Voorkom digitale inbraak met een Security Operations Center

Hoe richt je een effectief Security Operations Center in?

Het Security Operations Center (SOC) maakt veilige digitale dienstverlening mogelijk met de juiste inrichting van organisatie, processen, informatie en technologie.

Highlights

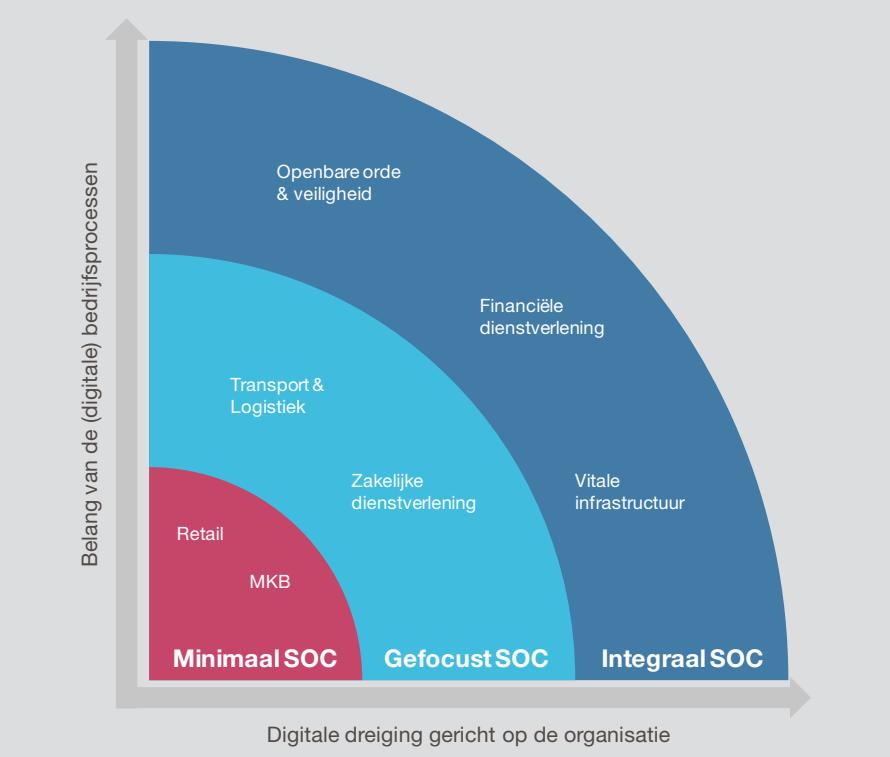
- Beveiligingsincidenten zorgen – naast mogelijk financieel verlies – vaak tot reputatieschade bij burgers, klanten en ketenpartners.
- Een SOC zorgt ervoor dat digitale aanvallen vroegtijdig worden gesignaleerd en daarmee zoveel mogelijk worden voorkomen.
- Het SOC combineert technologie met processen en procedures om incidenten af te handelen en de organisatie 'in business' te houden.
- Een hybride SOC combineert externe expertise met diepgaande kennis vanuit de eigen organisatie.
- Sluit aan op de huidige behoefte van de organisatie en de kennis van de medewerkers, maar zorg ook dat het SOC mee kan groeien naar de toekomst.

Introductie

De overheid communiceert in toenemende mate digitaal met burgers, bedrijven en partners. Dit leidt niet alleen tot een efficiënte en klantgerichte overheid, maar resulteert ook in risico's op de betrouwbaarheid en continuïteit van de informatievoorziening. De impact is groot als bijvoorbeeld de digitale loketten van de overheid niet beschikbaar zijn of de afhandeling van aanvragen voor een paspoort, niet of foutief worden behandeld. Volgens het Trends in Veiligheid onderzoek 2015 van Capgemini, uitgevoerd door TNS NIPO, vertrouwt slechts vier op de tien Nederlanders dat de overheid veilig met (persoonlijke) gegevens omgaat. Dit betekent dat overheidsorganisaties niet alleen voor de uitdaging staan om de risico's het hoofd te bieden, maar ook om het imago als veilige gegevensverwerker te verbeteren.

Het is tegenwoordig niet meer voldoende om een 'groot digitaal hek' om de organisatie neer te zetten. Het beveiligen van informatie vereist dat digitale bedreigingen vroegtijdig worden gesignaleerd en gemitigeerd. Een centrale rol is hierbij weggelegd voor een zogenaamd Security Operations Center (SOC).

Figuur 1: Noodzaak en meerwaarde van het Security Operations Center.



De meerwaarde van een Security Operations Center

Een SOC is een organisatieonderdeel dat specifiek is gericht op het vroegtijdig signaleren en voorkomen van cybersecurity-incidenten. Een SOC combineert de technologie voor het monitoren, voorkomen en detecteren van een digitale inbraak met procedures om incidenten effectief af te handelen en de organisatie 'in business' te houden. Daarmee ondersteunt het SOC de (overheids)organisatie bij het voeren van een veilige digitale bedrijfsvoering.

Het SOC richt zich zowel op de beveiliging van digitale communicatie binnen de organisatie, als op de digitale dienstverlening die aan burgers, bedrijven en partners wordt geboden. Om een veilige digitale dienstverlening mogelijk te maken, beschikt het SOC over systemen waarmee het real-time informatie verzamelt vanuit de informatievoorziening van de organisatie en haar ketenpartners. Met geavanceerde technieken wordt deze informatie geanalyseerd en kunnen digitale aanvallen worden herkend voordat zij daadwerkelijk schade kunnen toebrengen.

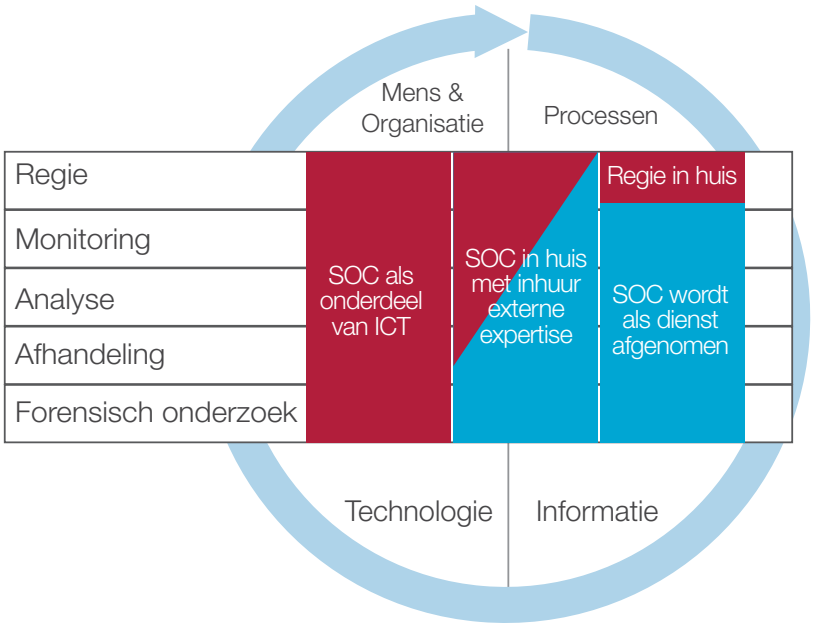
Het belang van de digitale bedrijfsvoering voor de organisatie en het digitale dreigingsniveau bepalen de noodzaak en meerwaarde van het SOC (zie figuur 1). Zo zal de informatievoorziening van een bank of defensieorganisatie meer extensieve SOC-diensten vereisen dan een retailer of een gemeente. De inrichting van een SOC is dus afhankelijk van de beoogde breedte en kwaliteit van de dienstverlening. De behoefte vanuit de afdelingen in het primaire proces vertaalt zich in een missie van het SOC, wat er in de producten- en dienstencatalogus van het SOC wordt opgenomen en welk niveau van dienstverlening nodig is.

Het is voor het inrichten van een SOC noodzakelijk om na te denken over de essentiële ontwerpprincipes en daarbij de assen van het operating model: *mens en organisatie, processen, technologie en informatie* in samenhang te beschouwen. Zie ook het artikel “Samen stap voor stap naar digitale dienstverlening bij de rechtspraak” van Maarten van den Berg en Marnix de Graaff.

De inrichting van een Security Operations Center

De hoge investeringskosten die nodig zijn om een SOC op te zetten, zorgen ervoor dat nog maar weinig organisaties zelfstandig een SOC ingericht hebben. Zij kiezen in plaats daarvan voor een hybride model, waarbij delen van het SOC intern worden ingericht en andere delen als dienst worden afgenomen en door een gespecialiseerd bedrijf worden uitgevoerd.

Figuur 2: Ontwerp-principes bepalen hoe het SOC wordt ingericht.



Figuur 2 geeft een aantal varianten voor de inrichting van een SOC weer. Een SOC heeft een aantal vaste taakgebieden. De regiefunctie zorgt voor verankering in de organisatie en aansturing van het SOC. De kern van het SOC bestaat uit de operationele processen zoals het (real-time) monitoren van informatiestromen. Opvallend dataverkeer en vreemde transacties worden door medewerkers van het SOC geanalyseerd. Indien zich een daadwerkelijk incident (bijvoorbeeld digitale inbraak of netwerkverstoring) voordoet, zijn zij ook verantwoordelijk voor het afhandelen en oplossen van het incident. Eventueel kan dan forensisch onderzoek helpen om de daders op te sporen.

Een SOC bestaat uit een geïntegreerd geheel van mens & organisatie, processen, informatie en technologie. De benoemde taakgebieden moeten langs deze assen van het operating model worden ingericht. Mens en organisatie gaat over de organisatorische inrichting van het SOC en de plaats die het krijgt binnen de organisatie. De taakstelling van het SOC moet daarbij worden afgeleid van de bedrijfsdoelstelling. De administratieve, operationele en technologische processen van het SOC moeten zodanig worden ingericht dat zij hierop aansluiten. Op basis van een risicoanalyse

wordt bepaald wat de meest kritische informatiestromen (de ‘kroonjuwelen’) van de organisatie zijn die primair door het SOC gemonitord, geanalyseerd en beschermd moeten worden. Zie voor integraal risicomanagement ten behoeve van informatiebeveiliging ook het artikel ‘Business value van security begint bij gemeenschappelijk framework’ van Laurens van Nes. De keuzes die hierin gemaakt worden, bepalen mede welke technologische ondersteuning is vereist.

Sommige organisaties (met name in de openbare orde en veiligheidssector) kiezen er – gegeven de gevoeligheid en het belang van de informatie – voor om een SOC volledig intern in te richten, terwijl andere organisaties meer gebaat zijn bij uitbesteding zodat zij de juiste kennis en ervaring binnen halen voor een effectief en efficiënt SOC en zich kunnen focussen op hun core business.

Het hybride model voor een SOC

In een hybride model van een SOC worden enerzijds bepaalde taken binnenshuis uitgevoerd, bijvoorbeeld omdat daarvoor kennis van de organisatie nodig is of omdat bepaalde informatie vanwege wetgeving de organisatie niet uit mag. Anderzijds worden bepaalde taken uitbesteed omdat de organisatie daar zelf de mensen en/of kennis niet voor in huis heeft.

De tabel op de volgende pagina beschrijft de inrichting van het hybride SOC. Langs de assen van het operating model zijn de belangrijkste inrichtingskeuzes benoemd. In de meest rechter kolom zijn deze vertaald naar het hybride model. Door het SOC langs deze assen in te richten, sluit het optimaal aan op de huidige organisatie terwijl het in staat is mee te groeien met veranderende behoeften.

Aspect	Inrichtingskeuzes	Hybride SOC
Mens & Organisatie	1. Waar wordt de verantwoordelijkheid van het SOC belegd? 2. Centraal of decentraal inrichten? 3. Alles zelf doen of taken uitbesteden? 4. Bemensen met intern of extern personeel?	Om het SOC optimaal bij te laten dragen aan bedrijfsdoelstellingen van de organisatie is het essentieel dat het SOC onder een vertegenwoordiger van het primaire proces wordt belegd[1]. Een hybride SOC combineert externe expertise met diepgaande kennis vanuit de eigen organisatie. Logisch is daarbij om het SOC centraal in te richten met eventueel decentrale voorzieningen als locaties geografisch ver uit elkaar liggen.
Processen	1. Welke SOC-processen intern inrichten, welke processen extern laten afhandelen? 2. Hoe worden sturing en kwaliteitsbewaking goed ingericht?	Om het hybride SOC optimaal te laten functioneren, moeten de processen die intern worden belegd en de processen die worden uitbesteed naadloos op elkaar aansluiten. De aansturing van het SOC moet in eigen organisatie worden ingericht. Om te zorgen dat de missie en visie van de organisatie doorklinkt in de doelstelling van het SOC, is het goed om de processen voor sturing en kwaliteitsbewaking intern in te richten. Voor uitvoering van de specialistische taken, zoals diepgaande analyses en forensisch onderzoek, wordt de expertise van een externe partij ingezet.
Informatie	1. Welke bedrijfsprocessen en welke bedrijfsinformatie moeten als eerste worden beschermd? 2. Welke informatie wordt met welke diepgang en welke frequentie door het SOC verzameld? 3. Welke analysemethoden worden ingezet om inbraak vroegtijdig te detecteren?	Om snel waarde toe te voegen, is het belangrijk om te beginnen met het beschermen van de gegevens met de hoogste waarde. Begin dus met bepalen welke gegevensstromen moeten worden gemonitord, op welke wijze events worden gefilterd, met welke diepgang de gegevens worden geanalyseerd en hoe met de uitkomsten wordt omgegaan qua afhandeling en rapportage. Sommige gegevens kunnen bedrijfs- en/of privacygevoelig zijn of onderhevig zijn aan wet- en regelgeving. Een risicoanalyse helpt bij het bepalen welke gegevens het kwetsbaarst zijn en welke maatregelen nodig zijn om de integriteit en vertrouwelijkheid van de gegevens te beschermen.
Technologie	1. Hoe kan de (nieuwe) SOC-technologie zo efficiënt mogelijk worden aangesloten op de eigen infrastructuur? 2. Welke technologische ondersteuning is noodzakelijk (voor de operationele processen en voor de regiefunctie)?	In het hybride model worden de technische systemen van de leverancier gebruikt om gegevens te verzamelen en analyseren. Tegelijkertijd moet de eigen bemanning van het SOC de juiste toegang hebben zodat zij hun werkzaamheden kunnen uitvoeren. Het is belangrijk dat nieuwe technische voorzieningen worden afgestemd op bestaande technische voorzieningen binnen de organisatie. De keuze voor de benodigde technologische ondersteuning zal voor een groot deel op economische gronden worden gemaakt. Daarom is het belangrijk dat er soft- en hardware wordt gekozen dat nu aansluit op de behoefte van de organisatie en de kennis van de medewerkers, maar ook mee kan groeien naar de toekomst.

[1] Zie het artikel "De 7 kritische succesfactoren voor een Security Operations Center" dat Capgemini in opdracht van het Centrum voor Informatiebeveiliging en Privacybescherming (CIP) heeft geschreven.

Hiervoor genoemde inrichtingskeuzes helpen bij het inrichten van een volwassen SOC. Een trend die we de komende jaren steeds vaker gaan tegenkomen is het Security Intelligence Center (SIC), waarin geavanceerde post-incidentanalyse en forensisch onderzoek op de grote hoeveelheden data worden uitgevoerd. Nog een stap verder kan een SIC door de verbeterde analysecapaciteit zich beter wapenen tegen langdurige en doelgerichte cyberaanvallen (zogenoemde advanced persistent threats). Daarnaast zullen we steeds vaker SOC-diensten in de cloud tegenkomen, zoals bijvoorbeeld SIEM-on-top-of-cloud.

Conclusie

In de komende jaren transformeert de overheid naar een moderne, digitale en klantgerichte dienstverlener. Dat vraagt om digitalisering van de kanalen waarmee de overheid communiceert met burgers, bedrijfsleven en partners. Maar het vraagt ook om innovatie van de processen en de ICT naar de digitale manier van werken. Essentiële randvoorwaarde daarbij is dat de betrouwbaarheid, beveiliging en privacy van de digitale dienstverlening van de overheid wordt geborgd. Dat lukt alleen als cybersecurity proactief wordt aangepakt met de inzet van een Security Operations Center.

Over de auteurs

Michail Theuns MSc en Roger Wannee zijn respectievelijk consultant en principal consultant bij Capgemini en als zodanig actief op het gebied van openbare orde en veiligheid. Specifiek richten zij zich op vraagstukken op het vlak van cybersecurity, crisisbeheersing, beleidsrealisatie en bedrijfsvoering.

Voor meer informatie kunt u contact met de auteurs opnemen via michail.theuns@capgemini.com en roger.wannee@capgemini.com