DataNavigator

EUROGROUP CONSULTING

DataNavigator #13

September 2022 ISSN 2702-1904

Aufbau eines SOC (Security Operations Center) als Kommandozentrale zur Cyberabwehr

Stefan Bauer

Das steigende Cyber-Risiko erfordert Handeln

Die allgemeine Bedrohungslage in der Informationssicherheit ist gestiegen und verschärft sich weiter. Das Allianz Risk Barometer 2022 schätzt derzeit Cybervorfälle als zweitgrößtes Risiko für Unternehmen in Deutschland ein, gleich nach Betriebsunterbrechungen. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) stellt zudem in Anbetracht des russischen Angriffskrieges gegen die Ukraine eine erhöhte Bedrohungslage für Deutschland fest, insbesondere für die kritische Infrastruktur, der auch Finanzdienstleister zugerechnet werden. Und das wachsende Angebot im Darknet an „Ransomware as a Service“ senkt die technische Einstiegshürde für Cyberkriminelle und hat bereits im Jahr 2021 zu einem starken Anstieg an Ransomware-Angriffen geführt, bei denen Datenbestände des angegriffenen Unternehmens verschlüsselt und damit unbrauchbar gemacht werden.

Es ist daher nicht verwunderlich, dass das Thema IT-Security – und insbesondere Cyber-Security – zunehmend in den Fokus der Aufsicht rückt. Das zeigt sich bspw. in den EBA-Leitlinien für das Management von IKT- und Sicherheitsrisiken (EBA/GL/2019/04) und der Publikation „Risiken im Fokus der BaFin“ vom März 2022, in der Cyberrisiken zu den sechs Hauptrisiken gezählt werden. Die BaFin kündigt darin u.a. an, sich auch im Jahr 2022 intensiv mit Cyberrisiken zu befassen und dazu unter anderem verstärkt dedizierte IT-Prüfungen bei den Instituten und Unternehmen vorzunehmen.

Die zunehmende Nutzung von Open-Source-Software (v. a. Libraries) und verteiltes Arbeiten in der Softwareentwicklung über mehrere Unternehmen (inkl. IT-Dienstleister) hinweg bieten darüber hinaus Raum für weitere Cyber-Angriffsszenarien. Beispielhaft seien zwei Sicherheitsschwachstellen erwähnt: Mitte 2022 wurde entdeckt, dass Unbekannte auf GitHub über 35.000 Repositories kopiert und die Kopien mit einem bösartigen Link versehen haben, der den Angreifern nicht nur kryptografische Schlüssel liefert, sondern auch Zugangstoken für Cloudplattformen.

Die Nutzung von State-of-the-Art-Frameworks in der Softwareentwicklung hat das Sicherheitsniveau der Anwendungen deutlich angehoben, jedoch sind auch diese nicht gegen Sicherheitslücken gefeit, wie das Beispiel der Ende 2021 erkannten Log4Shell-Sicherheitslücke zeigt. Das BSI spricht diesbezüglich von einer „extrem kritischen Bedrohungslage".

Ein Security Operations Center (SOC) ist ein wesentlicher Baustein der Cyber-Security und erhöht die Abwehrfähigkeit signifikant

Um den vielfältigen Bedrohungen durch Cyber-Attacken dauerhaft wirksam begegnen zu können, empfiehlt sich der Aufbau eines Security Operations Centers (SOC). Das SOC bündelt die IT-Security-relevanten Informationen und Aufgaben in einer Kommandozentrale, die stets ein aktuelles Bedrohungslagebild liefert. Zu den Kernaufgaben des Security Operations Centers zählen:

- Governance, d.h. die Erstellung von Richtlinien im Rahmen der Security Governance und Überwachung deren Einhaltung.
- Prevention, d.h. präventive Maßnahmen, wie bspw. kontinuierliche Bedrohungsanalyse, Erkennen von Schwachstellen, Durchführung von Security Assessments etc.
- Monitoring, d.h. proaktives Überwachen des Netzwerks und der Systeme bis zum Endpoint.
- Response, d.h. Maßnahmen zur Schadensbegrenzung und Schadensbehebung, wie bspw. Sperrung und Desinfektion infizierter Clients, Blockieren der weiteren Ausbreitung im Netzwerk etc.
- Analysis, d.h. vertiefte Analysen bei umfangreichen und/oder komplexen Angriffen.

Das SOC bietet damit ein wirksames und umfassendes Instrumentarium für das Vermeiden und Erkennen von IT-Bedrohungen, das Eindämmen und Stoppen von Angriffen sowie zur Schadensbehebung und erhöht damit die Schlagkraft der Cyberabwehr signifikant.

Das SOC kann funktional und organisatorisch minimalinvasiv in die bestehende IT-Organisation eingepasst werden

Das SOC ersetzt nicht die im Unternehmen bereits bestehenden Funktionen der IT-Security, wie bspw. Netzwerk-Sicherheit oder Security Information and Event Management (SIEM), sondern bündelt sie. Dabei müssen IT-Security-Funktionen nicht notwendigerweise organisatorisch dem SOC zugeordnet werden. Jedoch ist im Rahmen der SOC-Governance festzulegen, auf welche in anderen Organisationseinheiten angesiedelten Funktionen der SOC-Manager Durchgriff hat und wie die Berichtswege an das SOC gestaltet sein sollen.
Insbesondere ist ein Zusammenführen aller Cyber-Security-relevanten Informationen im SOC erforderlich, um Doppelarbeiten (bspw. zwischen Analysten im SOC und in der Netzwerk- oder Endpoint-Security) zu vermeiden, um keine Sicherheitslücken durch mangelnde Kommunikation entstehen zu lassen, wenn beispielsweise zwei Organisationseinheiten potenziell dieselben Aufgaben wahrnehmen können, sowie um im Sicherheitsnotfall schnell das vollständige Bild der Bedrohungslage erzeugen zu können.

Abbildung 1 zeigt an einem vereinfachten Praxisbeispiel, dass Kernfunktionen der IT-Security organisatorisch außerhalb des SOC angesiedelt sein können.

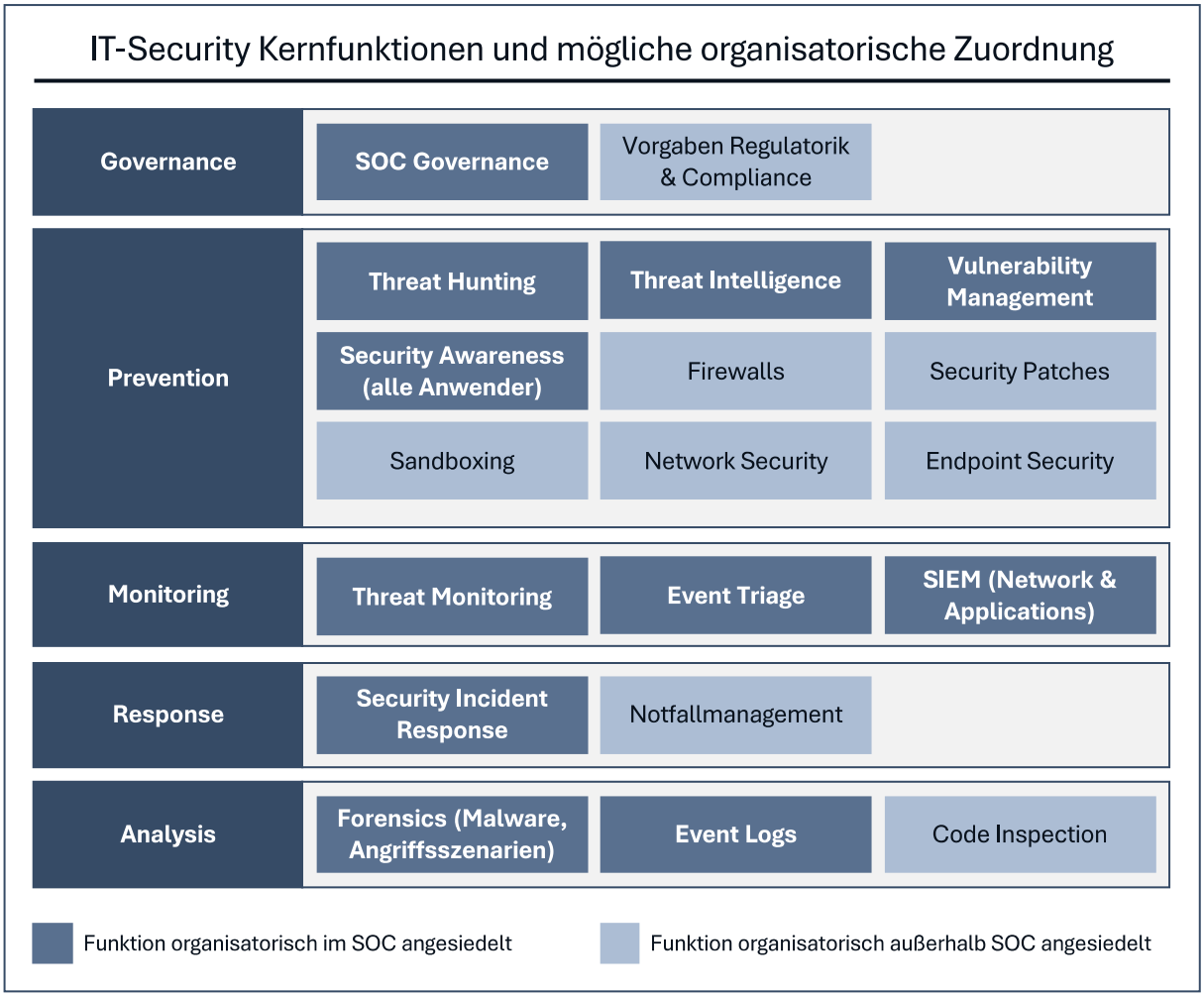

Abbildung 1: IT-Security Kernfunktionen und mögliche organisatorische Zuordnung

Für jede der IT-Security-Kernfunktionen sind die organisatorische Zuordnung (zentral im SOC vs. dezentral in anderen Organisationseinheiten) und die Reichweite der Verantwortung des SOC-Managers – von reiner Informations- über steuernde bis hin zu inhaltlicher Verantwortung – festzulegen. Abbildung 2 zeigt die grundsätzlich möglichen Zuordnungen der IT-Security-Funktionen und deren Verantwortung im SOC.

Abbildung 2: Organisatorische Zuordnung von Funktionen und Verantwortung im SOC

Die hybride Ausrichtung des SOC erlaubt geringeren Personalbedarf und schnellere Implementierung gegenüber einem internen SOC

Der interne Betrieb eines SOC kann sehr personalintensiv sein. Für eine personelle Mindestausstattung ist selbst in kleineren Häusern mit mindestens drei bis vier Personen für jede der drei Analystenrollen zu rechnen. Hinzu kommt, dass Arbeitskräfte mit dem erforderlichen Know-how derzeit schwer am Markt zu finden sind. Der Aufbau eines rein internen SOC-Teams sowie der erforderlichen Know-how-Reife kann damit mehr als drei Jahre in Anspruch nehmen.

Zur Reduzierung des erforderlichen Personalaufbaus und Beschleunigung der SOC-Implementierung bietet sich der Aufbau und Betrieb eines sogenannten hybriden SOC mittels Teilauslagerung an einen Managed Security Service Provider als valide Lösungsoption an.

Neben der schnelleren Umsetzung aufgrund eines eingespielten Teams beim Service Provider ist insbesondere die Nutzung von langjährigem Cyber-Security Know-how des Providers im operativen Betrieb von Vorteil. Der Nachweis dieses Know-hows, bestätigt durch Referenz-kunden, stellt ein wichtiges Entscheidungskriterium im Auswahlprozess dar. Abbildung 3 zeigt ein Kundenbeispiel für die organisatorische Aufstellung eines hybriden SOC.

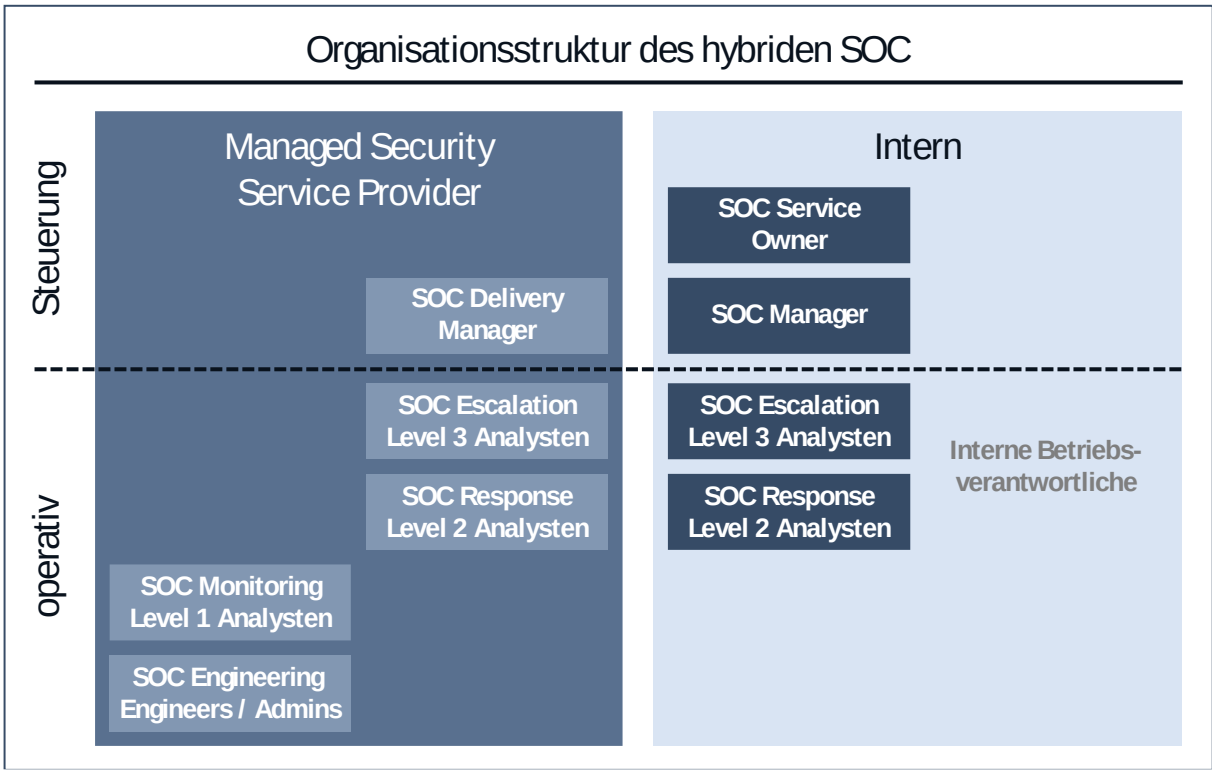

Abbildung 3: Organisationsstruktur des hybriden SOC

Beim hybriden SOC werden intern die Funktionen zur Steuerung und Entscheidung wahrgenommen, während die Hauptlast in Monitoring und Analyse bei dem mit größerem Spezial-Know-how und skalierbaren Kapazitäten ausgestatteten Service Provider liegt. Die Analysten des Providers liefern ihre Ergebnisse an die internen Level-2- und Level-3-Analysten zu, die über das weitere Vorgehen entscheiden.

Die Rollen im SOC

Der SOC-Manger leitet das SOC, stellt die oberste Eskalationsinstanz dar, ist verantwortlich für die Entwicklung und Umsetzung der Cyber-Security-Strategie und SOC-Governance und bildet die Schnittstelle zum SOC Delivery Manager des Providers.

Level-1-Analysten überwachen rund um die Uhr das Auftreten von Sicherheitsvorfällen. Dazu gehören die Überprüfung und Einstufung der Dringlichkeit potenzieller Bedrohungen sowie die Ausfilterung der False-Positive-Fälle (sogenannte Event Triage).

Level-2-Analysten ermitteln Umfang und Ursprung des Angriffs und ergreifen Maßnahmen zur Beseitigung oder zumindest Eindämmung, sowie zur Wiederherstellung von Daten. Bei sehr umfangreichen und/oder komplexen Angriffsszenarien erfolgt die Weitergabe an Level 3.

Level-3-Analysten führen tiefergehende Analysen von Angriffsszenarien (ex-post) und die vertiefte Suche nach sicherheitskritischen Schwachstellen (ex-ante) durch.

SOC-Engineers/Admins sind für Aufbau, Einrichtung und Customizing der eingesetzten Systeme und Tools verantwortlich, sowie für Wartung/Pflege und Administration.

Fazit und Ausblick

Das hybride Security Operations Center

Der Einsatz eines SOC bietet ein umfassendes und wirksames Instrumentarium für das Vermeiden und Erkennen von IT-Bedrohungen, das Eindämmen und Stoppen von Angriffen sowie zur Schadensbehebung. Für Finanzdienstleister ist das SOC ein wesentlicher Baustein zur Erfüllung der gesetzlichen und aufsichtsrechtlichen Anforderungen an die IT-Security.

Die Auslegung als hybrides SOC – unter Nutzung eines Managed Security Service Providers – ermöglicht eine beschleunigte Umsetzung mit reduziertem Personalaufbau im Vergleich zu einer vollständig selbst betriebenen und gemanagten Lösung.

Der Faktor „Mensch“

Dieser Artikel wäre unvollständig ohne einen Hinweis auf die Grenzen der Technik und die Bedeutung des Faktors „Mensch“. Nicht zuletzt aufgrund der verbesserten technischen Möglichkeiten zur Absicherung der IT-Systeme wächst die Anzahl der Angriffe durch sogenanntes *Social Engineering*. Darunter versteht man den Versuch von Angreifern, durch Vorspiegeln einer falschen Identität (vermeintlicher Kollege, angeblich beauftragter IT-Dienstleister etc.) Mitarbeitende zur Preisgabe von internen Informationen oder gar Passwörtern, dem Weiterleiten interner Dokumente oder anderen Schaden erzeugenden Handlungen zu bewegen. Zur Abwehr von Social-Engineering-Angriffen gilt es, alle Mitarbeitenden regelmäßig zu schulen, und zwar zielgruppengerecht, d.h. ohne zu viel „Tech-speak“, beispielweise durch anschauliche Use Cases für Social-Engineering-Angriffsszenarien.

Stay safe, stay secure!

Stefan Bauer ist Manager bei Eurogroup Consulting und Experte für IT-Architektur und IT-Management. Seine Projektexpertise umfasst u.a. die Durchführung von IT-Assessments, IT-Architekturanalysen und Neuaufstellung von Anwendungslandschaften, IT-Strategie, IT-Security, IT-Prozessmanagement sowie die Neuausrichtung von IT-Organisationen. Seit 25 Jahren unterstützt er Kunden aus dem Banken- und Versicherungsumfeld bei der Konzeption und Umsetzung ihrer Vorhaben. Zuvor war er 6 Jahre als Diplom-Informatiker in der Softwareentwicklung tätig.

www.datanavigator.de ISSN 2702-1904

Über den DataNavigator

Unterschiedliche Autoren beleuchten in der Reihe DataNavigator die vielfältigen Facetten des Datenmanagements und zeigen Ihnen interessante Aspekte auf. Der DataNavigator wird von Eurogroup Consulting regelmäßig zweimonatlich herausgegeben und möchte Ihnen interessante Denkanstöße liefern. Wir freuen uns, Ihnen mit dem DataNavigator unsere Erfahrungen weiterzugeben und stehen Ihnen für die Diskussion gerne zur Verfügung! Sie erreichen Autoren und Herausgeber bei Anregungen und Feedback unter der E-Mail-Adresse *datanavigator@eurogroupconsulting.de*.

Bisher erschienen:

#1 Dr. Marco Weiß – *Welt und Wesen des Datenmanagements*; September 2020

#2 Mario Kubik – *„DLT" – Potenzial zur Zukunftstechnologie?*; November 2020

#3 Jonathan Misler – *Verwendung von Daten und Modellen in datengetriebenen Geschäftsmodellen*; Januar 2021

#4 Johannes Bänsch – *Data Analytics und die Cloud*; März 2021

#5 Kurt Tanneberger – *Ja, wo sind sie denn? – Daten im IT-Betrieb*; Mai 2021

#6 Thomas Tiebor – *Data Governance als Fundament guten Datenmanagements*; Juli 2021

#7 Dr. Marco Weiß – *Artificial Intelligence – Nature or Nurture?*; September 2021

#8 Binjamin Sancar, Hermann Sgardelli – *Vertriebschancen in einer Bank durch Nutzung ihrer Daten und ihres Ökosystems*; November 2021

#9 Abdalla El Kadi – *Datenvisualisierung – eine Geschichte in Bildern*; Januar 2022

#10 Carsten Kuhlmann – *Kundenfokussierung: Daten und Technik*; März 2022

#11 Luca Winters – *CIEM – Cloud Infrastructure Entitlements Management*; Mai 2022

#12 Kristian Buric – *Der Informationsverbund - Daten (nur) für die Aufsicht?*; Juli 2022

#13 Stefan Bauer – *Aufbau eines SOC (Security Operations Center) als Kommandozentrale zur Cyberabwehr*; September 2022