Vorüberlegungen zum Betrieb eines Security Operations Center

Vorgeschaltete Sicherheit

Tim Cappelmann

IT-Sicherheit kommt ohne vorgelagerte automatisierte Erkennungsprozesse kaum mehr aus. Durchgesetzt haben sich sogenannte Security Operations Center, die man selbst betreiben oder ganz oder teilweise Dienstleistern überlassen kann.

Der Betrieb eines Security Operations Center (SOC) ist eine effektive Möglichkeit, auf die heute zu beobachtenden Cyberangriffe zeitgemäß zu reagieren (siehe Kasten „Was ist ein Security Operations Center?“). Kein IT-System ist frei von ausnutzbaren Fehlern (Exploits). Angriffe aus Schadcode nutzen zudem heutzutage gern mehrere Angriffsvektoren gleichzeitig. So ist eine singuläre Perimeterabwehrtechnologie nicht mehr in der Lage, die Angriffe verlässlich zu detektieren.

IT-Nutzer reagieren zunehmend, indem sie klassische IT-Security-Disziplinen wie Schadcodescanner, Firewalls, Intrusion Detection (siehe Glossar) et cetera vernetzen. Die Hersteller der Branche implementieren dazu APIs und bilden Ökosysteme für die Interaktion miteinander. Doch auch bei einer Verbindung dieser „Best-of-Breed“-Technologien wird ein Angriff mittels signaturbasierter Erkennung nicht mehr zum Erfolg führen. Ein Schadcode „überlebt“ im statistischen Mittelwert oft nur Minuten oder Sekunden, bevor er wieder permutiert und für signaturbasierte Scanner bis zum nächsten Update nicht mehr zu erkennen ist.

Die Anatomie der Attacken erfordert es, nicht mehr ausschließlich nach „bekanntem Code“ zu suchen, sondern vielmehr „bekannte Methoden“ im Datenstrom auszumachen. Maschinenbasiertes Lernen, SIEM-Technologien (Security Information and Event Management) und die Erfassung aller Verbindungsdaten an exponierten Punkten im Netzwerk sind die Grundvoraussetzung für eine vollständige Darstellung der aktuellen Lage. Nach den Konzernen passen längst auch Mittelstandsunternehmen die IT-Security an die neuen Gegebenheiten an.

Keine Chance ohne Sicherheitsexperten

Bereits in der Planung der technologischen Ausrichtung stellt sich die bekannte Frage nach möglichen „Plug-and-Play“-Ansätzen, doch diese bleiben letztlich ein Feigenblatt. Hersteller bewerben Umbrella-Lösungen und SIEM-Systeme gern als wartungsarm – doch die Realität sieht leider anders aus. Denn neben der Systempflege durch Spezialisten benötigt jede Erkennungstechnik auch die Sicherheitsanalysten, die der Arbeitsmarkt heute kaum noch bereithält. Ein Security-Analyst wird aufwendig ausgebildet und kennt seinen Marktwert. Die Hochschullandschaft hat zwar mit entsprechenden Vertiefungsrichtungen der Studiengänge reagiert, der Bedarf an Security-Spezialisten wächst allerdings schneller, als diese ausgebildet werden können.

Die Leitungsebene einer IT-Organisation steht damit vor einer gewichtigen Entscheidung, die noch weit vor der Lösung technischer Toolprobleme zu klären ist: „Make IT oder buy IT?“ Diese Bewertung gehört daher ganz nach oben in jede Entscheidungsvorlage zur Implementie-

rung eines eigenen Security Operations Center. Doch sind die Spielarten tatsächlich so digital? Es lohnt sich immer, zunächst alle zu treffenden Entscheidungen für ein mögliches SOC aufzulisten:

– Wer ist verantwortlich für das SOC?
– Lässt sich die SOC-Mission eindeutig beschreiben?
– Welche Stakeholder gibt es, wie sind die Anforderungen zu priorisieren?
– Welche Möglichkeiten für Incident Response stehen prinzipiell zur Verfügung?

Diese Fragestellungen lassen sich weiter auffächern. Mit einer ausreichenden Detailtiefe kommt hier ein nicht zu unterschätzender Change-Prozess an die Oberfläche, der mindestens eine eindeutige Legitimation durch hohe Führungsebenen der Organisation erfordert (Abbildung 1). Ein klarer Auftrag und Kompetenzregelungen sind die absoluten Mindestanforderungen, bevor ein SOC geplant, budgetiert und in der Organisation verortet werden kann. Ein „SOC-Projekt“ auf der Ebene eines IT-Teams erscheint daher unrealistisch – nicht zuletzt weil strategische Fragestellungen zu klären sind. Doch zurück zu den skizzierten Fragen.

Wer ist verantwortlich für das SOC?

Eine reflexartige Zuschreibung von Zuständigkeiten ist oft zu beobachten. Es geht im SOC doch um Cyber-Security-Themen, also ist dies offenbar ein klarer Fall für die Firewall-Admins. Weit gefehlt! Dieser Schluss ist nicht zwingend, oft genug birgt diese Aufgabenbündelung zusätzliche Herausforderungen. Bei der Beschreibung der SOC-Mission wird dies später verdeutlicht.

Ein SOC sollte idealerweise in einer Stabsstelle der Organisation angesiedelt werden – hier bietet sich beispielsweise das Informationssicherheits- oder das Risikomanagement an. Innerhalb bestehender Governance-Funktionsstellen wird sich eine Heimat für das SOC finden. Ob die eingesetzten Analysten dann disziplinarisch in der IT-Linie arbeiten (der Stabsstelle untergeordnet) oder selbst vollständig als Stab agieren, ist zweitrangig.

Die taktische und strategische Ausrichtung sollte man nicht den Firewall-Admins überlassen. Zum einen kontrolliert das SOC auch die Regelqualität der Firewalls – dabei steht im Raum, wie einzelne Funktionen voneinander zu trennen sind –, zum anderen werden Daten aus allen IT-Bereichen und gegebenenfalls auch aus dem Business erhoben. Hier scheitert das Firewall-Team voraussichtlich an Hierarchiegrenzen. Welcher Firewall-Admin hat schon Zugriff auf die Virenscanner der Server, auf die Datenbanklogs des ERP-Systems oder gar auf die Cloud-Instanzen? Der Fokus liegt dabei auf mehr Dingen als auf dem reinen Perimeter. Auch ein Verständnis für Gesamtzusammenhänge der kompletten IT-Architektur darf nicht zwangsläufig dem Firewall-Team zugeschrieben werden. Viele Systemspezialisten richten ihre Aufmerksamkeit zu schnell auf die Technologie.

Was ist ein Security Operations Center?

Das Security Operations Center (SOC) bezeichnet eine Organisationseinheit, die sich ausschließlich um die Cybersicherheit der IT-Systeme kümmert. Ein SOC setzt sich aus Know-how, Technik und den geeigneten Organisationen zusammen. Meist werden Security-Analysten in einem speziellen Leitstand zusammengezogen, von dem aus sie mit IT-Sensorik die Security permanent überwachen und steuern. Ein SOC greift bei Sicherheitsverletzungen ein und lenkt die Gegenmaßnahmen. Dabei besitzen die Spezialisten Methodenkenntnisse der Angreifer und verfolgen stets die aktuellen Trends und Sicherheitslücken auf der Suche nach aktuellen „Indicators of Compromise“ (IoC).

Eindeutiger Zweck eines SOC

An erster Stelle steht die Beschreibung der Mission. Dabei lohnt es sich, über die Details nachzudenken – ein simples Statement „Cyber Security Incidents entdecken“ reicht bei Weitem nicht aus. Die konkrete Beschreibung ist nicht zuletzt deswegen wichtig, weil daraus alle Anforderungen an Technik, Personal und Kompetenzen kausal abgeleitet werden müssen. Das Topmanagement muss einen konkreten Auftrag an das SOC unterschreiben, denn bei der Interaktion mit den vielen beteiligten Organisationseinheiten sind Widerstände absehbar.

Aus der Mission sind Prozessbeschreibungen abzuleiten. Dabei ist Transparenz zu wahren. Alle Vorfälle müssen in gleicher Weise und in vorgegebenen Rechercheschritten bearbeitet werden. Die Prozeduren sollten auch einer Revision standhalten. Ein SOC sollte Cyber Security Incidents verfolgen und nach Bedarf ein Computer Emergency Response Team (CERT) aktivieren. Die Behandlung der Vorfälle durch Field Services und CERT muss nicht mehr zwingend durch das SOC geschehen. Hier bietet sich bereits eine Übertragung der Zuständigkeiten an.

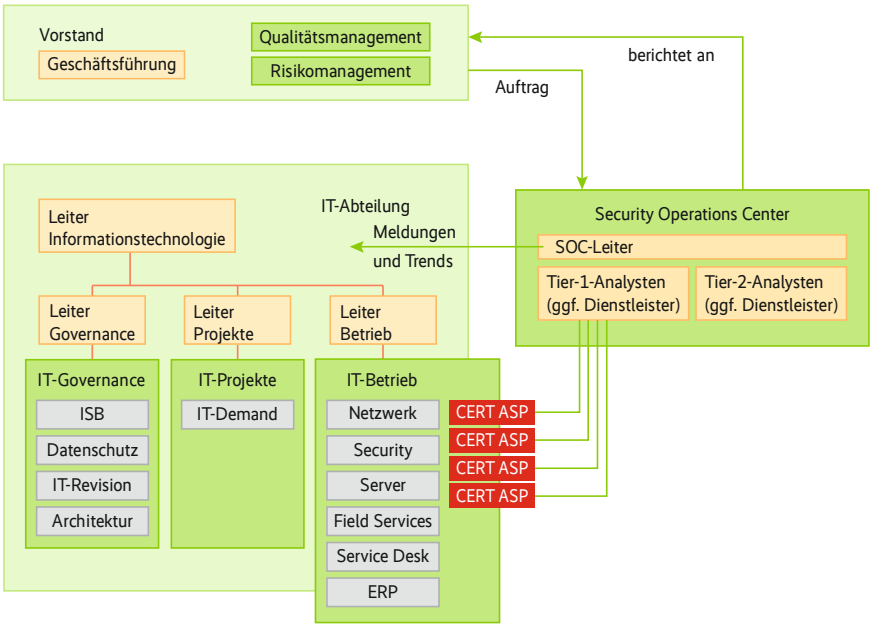
Weiterhin liefert ein SOC Kennzahlen für alle Stakeholder aus dem Bereich Governance, beispielsweise für den Risikomanagementbeauftragten, den Datenschützer, den Informationssicherheitsmanager. Ein SOC hinterfragt permanent die verarbeitete Datenqualität der eigenen Sensorik und justiert diese nach. Alles in allem lässt sich – abgesehen von Katastrophenszenarien – ein SOC als beratende und auch anweisende Organisation beschreiben, weniger als eine Gruppierung der konfigurierenden Systemspezialisten für Perimetersicherheit.

Stakeholder, Anforderungen, Prioritäten

Viele Argumentationen zielen auf das eigene SOC. Compliance-getriebene Organisationsformen werden schnell Kennzahlen und Risikoberichte einfordern. Es

iX-TRACT

- Die Zeit des reinen Perimeterschutzes und der singulären Sicherheitssysteme ist endgültig vorbei – wer sein Unternehmen vor Cyberangriffen schützen will, kommt um eine vorgelagerte Angriffs- und Datenanalyse nicht herum. Etabliert haben sich sogenannte Security Operations Center.
- Nicht für jedes Unternehmen ist es sinnvoll, ein SOC in Eigenregie zu betreiben. Je nach Größe, Personalsituation, Know-how und weiteren Faktoren lohnt es sich, das „Vorfiltern“ und Interpretieren Security-relevanter Daten auszulagern – auch teilweise.
- Beendet ist ein solches Projekt wie auch die IT-Sicherheit im Allgemeinen nie: Stets gilt es, neue Erkenntnisse und Trends, aber auch Erfahrungen und Gelerntes in den Regelbetrieb einfließen zu lassen.

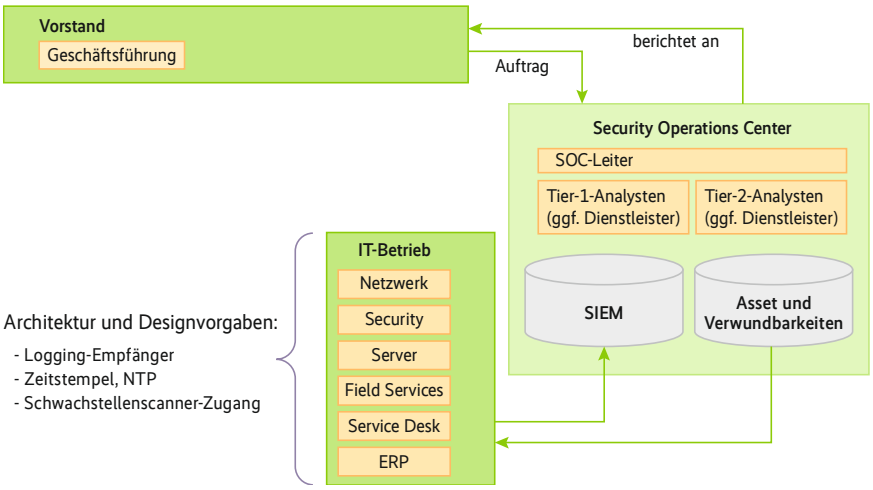


So sieht die ideale Organisation eines SOC im Unternehmen aus: Die oberste Leitungsebene beauftragt und legitimiert das SOC, das wiederum über die benannten Ansprechpartner (ASP) die relevanten Fachteams steuert. Die CERT-Mitarbeiter müssen dem SOC nicht disziplinarisch unterstehen, es reicht hier die fachliche Steuerung durch das SOC (Abb. 1).

besteht die Gefahr, bei den Aufgaben das Augenmerk zu stark auf Reporting-Anforderungen zu richten. Wenn Systemspezialisten ein SOC organisieren, droht hingegen eine Technikschlacht. Administratoren beschaffen in einem solchen Projekt Lieblingssysteme, um eine Waffengleichheit mit den Angreifern herzustellen.

Der Betriebsrat wittert hingegen Leistungskontrolle und bringt Ideen zur Beschränkung allzu umfangreicher Analysen ein. IT-Teams befürchten potenziellen Machtverlust und geben die benötigten Daten „ihrer Systeme“ nicht freiwillig preis. Die mit einem SOC erzeugte Transparenz wird auch nicht von jedem Systembetreuer unterstützt werden. Doch Security-Know-how-Silos sind im Kontext der heutigen Anatomie einer Attacke nicht mehr sinnvoll.

Die Frage nach den beteiligten Interessengruppen ist frühzeitig zu beantworten, eine klare Priorisierung des SOC-Auftrages sollte neben der Unterschrift einer hohen Leitungsebene helfen. Ohne einen unumstößlichen Auftrag wird ein Querschnittsprojekt wie die Etablierung eines SOC in der Organisation nahezu zwangsläufig scheitern.



Jedes beteiligte IT-System muss zwei Designrichtlinien erfüllen: Zum einen muss es Logs an das SIEM im Verantwortungsbereich des SOC senden, zum anderen werden alle Netzteilnehmer aktiv auf Verwundbarkeiten gescannt. Komplexe technische Verflechtungen mit den jeweils eingesetzten IT-Technologien muss es nicht geben (Abb. 2).

Bei der Planung eines SOC muss man sich fragen, welche eigenen Möglichkeiten man hat, auf Security-Vorfälle zu reagieren. Auch wenn ein SOC nicht zwangsläufig die Incident Response übernehmen muss, so sind doch bereits Leitplanken für die benötigten Aufwendungen des SOC erkennbar. Wieso sollte ein SOC 24 × 7 arbeiten, wenn die gegebenenfalls benötigten Fachteams für ein Reagieren gar keine Rufbereitschaft bereitstellen? Wenn keine Regelungen zum Umgang mit verdächtigen Netzteilnehmern existieren, wieso sind dann Field Services oder gar Forensiker auszubilden?

Die Anforderungen aus dem Business werden ganz individuell formuliert. Ein produzierendes Unternehmen in der Linienfertigung wird kompromittierte Systeme nicht abschalten, sondern allenfalls isolieren. Die Entscheidung trifft die Produktion, nicht die IT. Ein Finanzdienstleister wird bei bestätigten Incidents anders reagieren als ein Krankenhausbetreiber. Die denkbaren Varianten der letztlich möglichen Reaktionen geben Hinweise auf ein maßvoll ausgestaltetes SOC.

Strategien zum Aufbau

Bei der Implementierung eines SOC wird es vermutlich immer einfacher sein, ein neues Feld zu bestellen, als bestehende Ablauforganisationen nachhaltig zu verändern. Ein SOC benötigt ein klares und unumstößliches Mandat und erhält damit zwangsläufig auch Macht. Ein vormals gleichberechtigtes IT-Team nun mit dem Teilzeitauftrag zum SOC zu erheben, kann deshalb eigentlich nur scheitern. Eine neue Organisationseinheit mit einer Steuerung aus einer Stabsstelle heraus erscheint nach diesen Überlegungen der schnellste und zugleich krisensicherste Weg zum Ziel zu sein.

Die neue Organisation kann auch skalieren – nicht gleich zu Beginn müssen alle Analysten ausgebildet und am Arbeitsmarkt akquiriert sein. Solange IT-Security nicht das Kerngeschäft des Unternehmens ist, kann man den Einsatz von Spezialisten besser per Service Level Agreement sicherstellen. Eine Aufteilung in Tier-1- (Erstanalyse, Nachweis von False Positives) und Tier-2-Analysten (tiefgehende Forensik) kann hier durchaus helfen.

Es gibt einige Argumente für die Fremdvergabe der Tier-1-Analyse an Dienstleister. Mit dem eigenen Know-how weniger Experten im Hause kann die Dienstleisterqualität weiterhin bewertet werden. Dagegen sind Tier-2-Analysten selten am Wochenende oder nachts im Einsatz, dies kann den eigenen Experten zugemutet werden. Das Outtasking für die First Triage erzielt hingegen sofort Skaleneffekte und Spezialisierungsvorteile – und dies nicht erst im Dreischichtbetrieb.

Tier-2-Analysten müssen in ihren Untersuchungen weiterhin potenziell mit involvierten Anwendern in den Dialog treten. Dies ist mit Dienstleistern ohne Stallgeruch schwer zu organisieren. Eigene Kollegen können benötigte Informationen über zu untersuchende Vorgänge auf dem kurzen Dienstweg effizienter zusammentragen, als dies für externe Spezialisten jemals möglich wäre.

Aus einem weiteren Grund eignet sich die Rolle des Tier-2-Analysten weniger gut für eine Besetzung von außen: Hier ist auch das Verständnis des Business vom Analysten gefordert. Nichtsdestotrotz können Abrufkontingente für einen direkten Zugriff auf Tier-2-Analysten oder IT-Forensiker das eigene SOC schnell handlungsfähig machen.

Letzte Vorbereitungen vor dem Start

Wenn die Aufstellung des Teams steht, ob nun mit Hilfe eines Dienstleisters oder ohne, ist organisationsweit eine simple Architekturvorgabe zu machen. Jeder Netzteilnehmer hat dann ab sofort

- die Systemzeit zu synchronisieren,
- Eventlogs an ein zentrales SIEM zu senden,
- zyklisch Schwachstellenscans aus dem SOC über sich ergehen zu lassen.

Die Umsetzung dieser wenigen Vorgaben hat Projektcharakter, ist aus der Praxis heraus jedoch nicht sonderlich kompliziert (Abbildung 2). Vorbehalte sind zu bearbeiten, die Umsetzung muss überwacht werden. Im SOC hingegen entsteht nun die eigene und sehr spannende interne Tool-Landschaft, die mindestens aus einem SIEM und einem Asset-Management-Werkzeug besteht. Ein internes Ticketsystem, ein Betriebslogbuch und viele begleitende Tools sind als verbindliche Werkzeuge im SOC festzuschreiben.

Schriftliche Prozesse und Handlungsanweisungen innerhalb des SOC sorgen für Transparenz, Formulare für Handlungsempfehlungen und Advisories an die IT-Fachteams helfen in der Gleichbehandlung aller Vorfälle. Gesonderte Geheimhaltungsvereinbarungen mit den Mitarbeitern des SOC-Teams sollten bedacht werden. Kennzahlen sind an den Hauptprozessen zu erheben, um Trends zu erkennen und eine langfristige Steuerung der Qualität des Security Operations Center zu gewährleisten. Jede untersuchte Fehlmeldung triggert einen Lernprozess zur Verbesserung der eigenen Effizienz.

Das SOC arbeitet produktiv – und nun?

Nach einer durchlaufenen Lernkurve wird das SOC in einen Regelbetrieb überführt. Doch auch dann ist die Arbeit nicht abgeschlossen. Die SOC-Leitung muss fortwährend darauf achten, dass die Mission geschützt wird. Die Wahrung der Transparenz und der vorhersehbaren Leistung hilft, Vorbehalte aus zunächst nicht beteiligten Fachteams abzubauen. Eine gewisse Verschwiegenheit und professionelle Kommunikation aller Stakeholder bleibt grade in der Betriebsphase wichtig. Daher ein simpler Ratschlag zum Schluss: Halten Sie sich mit detaillierten PowerPoint-Präsentationen über das eigene SOC lieber zurück.

(ur@ix.de)

Glossar

ASP: Ansprechpartner

Best of Breed: Marktführer seiner Technik

CERT: Computer Emergency Response Team

ERP: Enterprise Ressource Planning: Kernsoftware wirtschaftlicher Steuerung

False Positives: Fehlalarme

First Triage: erste Untersuchung aller Daten, Klassifizierung

IDS, Intrusion Detection System: Sensoren zur Erkennung von Schadcode und Anomalien

ISB: Informationssicherheitsbeauftragter

Incident: Vorfall nach ITIL

Incident Response: Einleitung von Gegenmaßnahmen nach Vorfall

Outtasking: teilweises Outsourcing

SIEM, Security Information and Event Management: Korrelationssoftware zur Logverarbeitung

SLA, Service Level Agreement: vertragliche Verpflichtung eines Dienstleisters

SOC, Security Operations Center: Organisationseinheit zur Überwachung der IT-Sicherheit

Dipl.-Ing. Tim Cappelmann, MBA,
ist Leiter Managed Services bei der AirITSystems GmbH.