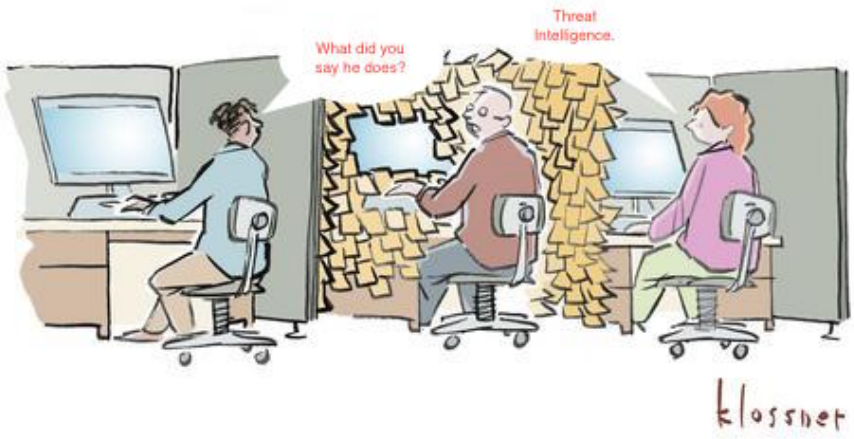
Haalbaarheidsonderzoek Security Operations Center

Programma: P8 – Betrouwbare en veilige omgeving
Deliverable: D.08.03.04.00.D-3
Onderdeel: Adviesrapport



Samenvatting

In hoofdstuk 1 staat een overzicht van alle diensten die door een CERT kunnen worden geleverd en de diensten die door een SOC kunnen worden geleverd. De door een SOC geleverde diensten hangen wel af van het type SOC: controlling, monitoring of operational.

Verder zijn de behoeftes van instellingen op een rij gezet en vergeleken met de verschillende types SOC.

In hoofdstuk 2 is iedere SOC dienst beschreven, waarbij steeds is aangegeven of en hoe SURFnet diensten op het betreffende gebied levert. In een aantal gevallen levert SURFnet onderdelen van een dienst niet, maar is dat ook niet altijd wenselijk. De reden daarvoor is dan bijna altijd dat het leveren van zo'n dienst direct zou ingrijpen op interne (soms primaire) processen binnen een instelling zelf.

Hoofdstuk 3 gaat in op de haalbaarheid van een gecentraliseerd SOC en welke diensten daar dan deel van zouden moeten uitmaken. De conclusie is dat gezien de huidige vraag naar 24*7 dienstverlening en de hoge additionele kosten een gecentraliseerd SOC niet wenselijk is en ook te diep zou ingrijpen op de interne processen binnen de instelling zelf.

In hoofdstuk 4 volgt de aanbeveling om op korte termijn de belangrijkste behoeften op het gebied van SOC onderdelen in te richten met diensten of dienstverlening die recht doet aan de huidige scheiding van verantwoordelijkheden in plaats van te focussen op een 24*7 SOC.

Bepaalde diensten, zoals Security Advies, kunnen door leden van SCIRT/SCIPR geleverd worden en SURFcert kan, voor zover die dat niet al doet, een aantal SOC taken vervullen.

De volgende stap is dan om samen met de instellingen, de communities en SURFcert, te onderzoeken aan welke diensten de grootste behoefte is en of die diensten haalbaar zijn.

Colofon

Programma	P8 – Betrouwbare en Veilige Omgeving
Projectjaar	2016
Projectmanager	Remco Poortinga-van Wijnen, SURFnet
Auteur(s)	Bart Bosma, SURFnet
Reviewers	Thijs Kinkhorst, Xander Jansen
Verschijningsdatum	7 februari 2017
Versie	1.0
Toegangsrechten	extern

This project was made possible by the support of SURF, the collaborative organisation for higher education institutes and research institutes aimed at breakthrough innovations in ICT. More information on SURF is available on the website www.surf.nl.

Inhoudsopgave

1 Achtergrond

In het kader van het innovatieprogramma “Betrouwbare en veilige omgeving” (P8) voert SURFnet een onderzoek uit naar de haalbaarheid van een Security Operations Center.

In dit rapport worden eerst de taken en diensten van zowel een CERT als een SOC op een rij gezet. Voor de taken van een SOC wordt onderscheid gemaakt tussen het type SOC (controlling, monitoring, operational) en wordt per taak aangegeven bij welk type(n) SOC deze hoort. De verschillende taken worden hierna stuk voor stuk kort toegelicht, waarbij ook wordt gekeken in hoeverre deze al door bestaande SURFnet diensten of dienstverlening wordt geleverd. Vervolgens wordt de haalbaarheid van het opzetten van een SOC geanalyseerd, gevolgd door conclusies en een advies voor verdere stappen.

Een aantal SOC taken wordt al (deels) uitgevoerd door SURFcert[1]. SURFcert is geaccrediteerd door FIRST[2]. Met SURFcert heeft een instelling 24 uur per dag, 7 dagen per week ondersteuning bij beveiligingsincidenten. Naast deze ondersteuning biedt SURFcert tools en middelen om de beveiliging in samenwerking met de instellingen te optimaliseren, bijvoorbeeld door ondersteuning bij het opzetten van een lokaal CERT, door een trainingsprogramma (TRANSITS) voor leden van CERT’s te faciliteren en door het verkeer van en naar instellingen te analyseren om vroegtijdig aanvallen te kunnen detecteren.

1.1 CERT diensten

Volgens CERT.org[3] moet een CERT (of CSIRT) vaststellen welke diensten het aanbiedt. Daarbij wordt onderscheid gemaakt tussen reactieve diensten, proactieve diensten en (security) kwaliteitsmanagement.

- **Reactief.** Reactieve diensten worden getriggerd door een gebeurtenis of verzoek, bijv. een melding over een gecompromitteerd systeem, een malwareverspreiding, een kwetsbaarheid in software, of iets dat in een IDS log is gevonden.
- **Proactief.** Proactieve diensten helpen instellingen om hun systemen voor te bereiden op, te beschermen tegen en veilig te maken voor aanvallen, problemen en incidenten. Dit vermindert het aantal incidenten in de toekomst.
- **(Security) kwaliteitsmanagement.** Dit is een aanvulling op bestaande diensten die los staan van incidentafhandeling en wordt in het algemeen uitgevoerd door afdelingen als IT, audit en training. Wanneer een CERT dit uitvoert of erbij assisteert, kan de security van de organisatie verbeterd worden doordat specifieke expertise beschikbaar is. Zo kunnen risico’s, bedreigingen en kwetsbaarheden in systemen sneller geïdentificeerd worden en kan het aantal incidenten uiteindelijk verminderd worden.

In onderstaande tabel staat een overzicht van de diverse diensten die door een CERT uitgevoerd kunnen worden, onderscheiden in de bovengenoemde categorieën. De schuingedrukte diensten worden (geheel of gedeeltelijk) door SURFcert geleverd. Hierop wordt in Hoofdstuk 2 en 3 verder ingegaan.

Reactive Services	**Proactive Services**	**Security Quality Management Services**
Alerts and Warnings *Incident Handling* ▪ *Incident analysis* ▪ Incident response on site ▪ *Incident response support* ▪ *Incident response coordination*	*Announcements* Technology Watch Security Audits or Assessments Configuration and Maintenance of Security Tools, Applications, and Infrastructures	Risk Analysis Business Continuity and Disaster Recovery Planning *Security Consulting* *Awareness Building* *Education/Training*

[1] https://www.surf.nl/diensten-en-producten/surfcert/index.html
[2] Forum for Incident Response and Security Teams, https://www.first.org/
[3] http://www.cert.org/incident-management/services.cfm

Reactive Services	Proactive Services	Security Quality Management Services
Vulnerability Handling ▪ Vulnerability analysis ▪ Vulnerability response ▪ Vulnerability response coordination *Artifact Handling* ▪ Artifact analysis ▪ Artifact response ▪ Artifact response coordination	*Development of Security Tools* *Intrusion Detection Services* *Security-Related Information Dissemination*	Product Evaluation or Certification

Tabel 1: CERT diensten (bron: http://www.cert.org/incident-management/services.cfm)

Hoewel het beeld van de taken en verantwoordelijkheden van een SOC door iedereen anders worden geïnterpreteerd, is deze doorgaans wel breder dan de lijst die traditioneel als behorend bij een CERT/CSIRT wordt gezien.

1.2 Security Operations

In een vorig jaar (intern) gepubliceerde verkenning[4] zijn een aantal vormen van Security Operations onderkend aan de hand van de taken die door een SOC worden uitgevoerd:

- Controlling SOC – uitvoeren van vulnerability scans, compliance testing;
- Monitoring SOC – monitoren van firewalls, Intrusion Detection Systems (IDS), virusscanners;
- Operational SOC – uitvoeren van beheer op firewalls, IDS, certificate management.

Ten opzichte van de originele tabel is (D)DoS protection and mitigation nog toegevoegd. In de SURFnet context wordt dit als vanzelfsprekend aangenomen als één van de door SURFcert geleverde diensten, maar buiten deze context hoeft dat niet zo te zijn (dat wil zeggen: niet ieder CERT/CSIRT levert ook (D)DoS protection and mitigation).

Type SOC	Controlling	Monitoring	Operational
Firewall loganalyse	✔	✔	
Firewall beheer			✔
Intrusion Detection and Prevention (IDP) loganalyse		✔	
Intrusion Detection and Prevention (IDP) beheer			✔
Vulnerability Scan	✔		
Penetration Test	✔		
Compliance Management	✔		
Identity and Access management (IAM) beheer			✔
Risico Assessment	✔		
Sleutel Management			✔
Digitale Kluis			✔
Cyber Intelligence		✔	
Forensics		✔	

[4] WP_Operational_Intelligence_v1.0.pdf

Type SOC	Controlling	Monitoring	Operational
Computer Emergency Response Team (CERT)		✔	
(D)DoS Protection and Mitigation		✔	✔
Data Loss Prevention (DLP)			✔
Security advies	✔	✔	✔
Security Information and Event Management (SIEM)		✔	
Privileged User Management			✔

Tabel 2: Voorbeeld van taken bij verschillende soorten SOCs [1]

1.3 Behoefte bij instellingen

Uit gesprekken met Security Officers van diverse instellingen (zowel universitair als hbo als mbo) en feedback ontvangen na het “SOC seminar” van 15 september 2016, blijkt dat er bij instellingen vooral behoefte is aan:

- Het bundelen van resources, zodat per instelling de kosten lager zijn;
- Het centraal hosten van software oplossingen, zodat per instelling de kosten lager zijn;
- Het analyseren van logbestanden om patronen te herkennen;
- Het ontvangen van “threat intelligence” op regelmatige en gestructureerde wijze;
- Handhaving bestaande incident response support (SURFcert).

In onderstaande tabel zijn de relevante security functies aangegeven; ze komen grotendeels overeen met het “Monitoring SOC”.

Type SOC	Controlling	Monitoring	Operational	Behoefte
Firewall loganalyse	✔	✔		✔
Firewall beheer			✔	✗
Intrusion Detection and Prevention (IDP) loganalyse		✔		✔
Intrusion Detection and Prevention (IDP) beheer			✔	✗
Vulnerability Scan	✔			✗
Penetration Test	✔			✗
Compliance Management	✔			✗
Identity and Access management (IAM) beheer			✔	✗
Risico Assessment	✔			✗
Sleutel Management			✔	✗
Digitale Kluis			✔	✗
Cyber Intelligence		✔		✔
Forensics		✔		✗
Computer Emergency Response Team (CERT)		✔		✔
(D)DoS Protection and Mitigation		✔	✔	✔
Data Loss Prevention (DLP)			✔	✗
Security Advies	✔	✔	✔	✔
Security Information and Event Management (SIEM)		✔		✔
Privileged User Management			✔	✗

Tabel 3: Behoefte van geïnterviewden van onderwijs- en onderzoeksinstellingen

De diensten waar de meeste behoefte aan lijkt te zijn worden hieronder kort beschreven:

1. **Loganalyse**. Door logfiles van systemen zoals firewalls en Intrusion Detection and Prevention (IDP) systemen te analyseren kan beoordeeld worden of zich incidenten hebben voorgedaan. Het meest efficiënt is om de data uit diverse logbestanden te verzamelen in een centraal systeem en die gecombineerde data te analyseren: aggregatie en correlatie. Op basis van de analyse kan een onderbouwd besluit worden genomen over de respons.
2. **Cyber Intelligence**. Het is voor een organisatie belangrijk om te kunnen anticiperen op dreigingen vanuit het internet. Virussen en spam zijn voorbeelden van dreigingen die al door organisaties worden beheerst, maar nieuwe en complexere dreigingen – zoals spear phishing - doen zich steeds vaker voor. Zowel het verzamelen van informatie hierover als het identificeren van aanvallen of georganiseerde criminaliteit vanuit het internet moet zo snel mogelijk plaatsvinden. Informatie uit externe bronnen is daarbij onontbeerlijk.
3. **CERT**. Een CERT kan diverse diensten verrichten en assistentie verlenen wanneer security incidenten zich voordoen.
4. **(D)DoS Protection and Mitigation.** Zoals eerder opgemerkt is dit in de SURFnet context een bijna vanzelfsprekend onderdeel van SURFcert. Met (Distributed) Denial-of-Service protection and mitigation worden instellingen beschermd tegen (D)DoS aanvallen met behulp van een ‘wasstraat’ (‘scrubbing center’), bestaande uit filters op de core routers en een appliance specifiek voor het diep reinigen van vies netwerkverkeer.
5. **Security Advies.** Wanneer security taken gecentraliseerd zijn, ontstaat een goed beeld van dreigingen die bestaan en incidenten die zich hebben voorgedaan. Deze kennis kan bijdragen aan adviezen voor oplossingen en implementaties.
6. **SIEM.** Met een Security Information en Event Management systeem is het mogelijk op basis van logging uit IT componenten, maar ook uit security systemen (firewalls, IDP systemen, enz.) en applicaties, verdachte of ongewenste patronen te herkennen en hierop te alarmeren.

Uiteraard kunnen de behoeftes verschillen per instelling en zal er variatie zijn afhankelijk van de sector/type van instelling (de behoeftes zullen bij het gemiddelde ROC bijvoorbeeld anders liggen dan bij een universiteit). Welke diensten door SURFnet worden geleverd (ongeacht of dit in de vorm van een SOC is) hangt echter uiteindelijk af van de grootste behoefte van de (meeste) instellingen. Dit zal dan gecombineerd moeten worden met een analyse om te bepalen voor welke daarvan het zinvol is deze centraal op te pakken en er zal een sluitende business case moeten zijn waarin ook financiële overwegingen worden meegenomen.

2 Samenhang met bestaande SURFnet diensten

2.1 Inleiding

SURFnet levert al een aantal diensten op het gebied van security, waarvan SURFcert het meest bekende voorbeeld is (hoewel dit wellicht niet wordt gezien als een typische dienst).

De kerndienstverlening van SURFcert is incident response. De basis is een team (kernel) van 10 mensen, 5 intern en 5 extern, die om de beurt weekdiensten draaien om incidenten en risico's te melden en klaar te staan voor assistentie. De kernelleden hebben ieder hun eigen expertises en doen vanuit die expertises vaak meer: ze geven trainingen, presentaties, doen extra projecten, schrijven blogs, etcetera. Op deze manier wordt al invulling gegeven aan een aantal onderdelen van de mogelijke werkzaamheden van een SOC (zie Tabel 2): Het Computer Emergency Response Team (CERT), Security Advies en (gedeeltelijk) Security Information Event Management (SIEM), Cyber Intelligence en Forensics. Het is de intentie van SURFcert om haar takenpakket uit te breiden op een aantal gebieden waar instellingen behoefte aan hebben, daarbij overigens wel oog hebbend voor de scheiding van verantwoordelijkheden tussen SURF(net) en de aangesloten instellingen.

Van oudsher heeft SURFnet zich nooit bemoeid met de invulling van interne processen en verantwoordelijkheden van instellingen, wel worden er voor het gebruik van diensten afspraken gemaakt over de eisen waaraan deze moeten voldoen (denk hierbij bijvoorbeeld aan Identity Management, of de eis dat gebruikers van het SURFnet netwerk voor de instelling identificeerbaar moeten zijn om zo op te kunnen treden bij misbruik van de geboden faciliteiten). In de afgelopen jaren is daar wel een lichte verschuiving in opgetreden, maar alleen daar waar interne processen overal precies gelijk zijn en de verantwoordelijkheden duidelijk afgebakend kunnen worden; SURFwireless is hiervan een voorbeeld. Security raakt potentieel echter alle interne processen, zodat eenzelfde verschuiving op het gebied van security dienstverlening niet zonder meer haalbaar is; het aantal en de verschillen in de processen tussen instellingen is daarvoor te groot om dit uniform te kunnen oplossen. Deze opstelling betekent dat in het algemeen geldt dat vooral die gedeelten van een operationeel SOC die interne processen raken niet door SURFnet kunnen worden ingevuld. Door de variaties in lokale opzet van infrastructuur zullen specialisten op centraal niveau ook over veel bredere specialistische kennis moeten beschikken dan de specialisten on campus, die 'alleen' zeer bekend hoeven te zijn met de eigen infrastructuur; waardoor centralisatie niet automatisch goedkoper is.

Zo zal een instelling zelf verantwoordelijk blijven voor haar eigen securitybeleid en de implementatie daarvan. Dit betekent dan ook dat 'instellings-interne' aangelegenheden (ook voor SURF) niet door SURFcert (kunnen) worden opgelost, uiteraard los van het geven van adviezen over hoe bepaalde zaken op/aan te pakken.

Andere onderdelen van een SOC worden al geheel of gedeeltelijk ingevuld door bestaande (security) diensten. In de rest van het hoofdstuk wordt per onderdeel aangegeven of – en zo ja, welke – een dienst hier geheel of gedeeltelijk invulling aan geeft.

2.2 Firewall beheer en loganalyse

De firewall staat – vanuit SURFnet gezien – 'achter' de aansluiting op het SURFnet netwerk. Dit betekent dan ook – zoals in de inleiding al beschreven – dat beheer daarvan of het doen van loganalyses de verantwoordelijkheid van de instelling zelf is. Overigens speelt hier ook mee dat logs van firewalls zeer privacygevoelig zijn, het verwerken of analyseren hiervan op een centrale plek is vanuit het oogpunt van privacybewaking dan ook niet aan te raden. Firewallbeheer en loganalyse zijn verder onderwerpen die prima door commerciële dienstverleners gedaan kunnen worden, dus ook het ontbreken van aanbod in de markt speelt hier niet. Wel zou – bij voldoende vraag hiernaar vanuit de instellingen – besloten kunnen worden tot een aanbesteding of het opnemen van een aantal aanbieders in de portal van SURFmarket. En uiteraard kunnen via de relevante communities (SCIPR/SCIRT) ervaringen worden uitgewisseld.

2.3 Intrusion Detection and Prevention

Tot een aantal jaren terug bood SURFnet de SURFids dienst aan. Hierbij werden sensors in het netwerk van een instelling aangesloten. De sensors waren eindpunten van (versleutelde) tunnels met een centrale monitoring service die in de gaten hield of er pogingen werden gedaan om toegang te krijgen tot de sensor. Dus eigenlijk was dit een gecentraliseerde honeypot service. Recentelijk is dit concept weer nieuw leven ingeblazen met het opzetten van het Anansi

project[5] in samenwerking met een aantal andere partijen. De sensoren in het netwerk van de aangesloten instellingen zijn 'passieve' monitors die door een strategische plaatsing 'early warnings' zouden kunnen geven van mogelijke bedreigingen en besmetting in het netwerk van de instelling. Doordat de sensoren passief zijn – ze luisteren alleen maar naar verkeer dat langskomt – verstoren ze ook niet de normale werking van het netwerk waarin ze worden geplaatst.

Een ander (nog lopend) project betreft een pilot voor netwerkmonitoring met een derde partij, waarbij een aantal sensoren in (een gedeelte van) het netwerk wordt geplaatst. Na een inwerkperiode om de monitoring in te regelen, zodat geleerd wordt wat gebruikelijk verkeer is, wordt gekeken of er ongebruikelijk verkeer gedetecteerd kan worden. De monitoring is eerst ingezet bij het beheernetwerk van SURFnet – hieruit kwamen geen ernstige dingen naar voren – en daarna bij een aantal instellingen en het popco (SURFnet's VM platform) netwerk in Amsterdam. De pilots moeten inzicht geven in de mogelijke meerwaarde van netwerkmonitoring. Mocht dit leiden tot dienstverlening dan ligt het meer voor de hand dat een dergelijke dienst gezamenlijk wordt ingekocht bij een derde partij dan dat het direct door SURFnet als een dienst wordt geleverd.

Naast deze twee projecten loopt er ook nog een pilot met een klein aantal instellingen in het kader van het Nationaal Detectie Netwerk (NDN)[6].

In alle gevallen zijn er sensors aanwezig in het netwerk van een instelling, wat zou kunnen leiden tot zorgen over mogelijke toegang tot het interne netwerk door (of via) SURF*.

2.4 Vulnerability Scanning

Vulnerability scanning is een effectieve manier om in gebruik zijnde systemen pro-actief en geautomatiseerd te controleren op correcte configuratie en aan-/afwezigheid van bekende kwetsbaarheden. Het wordt als dienst aangeboden in de portal van SURFmarket (bijvoorbeeld Outpost24, maar ook anderen). Verder kan een vulnerability scanner op een VM bij SURFnet gehost worden. Die wordt dan (virtueel) in het eigen netwerk gezet, zodat ook kwetsbaarheden en configuratiefouten op interne systemen gedetecteerd kunnen worden. Dit is een voorbeeld van een dienst waarbij de hardware/software bij SURFnet gehost wordt, maar het beheer ervan en de verantwoordelijkheid voor de data volledig bij de instelling zelf ligt.

2.5 Penetration Testing

Penetration testing is een aanvulling op vulnerability scanning die in de regel niet geautomatiseerd maar on-demand door een specialist wordt uitgevoerd. Terwijl bij vulnerability scanning eigenlijk alleen wordt gekeken of systemen gepatched zijn en of ze gevoelig zijn voor (bekende) kwetsbaarheden en bugs, is het doel van penetration testing (of pen testing) om actief misbruik te maken van zwakheden of tekortkomingen in de (architectuur van) systemen om binnen te dringen. Vaak wordt een pen test uitgevoerd aan de hand van de kwetsbaarheden die een vulnerability scanner heeft gevonden. Pen testing wordt momenteel niet als dienst aangeboden door SURF(net), wel is pen testing software beschikbaar in de portal van SURFmarket. Mogelijkheden om hier toch op een of andere manier invulling te geven is het (laten) geven van pen test cursussen (hier is in 2016 al voorbereidend werk voor gedaan), maar bijvoorbeeld ook het houden van red/blue team oefeningen of crisisoefeningen.

2.6 Compliance Management

Het normenkader Informatiebeveiliging Hoger Onderwijs (IBHO) is gebaseerd op een selectie van maatregelen uit ISO27002:2013. Het normenkader geeft aan wat een onderwijsinstelling tenminste geregeld moet hebben voor de veiligheid en continuïteit van bedrijfsgegevens en de privacy van studenten en medewerkers. De normen zijn gegroepeerd in 6 clusters en per cluster kan met behulp van SURFaudit[7] worden bepaald op welk volwassenheidsniveau (volgens het Capability Maturity Model – CMM) de instelling staat. De scores worden standaard bepaald door een self-assessment, maar SURFaudit biedt ook de mogelijkheid van peer reviews waarbij instellingen elkaars self-assessment beoordelen. Voor het goed kunnen uitvoeren van peer reviews worden cursussen georganiseerd.

[5] Zie: https://www.honeynet.org/node/1277
[6] https://www.ncsc.nl/samenwerking/nationaal-detectie-netwerk.html
[7] https://www.surf.nl/diensten-en-producten/surfaudit/index.html

Naast het IBHO is er ook het Juridisch Normenkader (Cloud)services (JNK)[8] dat normen voor vertrouwelijkheid, privacy, eigendom en beschikbaarheid bij het aangaan van contracten met (cloud)leveranciers beschrijft, conform (Europese) wetgeving. Het bevat standaardbepalingen en een model bewerkersovereenkomst die instellingen een stevige basis geven voor rechtmatige contracten met leveranciers.

2.7 Identity & Access Management beheer

Op het gebied van Identity & Access Management biedt SURFnet de SURFconext dienst aan die het mogelijk maakt met behulp van het instellingsaccount federatief in te loggen op allerhande diensten. Ook wordt met SURFteams de mogelijkheid geboden om – voor diensten die dit ondersteunen – toegang en rechten te verlenen op basis van groepslidmaatschap, zodat dit niet in iedere dienst opnieuw ingericht hoeft te worden. Identity & Access Management (IAM) werd in de inleiding al genoemd als voorbeeld waarbij – bij afname van een dienst door een instelling – afspraken worden gemaakt over de eisen waaraan interne processen en beheer moeten voldoen. Het is hierbij de verantwoordelijkheid van de instelling zelf ervoor te zorgen dat de implementatie aan deze afspraken voldoet.

SURFnet volgt ontwikkelingen op het gebied van het gebruik van externe of centrale identiteiten op de voet (of draagt daar actief aan bij), zoals bijvoorbeeld bij Idensys en iDIN. Maar ook dan zal, als die ontwikkelingen doorzetten, de verantwoordelijkheid van attribuutmanagement bij de instellingen blijven liggen en niet door SURFnet worden opgepakt.

2.8 Risico analyse/Risk management

Op dit moment worden er door SURF(net) geen diensten aangeboden op het gebied van risicoanalyse, risicomanagement of business continuity management. Intern is hier overigens wel een start mee gemaakt. Op langere termijn is dit mogelijk een geschikt onderwerp om verder met de (SCIPR) community uit te werken.

2.9 Sleutel management/Digitale kluis

Sleutel management (sleutelbeheer) wordt – in de strikte definitie – nu niet geboden door SURFnet, al kan SURFcertificaten worden gezien als passend bij dit onderwerp. Wel is er, vooral door het werken met DNSSEC, veel ervaring met het gebruik van HSM's[9]. Ook zal SURFnet in het Polymorfe Encryptie en Pseudonimisatie project van de Radboud Universiteit de rol op zich nemen van vertrouwde derde partij voor sleutelbeheer. De ervaringen die daarmee worden opgedaan kunnen een goede aanleiding zijn om te kijken of dienstverlening op dat gebied wenselijk en haalbaar is.

2.10 Cyber Intelligence/Threat Intelligence

Threat intelligence is het actief bijhouden en analyseren van huidige en mogelijke bedreigingen van een instelling. Afgezien van het herkennen van trends uit incidenten en het signaleren van mogelijke bedreigingen door SURFcert, doet SURFnet niet aan Threat Intelligence en is er ook geen dienstverlening op dit gebied. Wel wordt jaarlijks het cyberdreigingsbeeld[10] gepubliceerd en worden mogelijkheden van Threat Intelligence in innovatieprojecten onderzocht, zoals grootschalige monitoring van de DNS infrastructuur en het aggregeren van Open Source Intelligence.

Daarnaast is er in de communities rondom security (SCIPR/SCIRT) veel actuele kennis voorhanden op het gebied van actuele bedreigingen. Het bijhouden en analyseren hiervan gebeurt echter (nog) niet op gestructureerde wijze. De aanwezige potentie in zowel SURFcert als de communities kan wel een goede basis zijn om Threat Intelligence voor de gehele doelgroep op te zetten.

2.11 Forensics

Forensics is het (achteraf) analyseren van aanvallen en incidenten, met als doel om ervan te kunnen leren en maatregelen te nemen waarmee toekomstige vergelijkbare aanvallen of incidenten voorkomen kunnen worden. Dit is niet een dienst die SURFnet momenteel (structureel) aanbiedt. Wel is hiervoor expertise aanwezig (voornamelijk in SURFcert) die in

[8] https://www.surf.nl/kennisbank/2013/surf-juridisch-normenkader-cloudservices.html
[9] Hardware Security Module, de beveiligde hardware die wordt gebruikt voor digitaal sleutelbeheer.
[10] https://www.surf.nl/cyberdreigingsbeeld

voorkomende gevallen ook wordt ingezet op verzoek van een instelling (meestal na een incident). Dit komt echter slechts sporadisch voor. De vraag is wel of structurele dienstverlening op het gebied van forensics wenselijk is, aangezien er voldoende bedrijven zijn die dienstverlening op dit gebied aanbieden en er bovendien zeer gespecialiseerde kennis voor nodig is.

Het belang van forensics voor de doelgroep is wellicht nog niet eens de dienstverlening op dit gebied zelf, maar het breder kunnen profiteren van de lessen/maatregelen die hieruit voortkomen. Hierin kan SCIRT – de community op het gebied van operationele security – een goede rol spelen.

2.12 Computer Emergency Response Team

SURFnet levert met de dienst SURFcert[11] 24 uur per dag gedurende zeven dagen per week ondersteuning op het vlak van "incident response" aan instellingen die op het SURFnet-netwerk zijn aangesloten. Puur kijkend naar de CERT-functie, treedt SURFcert voornamelijk op als (ondersteunend) coördinator en zal dus niet zelf meldingen oplossen bij instellingen. Wel kunnen ze advies geven hoe om te gaan met incidenten.

2.13 (D)DoS Protection and Mitigation

Een andere belangrijke taak van SURFcert is het analyseren en mitigeren van (D)DoS aanvallen. Wanneer een (D)DoS bij SURFcert wordt gemeld, kan die filters activeren om het effect van de aanval teniet te doen. Bij zware aanvallen kan de “wasmachine” worden ingeschakeld, waarbij het “probleemverkeer” wordt weggewassen en gewoon verkeer wordt doorgelaten zodat de getroffen dienst weer kan functioneren. Dit gebeurt echter alleen na overleg met en in opdracht van de getroffen instelling. In uitzonderlijke gevallen, als de getroffen instelling niet bereikbaar is en alleen dan wanneer dit van tevoren is afgesproken, kan SURFcert mitigerende maatregelen zonder overleg vooraf nemen. Daarnaast onderhoudt SURFcert preventieve rate-limiting filters die permanent geactiveerd kunnen worden als een instelling daarvoor kiest.

2.14 Data Loss Prevention

Data Loss Prevention (software) is bedoeld om tijdig te ontdekken wanneer er (gevoelige) data wordt weggesluisd vanaf de systemen van een instelling en dit dan ook te voorkomen. SURFnet biedt momenteel geen diensten aan op dit gebied. Aangezien zo’n dienst direct zou ingrijpen op operationele systemen van een instelling ligt het ook niet voor de hand dat een dienst op dit gebied door SURFnet aangeboden zal worden. Uiteraard is het wel goed mogelijk dat SURFmarket – bij voldoende vraag vanuit de instellingen – gunstige condities bedingt bij leveranciers van dit soort producten of diensten.

2.15 Security Advies

Het geven van security advies gebeurt momenteel gefragmenteerd en vanuit verschillende kanalen. De communities (SCIRT en SCIPR) leveren hierin een grote bijdrage en zijn alleen daarom al erg waardevol. Ook vanuit SURFcert wordt security advies gegeven, meestal naar aanleiding van incidentmeldingen. Normenkaders zoals IBHO en JNK kunnen tot op zekere hoogte worden gezien als security advies. Daarnaast zijn er in samenwerking met SCIPR een aantal leidraden en starterkits beschikbaar op het gebied van informatiebeveiliging[12]. Voor een meer gestructureerde aanpak van het geven van security advies is het nodig om deze verschillende kanalen te bundelen of er nog meer samenhang in aan te brengen.

2.16 Security Information en Event Management (SIEM)

Security Information en Event Management (SIEM) is – naast SOC – een van de ‘buzzwords’ in de security community de afgelopen jaren. Net als SOC wordt ook SIEM verschillend uitgelegd afhankelijk van wie je het vraagt. Over het algemeen is SIEM het systeem (of proces) waarmee verschillende bronnen van (security) informatie worden gecombineerd en geaggregeerd om op die manier nuttige securityinformatie te krijgen waarop – indien nodig – actie kan worden ondernomen. Er ligt dus een sterke link tussen SIEM en Threat Intelligence. Hoewel SURFnet op dit moment nog geen dienstverlening (of systeem) op dit gebied heeft, lopen er nu wel een

[11] https://www.surf.nl/diensten-en-producten/surfcert/index.html
[12] https://www.surf.nl/over-surf/samenwerking/nationale-samenwerking/scipr/index.html

aantal testprojecten met SIEM's, waaronder Elastic Search/Logstash/Kibana (ELK) en Splunk voor het verzamelen van netwerk- en loggegevens[13] en een project om diverse publieke bronnen met informatie over kwetsbaarheden samen te voegen in een dashboard[14]. Ook wordt gekeken of informatie uit de eerder genoemde grootschalige DNS monitoring te gebruiken is om de filtering van mail (door SURFmailfilter) op spam en phishing te verbeteren.

2.17 Privileged User Management

Privileged User Management behelst het monitoren en autoriseren van speciale gebruikers zoals "root" en "administrator", die zeer veel rechten hebben op het netwerk en op systemen. Dit is typisch iets dat zich afspeelt op het interne netwerk van een instelling en zal daarom niet door SURF(net) worden uitgevoerd in de vorm van een dienst.

3 Haalbaarheid SOC

3.1 Inleiding

Een aantal diensten die door een nieuw in te richten SOC zouden worden uitgevoerd worden nu al door SURFcert/SURFnet uitgevoerd, maar verschillende door instellingen gewenste diensten worden nu (nog) niet door SURFcert/SURFnet uitgevoerd. Daarbij geldt dan wel dat de beschikbaarheid van een SOC 24*7*365 is, zodat te allen tijde alerts kunnen worden opgevolgd en actie kan worden ondernomen om problemen te verhelpen.

3.2 SURFcert

Op basis van de gepeilde behoeftes (zie tabel 3 en hoofdstuk 1.3) dekt het huidige dienstenportfolio van SURFcert een groot deel van de behoeftes af, terwijl een klein aantal zou moeten worden toegevoegd.

Bestaande diensten SURFcert	**Corresponderende SOC taak (tabel 1)**
• Incident response	Computer Emergency Response Team (CERT)
• 24/7 ondersteuning bij beveiligingsincidenten	Computer Emergency Response Team (CERT)
• Coördinatie van incidenten op hoger niveau	Computer Emergency Response Team (CERT)
• Voorlichting over beveiliging	Security Advies
• Forensisch onderzoek / root cause analysis	Forensics
• (D)DoS mitigatie	(D)DoS Protection and Mitigation
Toe te voegen diensten SOC	**Corresponderende SOC taak (tabel 1)**
• SIEM	Security Information and Event Management (SIEM)
• Loganalyse	Firewall loganalyse, Intrusion Detection and Prevention (IDP) loganalyse
• Threat Intelligence	Cyber Intelligence

Security Information and Event Management (SIEM)

SURFcert maakt gebruik van de Application for Incident Response Teams (AIRT)[15]. Met AIRT kunnen op een gestandaardiseerde manier de eigen (interne) beveiligingsinbraken en

[13] afstudeerscriptie Gijs Rijnders (Fontys Hogescholen)
[14] afstudeerscritpie Sjors Haanen (Fontys Hogescholen)
[15] http://airt.leune.com/

incidenten tussen de instelling en andere op SURFnet aangesloten instellingen opgepakt, geregistreerd en opgelost worden. De applicatie ondersteunt geautomatiseerde verwerking van incidentmeldingen en coördinatie van meervoudige incidenten.

Binnen SURFnet lopen op dit moment een aantal testprojecten met SIEM systemen op het gebied van informatieaggregatie en de toepassing hiervan (zie ook 2.16).

Loganalyse

Zoals al vermeld in paragraaf 2.2 zijn er bezwaren, met name op het privacyvlak, om logs centraal te verwerken en biedt de markt al voldoende diensten en producten om hierin te voorzien. Het toevoegen van dienstverlening op dit gebied zou dan ook ingevuld kunnen worden door een aanbesteding of het opnemen van een aantal aanbieders in de portal van SURFmarket. Wel kan worden overwogen hardware/software bij SURF te hosten, waarbij het beheer van het systeem en de verantwoordelijkheid voor de data bij de instelling zelf ligt.

Threat Intelligence

Threat Intelligence is volgens Gartner “kennis over bestaande of opkomende dreigingen, of over gevaren voor IT of informatiesystemen, die gebruikt kan worden om geïnformeerde beslissingen te nemen over maatregelen om die dreigingen of gevaren tegen te gaan”.

Ten dele wordt die kennis al gedeeld via SCIRT (en ook SCIPR) door SURFcert en andere leden van de community, maar dit gebeurt niet systematisch.

Er zijn diverse bronnen, zowel commercieel als publiekelijk beschikbaar, met informatie over actuele dreigingen[16]. Het aggregeren en correleren van informatie uit deze bronnen met lokaal verzamelde gegevens van netwerk- en serversystemen kan waardevolle informatie opleveren over voor instellingen relevante dreigingen, zodat ze effectieve maatregelen kunnen nemen om die dreigingen te voorkomen. Om het volume aan gegevens te kunnen verwerken is het wel noodzakelijk om ze geautomatiseerd te verwerken. Ook hierbij speelt een SIEM systeem een grote rol.

3.3 Inrichting

Verantwoordelijkheden

SURFcert heeft een mandaat om ondersteuning te bieden bij het oplossen van beveiligingsincidenten. De instelling kan beveiligingsinbreuken (incidenten) melden bij SURFcert die de instelling daarna informeert over de voortgang van het incident en (eventueel) advies geeft over het oplossen van het incident. Daarbij heeft SURFcert uitsluitend toegang tot gegevens op het SURFnet netwerk, dus niet op het instellingsnetwerk. Mocht een beveiligingsincident grote schade dreigen op te leveren voor andere instellingen, dan kan SURFcert een instelling in het uiterste geval (al dan niet deels) afsluiten om het functioneren van het SURFnet netwerk voor de andere instellingen veilig te stellen.

Het mandaat van SURFcert heeft dus een heldere en goed gedefinieerde grens.

Zoals ook al aangegeven in de inleiding van hoofdstuk 2 heeft SURFnet zich nooit bemoeid met de invulling van interne processen en verantwoordelijkheden van instellingen, afgezien van afspraken over de eisen waaraan deze moeten voldoen bij afname van specifieke diensten.

Daar waar wel een lichte verschuiving op dit standpunt is te zien – bij SURFwireless – kan dat alleen vanwege de onderliggende eenvormige processen en verantwoordelijkheden. Omdat security mogelijk alle interne processen raakt, is eenzelfde ‘verschuiving’ naar overname van interne verantwoordelijkheden alleen daarom al niet mogelijk op dit gebied en kunnen de gedeelten van een operationeel SOC die interne processen raken niet door SURFnet worden ingevuld.

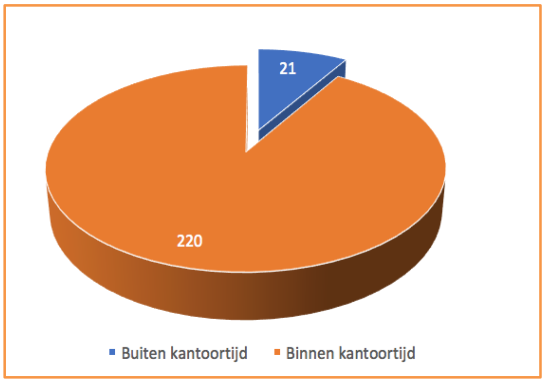
Personele bezetting

Een CERT is in principe reactief: op het moment dat een melding binnenkomt of een incident wordt gesignaleerd wordt er naar gehandeld. Mede daardoor is het voor SURFcert mogelijk met een relatief kleine bezetting (op dit moment 10 personen) alle taken uit te voeren. Om diensten proactief in te zetten en te kunnen voldoen aan een strakke SLA is een veel grotere bezetting noodzakelijk. Bovendien zou voor 24*7 dienstverlening gewerkt moeten worden met dag- en

[16] WP_Operational_Intelligence_v1.0.pdf

nachtbezetting wat een aanmerkelijke uitbreiding van het aantal medewerkers zou vereisen, die ook nog allemaal hoog gekwalificeerd moeten zijn. In de huidige opzet van SURFcert, waarbij de helft van het team bemand wordt door medewerkers van instellingen en de andere helft door medewerkers van SURFnet, die geen van allen hun SURFcert taak full-time doen, is dat niet haalbaar.

Een andere overweging is in hoeverre het huidige gebruik uitbreiding van de dienstverlening naar 24*7 rechtvaardigt. In 2016 zijn tot 12 december 241 telefonische meldingen binnengekomen bij SURFcert, waarvan er slechts 21 (9%) buiten kantoortijd waren (figuur 1).



Figuur 1: telefonische meldingen bij SURFcert in 2016 (tot 12/12/2016)

Het lijkt er dus op dat er momenteel weinig behoefte is aan hulp buiten kantooruren. Daar komt bij dat instellingen buiten kantoortijden (en dus ook in het weekend) slecht beschikbaar zijn, waardoor nu in principe alleen overdag maatregelen ingevoerd kunnen worden om problemen op te lossen.

Om als 24*7(*365) SOC effectief te kunnen opereren is bij iedere deelnemende instelling een lokaal contactpersoon nodig die ook buiten kantoortijd beschikbaar is om op locatie taken uit te (laten) voeren. Hoewel centralisatie van SOC taken kostenbesparing per instelling kan opleveren, blijven deze kosten hoog en, gezien de huidige vraag buiten kantooruren, niet verantwoord.

Huisvesting en voorzieningen

Ter ondersteuning van de SOC taken zijn er diverse voorzieningen nodig, denk bijvoorbeeld aan een aparte ruimte vanwege de gevoelige informatie die wordt getoond op schermen, geavanceerde fysieke beveiligingsmaatregelen om toegang te beperken tot geautoriseerde medewerkers, bezetting van en toegang tot de ruimte 24-uur per dag, speciale hard- en software, monitoring applicaties, enzovoort. De kosten hiervan zullen moeten opwegen tegen de mogelijke voordelen die met een centraal SOC worden behaald.

4 Conclusies en aanbevelingen

Uit de achtergrondinformatie rondom SOC diensten (hoofdstuk1) en de analyse van de samenhang met bestaande SURFnet diensten (hoofdstuk 2) wordt duidelijk dat uitbreiding van het SURFnet dienstenaanbod met (aanvullende) SOC diensten niet altijd wenselijk is.

Ook blijkt dat er in de praktijk (hoofdstuk 3.3) – gezien het aantal meldingen – weinig behoefte is aan hulp buiten kantooruren. Bovendien wordt van de diensten die een gewenst SOC zou leveren een aantal al door SURFnet of SURFcert geleverd. Van een aantal andere is het nu niet gewenst dat deze centraal geleverd worden, omdat ze - in ieder geval bij de huidige scheiding van verantwoordelijkheden - teveel in het domein van de instelling zelf zitten (of zouden ingrijpen).

Afgaand op de behoeften van instellingen, lijkt het dat de 'roep' om een SOC is ingegeven door de behoefte om bepaalde dienstverlening op securitygebied in te vullen zoals die typisch door een SOC geleverd worden. Binnen de huidige kaders zou SURFnet dat kunnen invullen door gewenste dienstverlening zo aan te bieden dat de functionaliteit centraal wordt aangeboden, maar de verantwoordelijkheid over de data bij de instelling blijft, bijvoorbeeld in de vorm van een gehoste SIEM. In die opzet is er geen bemensing vanuit SURFnet nodig.

Van de diensten geleverd door de verschillende typen SOCs wordt een aantal al (geheel of gedeeltelijk) ingevuld door SURFcert, SURFnet en/of de communities. Tabel 4 geeft hetzelfde overzicht van de onderdelen, met daarin per onderdeel aangemerkt of het bestaande dienstverlening is, nog te onderzoeken (of geplande) dienstverlening, danwel dat deze, in de huidige situatie waarbij de grens tussen intern voor de instelling en extern voor de instelling scherp is getrokken, expliciet bij de instelling zelf thuishoort.

Type SOC	Bestaand (gedeeltelijk)	Gepland/ te onderzoeken	Intern Instelling
Firewall loganalyse	✔	✔	
Firewall beheer			✔
Intrusion Detection and Prevention (IDP) loganalyse		✔	
Intrusion Detection and Prevention (IDP) beheer			✔
Vulnerability Scan	✔		
Penetration Test		✔	
Compliance Management	✔		
Identity and Access management (IAM) beheer			✔
Risico Assessment		✔	
Sleutel Management		✔	
Digitale Kluis			✔
Cyber Intelligence		✔	
Forensics	✔	✔	
Computer Emergency Response Team (CERT)	✔		
(D)DoS Protection and Mitigation	✔		
Data Loss Prevention (DLP)			✔
Security advies	✔	✔	
Security Information and Event Management (SIEM)		✔	
Privileged User Management			✔

Tabel 4: SOC diensten ingevuld door bestaande of geplande diensten/dienstverlening

4.1 Aanbevelingen

Gecombineerd met de vaststelling dat een centraal SOC diep in de primaire processen zou kunnen ingrijpen en dat bovendien voor een voltijds bemand SOC het ook nodig is dat er continu contactpersonen binnen de instellingen beschikbaar zijn, leidt dit tot de volgende aanbevelingen:

- Richt op korte termijn geen 24*7 SOC in, maar vul de belangrijkste behoeften op het gebied van SOC onderdelen in met diensten of dienstverlening die recht doet aan de huidige scheiding van verantwoordelijkheden.
    - Voor een gedeelte kan dit samen met de community; zo zal Security Advies ook door leden van SCIRT/SCIPR geleverd worden (zoals nu al gebeurt).
    - Bekijk samen met SURFcert welke dienstverlening door SURFcert kan worden opgepakt en welke apart moeten worden ontwikkeld of, indien bestaand, opgeschaald.
- Onderzoek samen met de instellingen en de communities (en ook met SURFcert) aan welke diensten de grootste behoefte is.
- Stel – samen met SURFcert – een roadmap/plan op voor het onderzoeken van haalbaarheid van die diensten en voer dit uit.