITERATUURLIJST

1. Best Practices for Building a Security Operations Center, augustus 2006, CA – whitepaper
2. Building a Security Operations Center, Randy Marchany, VA Tech IT Security Office and Lab
3. Hype Cycle for Governance, Risk and Compliance Technologies, 2010, 28 july 2010, Gartner, ID Number: G00205229
4. Keys to Implementing a Successful Security Information Management Solution (or Centralized Security Monitoring), December 12, 2003, Sans reading room
5. Guide to Integrating Forensic Techniques into Incident Response, Augustus 2006, NIST, Special Publication 800-86
6. Guide to Computer Security Log Management, September 2006, NIST, Special Publication 800-92
7. KPN IT Control Management Framework, 28 okt 2008, Solutions Stack SOC
8. Naar een integrale visie, Aandachtspunten voor inrichting van een SOC, TNO
9. Building a Successful Security Operations Center, ArcSight, Research 014-052809-09, Whitepaper
10. Outsourcing Managed Security Services, Januari 2003, Carnegie Mellon University
11. Building a Security Operations Center (SOC), Secure360, BT

16

APPENDIX GEBRUIKTE LICENTIEVORM

De expertbrief wordt gepubliceerd onder de volgende licentie:
Creative Commons Naamsvermelding-GelijkDelen versie 3.0
Meer informatie over deze licentie is the vinden op http://creativecommons.org/licenses/by-sa/3.0/nl/

Deze pagina ziet er op het moment van schrijven als volgt uit: