centrum informatiebeveiliging
en privacybescherming

7 Kritische succesfactoren voor een **Security Operations Center**

In het licht van overheidsbrede samenwerking

Deze publicatie kwam tot stand in nauwe samenwerking
met de volgende CIP-netwerkleden:

Inhoudsopgave

Introductie
en werkwijze

Introductie

Overheidsbedrijven en hun ketenpartners (zowel overheid als marktpartijen) verwerken grote hoeveelheden kwetsbare gegevens, waarvan diefstal en misbruik tot grote problemen kunnen leiden. Cyberdreigingen nemen alsmaar toe. Elke dag vinden er hackpogingen, aanvallen en andere incidenten plaats. Het permanent werken aan informatieveiligheid – individueel én gezamenlijk - is nodig om potentiële problemen te voorkomen en, daar waar ze zich voordoen, op te lossen. Werken aan zowel weerbaarheid (vooral preventief en signalerend) als herstelvermogen (vooral reactief en oplossend) is geboden. Het snel in kaart kunnen brengen en analyseren van aanvallen is noodzakelijk voor een snelle en correcte afhandeling van incidenten.

Met een Security Operations Center (SOC) kan een organisatie haar informatieveiligheid dag en nacht controleren en garanderen. Een moderne war-room, van waaruit de organisatie proactief gemonitord wordt. Een Security Operations Center moet echter niet gezien worden als de heilige graal. Zonder een goede inrichting van cybersecurity in de organisatie en een goede voorbereiding van het werken met een SOC, zullen risico's niet automatisch verminderd worden voor uw organisatie.

We zien een toenemende behoefte bij organisaties om een SOC in te richten, aan te haken bij een bestaand SOC of aansluiting te zoeken bij het Rijksbrede denken over een Rijks-SOC (zie rapport Noordbeek over verschillende opties).

Dit whitepaper is tot stand gekomen binnen de CIP-samenwerking. De volgende participanten en kennispartners hebben bijgedragen: Bart Jan Kelter (CAK), Matthijs Ros en Lieke Schepers (Capgemini), Jan van der Sluis en Jan Terpstra (HP), Robin de Haas (TNO) en Inez de Fluiter (UWV).

Met het in kaart brengen van de zeven kritische succesfactoren, willen we in een notendop een aantal belangrijke voorwaarden onder de aandacht te brengen, in de hoop dat het mee kan helpen bij het nadenken over de inrichting van een SOC en het maken van keuzen daaromtrent.

Werkwijze

Tijdens een van de themabijeenkomsten van het CIP Cyber Security Platform (CSP) werd besloten een verkenning te doen naar de mogelijkheden tot samenwerking op het gebied van SOC-activiteiten. Uit het platform werd daartoe bovenstaande werkgroep samengesteld.

In eerste instantie heeft de werkgroep de (zeven) kritische succesfactoren geïdentificeerd. Deze succesfactoren zijn door de werkgroep omschreven.

Vervolgens werden best practices benoemd en werden voor iedere succesfactor interviewvragen opgesteld.

Op basis van interviews binnen de Security Operations Centers van de Belastingdienst, Dictu, DJI, RWS en UWV zijn zeven aanvullend essentiële punten in kaart gebracht. Deze zijn van belang bij het inrichten van een effectief SOC.

De voorlopige resultaten werden gepresenteerd tijdens de najaarsconferentie van het CIP, op 27 november 2014. De uiteindelijke opbrengst van de verkenning vindt u in deze paper.

1. Bepaal je kroonjuwelen

Achtergrond

Weten wat de kroonjuwelen van een organisatie zijn, is essentieel om van een SOC een succes te maken. Kroonjuwelen zijn per organisatie verschillend en kunnen bestaan uit (niet limitatief):

- Privacygevoelige gegevens, informatie onder intellectueel eigendom, financiële data, strategische plannen.
- Procesbeschrijvingen voor vitale infrastructuur.
- Processen en bedrijfsmiddelen die ofwel in belangrijke mate van ICT afhankelijk zijn, ofwel door ICT worden gedreven.

Kortom: de kroonjuwelen zijn die gegevens – of breder gesteld: waarden - die vitaal zijn voor de business en de positie van de organisatie en die bij diefstal of ongewilde publicatie grote risico's voor de organisatie opleveren. Het identificeren en begrijpen van risico's van verlies van 'kroonjuwelen' is daarom een essentiële factor bij het inrichten van een SOC: het beschermen ervan is hét doel van een SOC.

Om de relevante kroonjuwelen per organisatie of zelfs nog per afdeling te kunnen bepalen, is het noodzakelijk om zowel de organisatie in kaart te brengen als de rol die zij speelt in verschillende ketens: een integrale risicomanagementaanpak is nodig om een compleet overzicht te verkrijgen. Met name bij complexe en dynamische ketens en netwerken, waar de regievoering vaak onduidelijk is, kan een als laag geïdentificeerd risico bij een andere organisatie in de keten grote impact betekenen.

Op basis van de aldus geïdentificeerde kroonjuwelen kan er vervolgens een plan worden opgesteld en uitgerold voor een Security Operations Center, dat effectief zal werken bij de bescherming van die kroonjuwelen.

Aanbevelingen

- Voer een risicoanalyse uit en kijk daarbij van buiten naar binnen. Eerste prioriteit is aandacht te geven aan dreigingen van buiten (cyberdreigingen).
- Kies voor 'laaghangend fruit', zo worden grote investeringen voorkomen en kan het bewustzijn van de organisatie ten aanzien van het belang van een SOC groeien.
- Bedenk dat een risicoanalyse alleen mogelijk is met een goed beeld van het IV-landschap.
- Maak een analyse van bekende incidenten, zodat herhaling voorkomen kan worden. Meldingen van incidenten vanuit de organisatie zijn vaak gebaseerd op het bewustzijn van het belang vanuit de eigen organisatie.

Interview

"Kroonjuwelen binnen de overheid zijn de primaire processen en het veilig behandelen van de persoonsgegevens."

"Risico's worden veelal in kaart gebracht met standaard risicomethoden (BIR, ISO 27001), aangevuld met kennis vanuit het NCSC en externe bronnen."

" Risico's dienen ook over de keten in kaart te worden gebracht."

"Organisaties die fysieke objecten beheren, zien deze objecten (waterkeringen, bruggen, sluizen) als hun kroonjuwelen."

2. Stel een Security Baseline vast

Achtergrond

Een Security Baseline bevat de minimale set van eisen waaraan een informatiesysteem moet voldoen om de beschikbaarheid, integriteit en vertrouwelijkheid van de verwerkte en opgeslagen data te garanderen. Compliancy aan de baseline garandeert dus een basisniveau van informatieveiligheid. Er zijn situaties waarin de baseline niet voldoende is. Wanneer dit in risicoanalyse blijkt, moeten aanvullende maatregelen bovenop het baselineniveau worden toegevoegd.

Bij het inrichten van een SOC is het van belang duidelijkheid te hebben over de beveiligingsniveaus. Dit geldt zowel voor SOC's binnen een organisatie als voor SOC's die voor ketens functioneren. Bij de monitoring door het SOC op de verschillende bedreigingen en bij de schifting naar de 'echte' signalen, is het van belang vanuit één zelfde referentiekader te communiceren. Dit geldt bijvoorbeeld voor de relatie tussen opdrachtgever en opdrachtnemer, voor gehanteerde definities, gegevensclassificaties etc.

Baselines zijn er op verschillende niveaus en voor verschillende aandachtsgebieden, bijvoorbeeld:

- Strategisch Niveau: VIR.
- Tactisch omvattend niveau: BIR, BIG, BIWA, IBI (Rijk, gemeenten, waterschappen, provincies).
- Aspectniveaus:
  - Software Development en -onderhoud: SSD (proces en normenkader) voor security by design;
  - NCSC-richtlijnen voor webapplicaties;
  - Privacygericht: verschillende practices voor de PIA.

Het implementeren van deze kaders en richtlijnen is niet eenvoudig, temeer omdat veel organisaties vanuit de historie eigen richtlijnen, kaders en processen hanteren. Het is echter wel van belang om een minimum te bepalen, waardoor elke organisatie ernaar kan streven dit minimum aan inrichting in de eigen organisatie te bereiken om zo gezamenlijk meer dezelfde taal te gaan spreken. Pas als er een basis aan minimale eisen gelegd is, zal de stap om gezamenlijk informatie te gaan delen, een veel kleinere stap zijn.

Aanbevelingen

- Implementeer de VIR/BIR (Voorschrift en Baseline Informatiebeveiliging Rijksdienst).
- Pas SSD (Secure Software Development) toe.
- Hanteer de PIA (Privacy Impact Assessment) als richtsnoer.

Interview

"ISO 27001 aangevuld met BIR wordt door meerdere partijen gebruikt als normenkader. Het gebruik van Secure Software Development is echter voor meerdere partijen geen standaard."

"De VIR/BIR is onder de geïnterviewden veelal de standaard. Wat betreft SSD en PIA is er nog werk te verrichten. Het is absoluut de moeite waard om hierin te investeren en hierbij ook de hulp van het CIP in te schakelen. Zo zijn er platforms (met name de Practitioners Communities) waar gebruikers van deze standaarden ervaringen delen en zorgen voor een continue update van het materiaal."

3. Bepaal de business impact

Achtergrond

Wanneer er een kwetsbaarheid of een incident bekend wordt, moet een Security Operations Center zo snel mogelijk in kaart brengen wat de mogelijke gevolgen zijn: het bepalen van de business impact. Het bepalen van de business impact is het onderscheiden van de kritieke en de niet-kritieke processen binnen een organisatie die geraakt kunnen worden bij incidenten en bedreigingen. De vraag is dan ook: wat is de concrete impact op de organisatie wanneer een mogelijke uitval of verstoring van deze processen plaatsvindt? Dit kan op vele delen van de bedrijfsvoering van toepassing zijn en kan consequenties hebben voor verschillende aspecten, zoals de compliance en beschikbaarheid van vitale processen, maar ook het beheer van vertrouwelijke data.

De business impact richt zich op de in- en externe gevolgen voor de reputatie van de organisatie en de informatievoorziening, en op de eventuele vervolging van betrokkenen. Een goede impact-bepaling vereist een vertaling naar onderliggende applicaties en systemen. Wanneer de situatie op dit niveau in kaart is gebracht, kan bepaald worden welke maatregelen getroffen dienen te worden om schade te voorkomen. Daarnaast dient er bepaald te worden wanneer en hoe betrokkenen geïnformeerd worden over de verder te nemen acties.

Het bepalen van de business impact is een iteratief proces. Nieuwe informatie kan leiden tot bijstelling van het beeld. Belangrijk is dat de actuele situatie onder controle gehouden wordt en dat aanvullende informatie niet tot drastische aanpassingen in de te nemen vervolgacties zal leiden.

Zodra de business impact in kaart is gebracht en de huidige organisatie stabiel is, is de organisatie meer ‘cyber secure’ te maken en een meer volwassen security-organisatie te waarborgen. De maatregelen worden doorgaans door de beheerorganisatie opgepakt en vallen daarmee buiten de verantwoordelijkheid van het SOC. Het SOC kan hier echter een belangrijke adviserende rol spelen. Door regelmatige tests en simulaties uit te voeren en herstelplannen vast te leggen, kan het SOC de alertheid en de weerbaarheid van de organisatie bevorderen.

Aanbevelingen

- Neem informatie die verschijnt op verschillende security fora mee tijdens het bepalen van de business impact. Zo kan er sneller en adequater worden gehandeld en kan mogelijk een zwaar incident worden voorkomen.
- Zorg ervoor dat het SOC hier middelen en aandacht voor heeft. Het monitoren van social media kan deze informatie completeren.
- Houd rapportages bij van testen en simulaties, teneinde de trend op de business impact te kunnen onderbouwen en genomen beslissingen al dan niet te rechtvaardigen.
- Zorg ervoor dat ‘snel schakelen’ organisatorisch mogelijk is. Zo kan het tijd schelen als het SOC de communicatie verzorgt.
- Houd een stekkermandaat achter de hand. In een uiterst geval zal het SOC kunnen besluiten of er systemen en/of processen worden afgesloten om erger te voorkomen.

Interview

“Toolsets helpen bij het in kaart brengen van kwetsbaarheden. Dreigingen worden op die manier aan de voordeur al opgemerkt.”

“Grote kwetsbaarheden, zoals de Heartbleed bug, worden al opgemerkt via social media monitoring. Daarna volgen het NCSC en de leveranciers.”

“Een stekkermandaat wordt ingezet in geval van een grote besmetting.”

4. Weet wat je in huis hebt

Achtergrond

Configuratiemanagement is van essentieel belang voor het adequaat opereren van een SOC. Configuratiemanagement behelst namelijk alle informatie op het gebied van IT welke nodig is om de impact van een incident in te kunnen schatten en daarmee te bepalen wat het business risico is dat de organisatie loopt naar aanleiding van dat incident.

Configuratiemanagement is noodzakelijk om tegen gerechtvaardigde kosten kwalitatief acceptabele diensten te realiseren in de context van de steeds wijzigende gebruikerswensen. Configuratiemanagement is het proces dat alle componenten van het IT-landschap en de daaraan gerelateerde documentatie onder controle brengt ter ondersteuning van incident-, probleem- en wijzigingsbeheer (definitie ITIL). Vanuit het oogpunt van informatiebeveiliging is configuratiemanagement vooral belangrijk als faciliterend proces aan het incidentbeheer, zijnde het tactische proces waaronder ook de informatiebeveiligingsincidenten vallen die in een SOC worden behandeld.

Om de impact van een informatiebeveiligingsincident correct te kunnen duiden, is kennis nodig omtrent de impact van het geraakte/verstoorde configuratie-item (systeemcomponent) op de gebruikersprocessen. In geval van een incident moet men weten welk configuratie item geraakt is en in welke processen het configuratie item gebruikt wordt.

Om een SOC goed te kunnen laten functioneren, is dus gedetailleerd inzicht nodig in het IT- landschap.
Configuratiemanagement geeft inzicht in de samenstelling van de verschillende componenten van het IT-landschap en van de structuur waarin die interacteren. Met deze informatie wordt het mogelijk de impact van een zwakheid in een IT-component te relateren aan een dienst en kan zo de impact voor de organisatie worden bepaald. Deze configuraties kunnen bijgehouden worden in een CM-database.

Voorbeeld:

Er blijkt een kwetsbaarheid te zitten in de gebruikte software van de webshop waardoor het mogelijk wordt om klantgegevens te onderscheppen.

Via het NCSC of eigen bronnen komen dagelijks meldingen van kwetsbaarheden in software binnen bij het SOC. Soms wordt daarbij verwezen naar een patch.

Allereerst wordt een check gedaan of de software gebruikt wordt binnen de organisatie. Uit deze check blijkt alleen of de desbetreffende software wordt gebruikt en of deze up-to-date is. Deze informatie geeft echter nog niet aan wat de impact hiervan is voor het bedrijf.

In de CM-database is echter ook opgenomen dat de betreffende software gebruikt wordt in het 'bestelproces' van de webshop. In de CM-database staat bijvoorbeeld beschreven dat dit proces is geclassificeerd als 'bedrijfskritisch' met een vertrouwelijkheidsniveau 'hoog' omdat er klantgegevens in worden verwerkt.

Op dat moment kan het SOC inschatten dat de impact van deze kwetsbaarheid 'hoog' is en het risico voor het bedrijf dus ook.

In de CM-database is ook de eigenaar van het proces en de eigenaar van het CM-item opgenomen. Beide worden op de hoogte gebracht en kunnen op basis van de informatie van het SOC passende maatregelen nemen.

Aanbevelingen

- Zorg voor eigenaarschap van alle relevante onderdelen voor het bepalen van risico's en te nemen maatregelen. IT-diensten, services en IT-componenten, zijn vastgelegd en worden actueel gehouden.
- Configuratiemanagement voor ingerichte processen staat niet op zichzelf. Dit moet continu gevoed worden door de, op hetzelfde kwaliteitsniveau ingerichte, aansluitende processen.
- Zorg voor de juiste afspraken. Alle taken, bevoegdheden en verantwoordelijkheden moeten goed zijn vastgelegd en bij alle deelnemers bekend zijn.
- Het beheren van een CM-database is complex en dient ondersteund te worden door tooling.
- Zorg voor een koppeling tussen de in de CMDB vastgelegde IT-componenten en de security maatregelen die van kracht zijn.

Interview

"ITIL wordt door de meeste organisaties gebruikt als beheermodel voor het afhandelen van incidenten, wijzigingen en problemen."

"Assets worden in een configuration management database (CMDB) vastgelegd en actief gescand."

"Zodra apparatuur en programmatuur niet door de fabrikanten worden ondersteund, wordt soms gekozen voor extended support. Deze situatie altijd voor zijn!"

5. Weet wie je in huis hebt

Achtergrond

IT-landschappen van organisaties worden steeds complexer. Een belangrijke oorzaak daarvoor is de toenemende hoeveelheid verschillende leveranciers die door de organisatie worden ingeschakeld voor levering en beheer van infrastructuren, applicaties, datacentra en diensten in de Cloud. Integrale Security is door die complexiteit een punt van bijzondere aandacht, maar is lang niet altijd afdoende ingericht. Zeker als de diversiteit aan leveranciers groot is, is bij een incident niet altijd direct duidelijk welke partijen verantwoordelijk zijn voor de afhandeling van het incident.

De incidentafhandeling zal steeds vaker in samenwerking en door meerdere partijen moeten worden afgehandeld, bijvoorbeeld wanneer het een incident betreft dat betrekking heeft op zowel de infrastructuur als de applicatie. Deugdelijk leveranciersmanagement is voor een Security Operations Center een belangrijke voorwaarde voor succes. Alleen door helder in beeld te hebben wie verantwoordelijk is voor welk deel van het IT-landschap kunnen incidenten effectief en efficiënt worden afgehandeld. Er dient dan ook een nauwe relatie te zijn tussen het Security Operations Center en de afdeling die verantwoordelijk is voor het contractmanagement en de Service Level Agreements (SLA's).

Aanbevelingen

- Betrek het SOC bij aanbestedingen.
- Zorg voor een actueel overzicht van het landschap van de organisaties met daarin de verantwoordelijkheden van de verschillende leveranciers.
- Onderhoud warme contacten met de incidentresponseorganisatie of Computer Emergency Respons Team (CERT) (intern/extern).

Interview

"Bij contractmanagement wordt de BIR meegenomen in aanbestedingen."

"Om de leveranciers duidelijke eisen mee te geven, hanteren we bij aanbestedingen 'Grip op beveiliging in Inkoopcontracten' en 'Grip op SSD."

"Leveranciersmanagement legt het fundament voor contractmanagement."

"Het volwassenheidsniveau van de vraag bepaalt het succes van leveranciersmanagement."

"Weet wat er in de markt mogelijk is en zorg dat het aansluit op jouw volwassenheid. Goede aansturing hangt af eigen volwassenheidsniveau."

"Kies een leverancier die meedenkt."

"Er is beperkte samenwerking met het contractmanagement. Leveranciersmanagement wordt ingeschakeld via overleggen en rapportages."

"Het SOC dient vanuit leveranciersmanagement/de organisatie geïnformeerd te worden over veranderingen in leveranciers."

6. Stel je processen vast

Achtergrond

Bij de detectie, analyse en oplossing van securityincidenten is het SOC de spin in het web. Om deze rol goed te kunnen vervullen en daarin ook herkenbaar en transparant te zijn, is het noodzakelijk een duidelijke procesgang te volgen. Heldere, strakke processen, beschreven in bijvoorbeeld een SOC-handboek, zijn hierbij nodig. De uitvoering zal op regelmatige basis moeten worden geaudit.

Tenminste moeten de volgende drie kritische processen worden gedocumenteerd en gevolgd:

1. Een auditable ingericht en gedocumenteerd “deployment” proces voor het installeren, configureren, in gebruik nemen en buiten gebruik stellen van hardware, software en communicatievoorzieningen. Het bijhouden van configuratiewijzigingen in een register (asset model, CMDB) van alle in gebruik zijnde apparatuur (ref: ITIL, COBIT) is van het grootste belang.
2. Een auditable ingerichte en gedocumenteerde werkwijze voor “patching”, dat wil zeggen het op gecontroleerde wijze aanbrengen van veiligheidsverbeteringen (patches) welke door de betreffende fabrikant beschikbaar worden gesteld.
3. Een up-to-date en voldoende gedocumenteerd plan voor managen van securityincidenten. Dit plan dient minimaal te bestaan uit:

- Globale beschrijving van de te nemen stappen voor het vaststellen van de ernst van een securityincident (triage).
- Beslissingsbevoegdheid en mandaatstelling.
- Een lijst met contactpersonen (email, telefoon) die door het SOC moeten worden gewaarschuwd in geval van het optreden van een securityincident.
- Een globale beschrijving van een herstelplan voor de kritische delen van de infrastructuur.
- Een beschrijving van een procedure om het incidentmanagementproces te testen. Deze test dient regelmatig te worden uitgevoerd.

Een nadere toelichting op het begrip mandaat. Een belangrijk organisatorisch principe van een crisisorganisatie in het algemeen, en voor het SOC in het bijzonder, is het mandaat. Deze voorziet in het neerleggen van de operationele verantwoordelijkheid v.w.b. veiligheidsincidenten bij het SOC, teneinde voldoende slagkracht te hebben tijdens crises. Het is duidelijk dat hiervoor draagvlak nodig is op directieniveau. Het mandaat regelt dat het SOC tijdens grotere beveiligingsincidenten op eigen initiatief maatregelen kan nemen en daarbij het primaat heeft boven de hiërarchische lijnen. Hiermee wordt het SOC in staat gesteld (maar ook verantwoordelijk gesteld) om snel te handelen als het echt nodig is.

Aanbevelingen

- Regel de operationele verantwoordelijkheid. Voor de dagelijkse gang van zaken ligt deze bij de hoogste functionaris binnen het SOC en kan niet direct worden beïnvloed door de aangesloten organisaties. Het SOC volgt hierbij erkende internationale standaarden en best practices, aangevuld met wettelijke en contractuele verplichtingen.
- Regel een goed mandaat. Een SOC heeft een eigen mandaat voor het adviseren, initiëren en prioriteren van acties om securityincidenten binnen de aangesloten organisaties op te lossen. Regel hierbij ook het zogenaamde stekkermandaat.
- Regel de financiën. Het mandaat van het SOC mag niet worden beïnvloed door of onderhevig zijn aan budgettaire consequenties.

Interview

“Het afhandelen van securityincidenten is in de meeste organisaties gebaseerd op de standaard serviceprocessen conform ITIL.”

“Via de Servicedesk vindt afhandeling van standaardincidenten plaats, niet-standaard zaken horen dan meer thuis bij een SOC.”

“Voor vertrouwelijkheid en integriteit zijn minder regels. Integriteit – is wanneer acceptabel? Welk percentage integriteit is nodig?”

“Securityincidenten worden op dezelfde wijze behandeld als normale incidenten en worden dan ook binnen het ITIL incidentproces afgehandeld. Wel krijgen ze een aparte markering in ITSM.”

7. Communicatie

Achtergrond

Communicatie, zowel intern als extern, is een vitale functie voor het SOC. Externe communicatie richt zich op burgers, ketenpartners en afnemers/klanten en betreft voornamelijk informatie-uitwisseling over incidenten; interne communicatie richt zich op stakeholders binnen de organisatie en richt zich naast incidentcommunicatie ook op awareness, gedrag en verandermanagement.

Externe communicatie

Externe communicatie richt zich op burgers, ketenpartners en afnemers/klanten en betreft voornamelijk informatieuitwisseling over incidenten. Voorbeelden van triggers voor externe communicatie: gegevens zijn gelekt, al of niet ten gevolge van een hack, door een aanval is een systeem of functionaliteit niet meer beschikbaar, door een storing bij een ketenpartner is de dienstverlening lamgelegd, etc.

Voor bepaalde typen events is er heersende of in maak zijnde wetgeving dan wel bestaan er vormen van protocollering. Belangrijk in dit verband zijn de Wet meldplicht datalekken en het protocol Responsible Disclosure van het NCSC.

Om op een juiste manier de communicatie te kunnen voeren, is het noodzakelijk deze binnen de eigen organisatie goed te protocolleren. Als er sprake is van samenwerking in een SOC met meerdere afdelingen of met andere partijen, dan is het van belang goed af te stemmen (en in het protocol vast te leggen) wat er gecommuniceerd wordt, hoe dat gedaan worden en wie welke rol daarbij heeft. Tijdens incidenten dient dit protocol dan als leidraad en verschaft het transparantie.

Bij incidenten die meerdere ketenpartners treffen, is deze afstemming extra complex. Veelal zal het nodig zijn specifieke onderlinge afspraken te maken op het moment dat communicatie over een incident nodig is.

Het gebrek aan een met betrokken partijen afgestemde communicatiestrategie kan resulteren in verlies van klanten of imago. Om dit te voorkomen, kan een aantal aanbevelingen worden gedaan.

Aanbevelingen voor externe crisiscommunicatie

- Maak een extern communicatieprotocol. Veranker daarin ook wettelijke verplichtingen vanuit de Wet meldplicht datalekken.
- Acteer tijdig en daadkrachtig op i ncidenten. Blijf in de lead.
- Anticipeer op behoeften aan businesscontinuïteit in tijden van crisis.
- Stel een multidisciplinair team samen waarin medewerkers zijn vertegenwoordigd met security-, business-, communicatie-, juridische- en risicomanagementexpertise.
- Deel de boodschap schriftelijk om misverstanden te voorkomen.
- Werk planmatig tijdens een crisis en stuur het crisisteam pas naar huis als het incident is geëindigd.
- Stel templates, een persbericht en overige schriftelijke communicatie op. Zorg dat dit transparant, eenduidig en professioneel gecommuniceerd wordt.
- Blijf servicegericht naar je klant. Daarbij werkt eerlijke communicatie het best.

Interne communicatie

Interne communicatie richt zich op stakeholders binnen de organisatie en richt zich naast incidentcommunicatie ook op awareness, gedrag en verandermanagement. De uitdaging die hier ligt betreft zowel het 'meenemen' van de eigen medewerkers in de nieuwe ontwikkeling, als communicatie met partners binnen het SOC. Het inrichten van een SOC is niet eenvoudig en samenwerking met partners maakt de inrichting nog complexer.

In de communicatie met partners is het belangrijk om een duidelijke en gezamenlijk gedragen doelstelling voor het SOC te formuleren. Hierin zal de doelstelling voor het SOC worden opgenomen en tevens verklaard worden welke veranderingen de organisatie zal ondergaan. Het succesvol verbeteren en de hele organisatie in de gewenste richting bewegen is een uitdagend traject. Continue monitoring van alle handelingen binnen een organisatie kan stuiten op weerstand. Goede uitleg van de doelstelling zal dit stigma helpen voorkomen. Transparante communicatie is hierbij cruciaal.

Motivatie van betrokken personen is bij interne communicatie cruciaal. Eenzijdige focus op regels, methodes en procedures geeft niet het gewenste resultaat bij het realiseren van verbeteringen. Menselijk gedrag speelt een belangrijke rol bij het slagen van een SOC. Het opleggen van sancties leidt in sommige gevallen tot het juiste resultaat, maar in veel gevallen werkt intrinsieke motivatie doorslaggevend. Draagvlak voor de gewenste verandering en compliance zijn grote drivers voor de gewenste verbetering

Het inrichten van een SOC is een goede motivator voor verbetering. Zowel met betrekking tot verbetering van cybersecurity, als voor de verbetering van de interne en externe communicatie. De informatie die uit een SOC voortkomt, helpt om het belang van goede informatiebeveiliging aan te tonen en te benadrukken. Met goede communicatie kan dit de interne medewerker stimuleren om hieraan actief bij te dragen en kan het extern helpen in een verbetering van imago of positie.

Aanbevelingen voor interne communicatie

- Zorg voor een balans in de mate van duidelijkheid en gedetailleerdheid van de richtlijnen en regels en het effect daarvan op menselijk gedrag.
- Wees bewust van het effect van de manier waarop er wordt gecommuniceerd over de gewenste verbetering.
- Vertoon voorbeeldgedrag.
- Geef duidelijkheid over het te bereiken einddoel.

Interview

"Acteren op mediaberichten over incidenten creëert meer bewustwording bij managers en medewerkers."

"Het SOC geeft inhoudelijk input aan corporate communicatie; daar ligt de woordvoering."

"Verantwoordelijkheid voor communicatie ligt primair bij de Security Manager en HRM."

Conclusie

Met een Security Operations Center (SOC) kan een organisatie haar informatieveiligheid dag en nacht controleren en garanderen. Zo'n SOC kan alleen slagvaardig acteren als het is gebouwd op een stevig fundament. Capgemini, CAK, DJI, HP, SVB, TNO en UWV hebben vastgesteld uit welke zeven ingrediënten het SOC-beton moet bestaan.

1. Zorg voor een goede identificatie van de kroonjuwelen die bij diefstal of ongewilde publicatie de grootste risico's voor de organisatie opleveren.
2. Zorg voor een duidelijke security baseline met daarin een minimale set van securityeisen waaraan een informatiesysteem moet voldoen.
3. Goed begrip van de business impact door het onderscheiden van de kritieke en de niet-kritieke processen binnen de organisatie die geraakt kunnen worden bij incidenten en bedreigingen.
4. Professioneel configuratiemanagement om altijd precies te weten wat er in huis is aan ICT.
5. Deugdelijk leveranciersmanagement met duidelijke verantwoordelijkheden voor alle partijen.
6. Heldere en strakke processen die zijn vastgelegd in een handboek binnen het SOC.
7. Goede interne en externe communicatie.

We hebben in dit rapport handvatten aangereikt om aan deze zeven kritische succesfactoren te voldoen. We zijn overtuigd dat ze bijdragen aan een succesvolle invoering van een professioneel Security Operations Center. Een goede voorbereiding is vaak al voldoende om cybercriminelen te ontmoedigen. Wacht niet tot het u overkomt maar maak werk van uw cybersecurity. De investeringskosten wegen gemakkelijk op tegen de mogelijk schadeposten. Kom in actie! Wij wensen u goede en veilige bedrijfsvoering.

Hierbij willen wij de volgende personen bedanken voor hun medewerking aan dit whitepaper.

Karl Lovink	De Belastingdienst	Lead Security Operations Center
Jaap van Wissen	RWS	Projectmanager SOC
Alex Kooistra	UWV	Team Manager Security
Koos van Rijs	Dictu	Manager SOC
Martijn Bouckaert	DJI	Security Officer SOC

centrum informatiebeveiliging en privacybescherming

Het CIP betracht zorgvuldigheid bij het samenstellen van zijn publicaties. Het kan echter voorkomen dat er toch sprake is omissies of onjuistheden, of gedateerdheid. Het is altijd de verantwoordelijkheid van de lezer zelf dit te beoordelen en desgewenst te corrigeren indien hij zich baseert op of gebruikmaakt van een CIP-publicatie. Het CIP ontvangt graag foutmeldingen, commentaar of suggesties.