SOC ABC

Anforderungen und Sinnhaftigkeit eines SOCs: Wer benötigt es?

23. Februar, 2024 05:46

Analog zum Irrtum „Wer soll mich schon hacken?" haben Security Operation Center sowohl für KRITIS-Betreiber, Großkonzerne aber auch für mittelständische Unternehmen eine elementare Daseinsberechtigung.

Zudem werden spätestens mit der EU NIS2-Umsetzung und dem KRITIS-Dachgesetz (EU RCE) strengere Cyber-Security-Vorschriften verpflichtend. Damit verschiebt sich die Gruppe derer, die ein SOC betreiben sollten, zu denen, die eines betreiben müssen. Gleich bleibt für alle allerdings die Frage, was es zu beachten gilt.

In einer digitalen Ära, in der Cyberkriminalität zunimmt, ist ein Security Operations Center ein unverzichtbares Instrument für den Schutz der Unternehmensdaten und die Aufrechterhaltung einer robusten Sicherheitsarchitektur. Das Konzept eines modernen SOCs berücksichtigt die sich ständig verändernde Bedrohungslandschaft und nutzt fortschrittliche Technologien, effiziente Prozesse und qualifiziertes Personal, um eine umfassende Sicherheitsstrategie zu gewährleisten und die Cyberresilienz zu fördern.

Es leuchtet ein, dass es für Betreiber kritischer Infrastrukturen erforderlich und für große Konzerne sinnvoll ist. Doch zeigt die Erfahrung, dass nicht nur diese Unternehmen Cyber-Bedrohungen ausgesetzt sind. Auch mittelständische Unternehmen sehen sich der täglichen Herausforderung ausgesetzt, ihre Daten zu schützen und Ausfälle zu verhindern, die beispielsweise durch erpresserische Angriffe verursacht werden.

Notwendig wie die Sicherheitszentrale im Kaufhaus

Welche Unternehmen über ein SOC nachdenken sollten, zeigt ein einfacher Vergleich: SOCs sind wie Sicherheitszentralen zum Beispiel in großen Einkaufszentren: Wo viele Geschäfte mit wertvoller Ware zusammenkommen, sollen Prozesse reibungslos funktionieren und Diebstähle sowie andere Vorfälle vermieden werden. Vergleichbar dazu, stellt ein SOC sicher, dass die digitale Sicherheit gewährleistet wird. Es identifiziert proaktiv Bedrohungen, reagiert schnell darauf und ergreift kontinuierlich Maßnahmen zur Verbesserung der Sicherheitslage.

Die Beweggründe für ein SOC entsprechen daher in etwa jenen für eine Sicherheitszentrale im Einkaufszentrum: Ist es ratsam Probleme frühzeitig zu erkennen, indem wie mit Kameras im Einkaufszentrum die Aktivitäten und Netzwerke ständig überwacht werden? Ist es erforderlich, dass die Experten im SOC auf verdächtige Aktivitäten, Anomalien oder Cyberbedrohungen schnell reagieren können und sie eindämmen? Soll eine zentrale Stelle eingerichtet werden, deren Aufgabe es nicht nur ist, koordiniert Maßnahmen einzuleiten, sondern auch Informationen zu protokollieren, zu dokumentieren, zu analysieren und für zukünftige Sicherheitsvorfälle daraus zu lernen?

Die Antwort auf diese Fragen lautet in der Regel „ja"! Insgesamt zeigt sich damit, dass die Einrichtung eines SOCs nicht nur eine strategische Entscheidung für große Unternehmen ist, sondern auch für kleine und mittelständische Unternehmen von großer Relevanz sein kann. Ein SOC stärkt die gesamte Sicherheitsinfrastruktur und verbessert die Reaktionsfähigkeit auf Sicherheitsvorfälle. Gleichzeitig ist es schlicht und ergreifend zur Einhaltung gesetzlicher Vorschriften manchmal notwendig.

Verpflichtend durch Gesetzesänderungen

Diese rechtliche Vorgaben sind das IT-Sicherheitsgesetz (IT-SIG) und die Network and Information Security Directive (NIS). Allgemein gilt für die meisten Gesetzte, dass sie laufend Änderungen und Anpassungen unterliegen. Das ist sinnvoll, insbesondere in der IT-Sicherheit, die sich selbst schnell entwickelt. Sie zielen auf die Stärkung der Cybersecurity ab und gelten für alle Betreiber kritischer Infrastrukturen. In Kürze greifen jedoch Änderungen durch das IT-SIG 2.0 und die NIS2, die dann mitunter auch Unternehmen betreffen, die bislang kein SOC betreiben mussten.

So gilt gemäß des IT-SIG 2.0, dass Unternehmen in der Lage sein müssen, IT-Sicherheitsvorfälle zu identifizieren und angemessen zu managen, Mindeststandards für die IT-Sicherheit einzuhalten und erhebliche IT-Sicherheitsvorfälle zu melden. Die NIS2 verlangt von Betreibern wesentlicher Dienstleistungen (OES), dass sie die Kontinuität ihrer Dienste sicherstellen, erhebliche Sicherheitsvorfälle identifizieren und melden sowie mit zuständigen Behörden zusammenarbeiten müssen.

Wer KRITIS-Betreibende sind, wie die neuen Sektoren nach den Gesetzesänderungen aufgeteilt sind und welche Einrichtungen neu betroffen sind, zeigen Seiten wie openkritis.de sehr anschaulich. Allgemein gilt aber, dass die Beweggründe für ein SOC im Kontext von IT-SIG 2.0 und NIS2 somit in der Erfüllung gesetzlicher Anforderungen liegen: der Sicherung der IT-Infrastruktur, der schnellen Identifikation von Sicherheitsvorfällen und der Förderung der Cyberresilienz von Unternehmen und kritischen Dienstleistungen.

Unterschiedliche Vorlaufzeiten bachten

Sind die Investitionen in ein Security Operation Center beschlossen, kommen neue Fragen auf: Was gilt es vorzubereiten? Die Vorlaufzeiten bis zur Inbetriebnahme können stark variieren und hängen von verschiedenen Faktoren ab. Ausschlaggebend sind beispielsweise die Größe und Komplexität des Unternehmens, die vorhandene IT-Infrastruktur, die Art der zu schützenden Daten, die Budgetverfügbarkeit und die erforderlichen technischen Ressourcen. Auch externe Faktoren beeinflussen die Vorlaufzeit, darunter die Verfügbarkeit von qualifiziertem Personal, die Auswahl geeigneter Sicherheitslösungen, die Integration von bestehenden Sicherheitsmechanismen oder die Einhaltung gesetzlicher Vorschriften.

Kleine Unternehmen, die weniger komplexe IT-Infrastrukturen haben, könnten ein SOC entsprechend schneller implementieren. In solchen Fällen kann die Einrichtung möglicherweise innerhalb von wenigen Wochen erfolgen. Für mittelgroße Unternehmen mit komplexeren Anforderungen könnte die Vorlaufzeit zwischen sechs Monaten und einem Jahr liegen. Dies umfasst die Evaluierung von Lösungen, die Anpassung an die Unternehmensstruktur, die Implementierung von Technologien und die Schulung von Mitarbeitern. Größere Unternehmen mit komplexen Netzwerken, umfangreichen IT-Ressourcen und einer Vielzahl von Anwendungen können mehr als ein Jahr in Vorlaufzeit einplanen.

In der Regel lässt sich sagen, dass die Einrichtung eines SOCs ein umfassender Prozess ist, der einige Zeit in Anspruch nimmt. Es ist jedoch wichtig zu beachten, dass es nicht nur mit der Einrichtung allein getan ist. Ebenso notwendig sind die kontinuierliche Anpassung und Verbesserung, um mit den sich ständig verändernden Bedrohungslandschaften Schritt zu halten. Diese Aufgaben erstrecken sich über den gesamten Lebenszyklus des SOCs.

Typische Fehler vermeiden

Bei der Einrichtung und dem Betrieb von SOC treten immer wieder vermeidbare Fehler auf. Ein häufiger Fehler ist es, die genauen Ziele des SOCs nicht klar zu definieren. Ohne klare Zielsetzung kann es schwierig sein, die Effektivität des SOCs zu messen und sicherzustellen. Diese wiederum können nur mit ausreichend finanziellen Mitteln, angemessenen technologischen Ressourcen und qualifiziertem Personal erreicht werden. Für Letzteres gilt: Ist das SOC-Personal nicht ausreichend geschult, kann dies zu schlechtem Incident Response Management führen.

Ein weiterer, häufiger Fehler besteht darin, verschiedene Sicherheitstechnologien zu nutzen, die sich nicht ergänzen beziehungsweise nicht effektiv miteinander kommunizieren. Dies kann zu einer fragmentierten Sicherheitsinfrastruktur führen und die Reaktionsfähigkeit beeinträchtigen. Auch die unzureichende Kommunikation innerhalb des SOC-Teams oder mit anderen Abteilungen des Unternehmens kann zu Informationslücken führen, die die Effizienz der Bedrohungserkennung und Reaktion beeinträchtigen.

Schließlich gehört zu den häufigsten, vermeidbaren Fehlern die fehlende Anpassung an die Bedrohungslandschaft. Ein SOC, das nicht kontinuierlich aktualisiert und an die sich ändernde Bedrohungslandschaft angepasst wird, kann an Wirksamkeit verlieren. Der Mangel an Flexibilität führt dazu, dass neue Bedrohungen übersehen werden. Gleichzeitig gilt, dass obwohl Automatisierung wichtig ist, eine übermäßige Abhängigkeit davon zu Fehlalarmen führen kann. Die menschliche Intuition und Überprüfung bleiben entscheidend, was wiederum Schulungen wichtig macht.

Fazit

Ein Security Operation Center ist weit mehr als nur die Erfüllung gesetzlicher Vorschriften. Unternehmen stellen sich durch SOCs gegen aktuelle Cyberbedrohungen und rüsten sich gleichzeitig durch aktive Weiterentwicklung gegen kommende. Moderne SOCs integrieren beispielsweise KI und maschinelles Lernen, dezentrale Intelligenz, Automatisierung und Orchestrierung, Incident Response-Planung oder Echtzeitanalysen und verbessern den Schutz gegen Cyber-Attacken kontinuierlich. Ein SOC ist daher auch eine strategische Entscheidung, um das Vertrauen von Kunden und Partnern zu stärken.

Jedoch ist ein SOC keine Amazon-Bestellung. Es benötigt vorab entsprechend Vorlaufzeit und professionelle Planung und während des Betriebes eine kontinuierliche Aktualisierung und Anpassung. Das betrifft auch das SOC-Personal, denn: Bei aller notwendiger Automatisierung, ohne fähige Mitarbeitende kommt es durch den Fehlerfaktor Mensch zu Fehlinterpretationen, Störungen oder anderweitig Problemen, die den reibungslosen Betrieb eines SOCs limitieren.

Birger Kaudasch

EWE TEL GmbH - Cyber Security Planner

Birger Kaudasch ist als Cyber Security Planner im Bereich SOC (Security Operations Center) verantwortlich für die Planung und Entwicklung der technischen Infrastruktur sowie der Prozesse. Er wählt Sicherheitstechnologien wie z.B. SIEM, IDS/IPS und EDR aus und implementiert sie, um eine effektive Erkennung, Analyse und Reaktion auf Sicherheitsvorfälle zu ermöglichen.