Bild: Pixabay

Um auch KMU zu unterstützen, wurde ein Konsortium zur Erarbeitung einer DIN SPEC gegründet.

Security Operation Center: Zentraler Pfeiler der Cybersecurity

Verschiedene Statistiken zeigen, dass zwischen einem erfolgreichen Einbruch in ein Computer-Netzwerk, bis zum Entstehen eines Schadens, zum Beispiel durch Datendiebstahl oder Ransomware, zwischen zwei Wochen und drei Monaten liegen.

In dieser Zeit konfigurieren die Hacker eine Hintertüre, damit sie jederzeit wieder Zugriff haben, sehen sich im Netzwerk nach spannenden Informationen um und planen, wie sie möglichst viel Geld erpressen können. In dieser Zeit hinterlassen sie Spuren auf Systemen und in Logdaten. Nur wenn diese genau untersucht werden, kommt man ihnen genügend früh auf die Schliche. Die oft mühsame Log-Analyse liefert wichtige Hinweise auf einen erfolgreichen Einbruch. Ein Security Operation Center (SOC) kann diese Aufgabe übernehmen und unterstützend wirken.

ZUM AUTOR

Andreas Wisler, Dipl. Ing FH
goSecurity AG
Schulstrasse 11
CH-8542 Wiesendangen

T +41 (0)52 511 37 37
www.goSecurity.ch
wisler@gosecurity.ch

Was ist ein SOC?

Ein SOC ist ein spezialisiertes Element, das sich auf die Überwachung, Analyse und Reaktion auf Cybersecurity-Bedrohungen rund um die Uhr konzentriert. Es handelt sich um eine zentrale Anlaufstelle, die aus Expertenteams besteht, die mit verschiedenen Tools und Technologien ausgestattet sind, um die IT-Infrastruktur eines Unternehmens zu schützen. Die Hauptaufgaben eines SOC umfassen das kontinuierliche Monitoring von Sicherheitsereignissen (Logdaten), die Erkennung von Anomalien, die Untersuchung von Sicherheitsvorfällen und die rasche Reaktion auf identifizierte Bedrohungen.

Vorteile eines SOC

Die Implementierung eines SOC bietet zahlreiche Vorteile:

- Proaktive Überwachung: Ein SOC ermöglicht die fortlaufende Überwachung und Analyse der Netzwerkaktivitäten, was zur frühzeitigen Erkennung potenzieller Sicherheitsbedrohungen führt.
- Schnelle Reaktionsfähigkeit: Bei Erkennung einer Bedrohung können sofortige Massnahmen ergriffen werden, um den Schaden zu minimieren. Oft sind SOCs 7x24 Stunden besetzt, was auch in der Nacht und am Wochenende eine schelle Reaktion ermöglicht.
- Expertise und Fachwissen: Sicherheitsexperten, die spezialisiertes Wissen über verschiedenste Bedrohungsvektoren und Schutzmassnahmen besitzen, untersuchen die Ereignisse.
- Compliance: Viele SOCs helfen Unternehmen, gesetzliche und regulatorische Anforderungen zu erfüllen, indem sie sicherstellen, dass die Sicherheitsmassnahmen auf dem neuesten Stand sind.

Nachteile eines SOC

Trotz der Vorteile gibt es auch Herausforderungen und Nachteile:

- Hohe Kosten: Der Betrieb eines SOC kann sehr kostspielig sein, insbesondere in Bezug auf die fortlaufende Weiterbildung, die technologische Ausstattung und die Personalkosten.
- False-positive Meldungen: Eine Überwachung kann zu einer Flut von Alarmen führen, von denen viele Falschmeldungen sein können, was zu unnötigem Arbeitsaufwand führt.
- Komplexität: Die Verwaltung eines SOC erfordert spezialisiertes technisches Wissen und kann für Unternehmen ohne ausreichendes Wissen überwältigend sein.

Nutzung eines SOC

Beim Einsatz eines SOC sollten Unternehmen folgende Punkte beachten:

- Klare Zielsetzung: Definieren Sie klar, was mit dem SOC erreicht werden soll, einschliesslich spezifischer Sicherheitsziele und -standards.
- Integration: Stellen Sie sicher, dass das SOC vollständig in die bestehende IT-Infrastruktur integriert ist.
- Schulung und Bewusstsein: Regelmässige Schulungen und Sensibilisierungsmassnahmen für Mitarbeitende sind entscheidend, um die Wirksamkeit des SOC zu maximieren.

Intern oder extern?

Die Entscheidung, ob ein SOC intern betrieben oder durch eine externe Firma verwaltet werden soll, hängt von verschiedenen Faktoren ab, einschliesslich Budget, Unternehmensgrösse, Branche, vorhandenem Wissen und spezifischen Sicherheitsanforderungen. Bevor dieser Schritt in Angriff genommen wird, sollte die Basisinfrastruktur auf einem guten Stand sein. Dazu gehören die Sicherheitsorganisation, eine (technische) Übersicht über das Netzwerk und die vorhandenen Systeme (Firewall, Server, Switches, Access Points, Clients, usw.) sowie die vorhandenen Prozesse (Active Directory Konfiguration, Malware-Schutz, Change-Management, Patch-Management, usw). Auch die notwendigen Ressourcen für die Abarbeitung der Meldungen, egal ob intern oder extern, inklusive einem Incident Response Prozess sollten definiert sein.

Hier sind einige Überlegungen, die bei der Entscheidung intern/extern helfen können:

Internes SOC

Vorteile:

- Kontrolle: Ein internes SOC bietet vollständige Kontrolle über die Sicherheitsoperationen, inklusive der (schnellen) Anpassung von Prozessen und Prioritäten an die spezifischen Bedürfnisse des Unternehmens.
- Datenschutz: Sensible Daten bleiben innerhalb des Unternehmens, was bei kritischen Branchen oder bei strengen Datenschutzanforderungen von Vorteil sein kann.
- Teamintegration: Ein internes SOC kann enger mit anderen Abteilungen zusammenarbeiten, was zu einer besseren Kommunikation und schnelleren Reaktionszeiten bei Sicherheitsvorfällen führen kann.

Nachteile:

- Hohe Kosten: Die Einrichtung und der Betrieb eines internen SOC sind oft mit hohen Anfangsinvestitionen und laufenden Kosten verbunden, einschliesslich für Mitarbeitende, Schulungen und Technologie (Hard- und Software).
- Ressourcenintensiv: Der Aufbau und die Aufrechterhaltung eines internen SOC erfordern erhebliche Ressourcen, sowohl finanziell als auch personell.
- Fachwissen: Es kann schwierig sein, qualifiziertes Personal zu finden und zu halten, das die notwendigen Fähigkeiten und Erfahrungen für den Betrieb eines SOC besitzt.

Externes SOC (Managed SOC)

Vorteile:

- Kostenersparnis: Ein Managed SOC kann kosteneffektiver sein, da die Kosten für Infrastruktur, Personal und Technologie auf den Anbieter übertragen werden.
- Sofortige Expertise: Externe SOCs bringen spezialisiertes Wissen und Erfahrung mit, was besonders für Unternehmen vorteilhaft ist, die intern nicht über ausreichende Cybersecurity-Kompetenzen verfügen.
- Skalierbarkeit: Externe Dienstleister können ihre Dienstleistungen leicht an das Wachstum und die sich ändernden Bedürfnisse eines Unternehmens anpassen.

Nachteile:

- Weniger Kontrolle: Die Abhängigkeit von einem externen Anbieter kann zu geringerer Kontrolle über die Sicherheitsoperationen führen.
- Datenschutzbedenken: Die Übertragung von Daten an einen externen Dienstleister kann Bedenken hinsichtlich des Datenschutzes und der Datenhoheit aufwerfen.
- Abhängigkeit: Eine zu starke Abhängigkeit von externen Dienstleistern kann riskant sein, besonders wenn der Dienstleister nicht die erwarteten Leistungen erbringt.

Entscheidungsfindung

Unternehmen sollten die Entscheidung, ob sie ein SOC intern betreiben oder extern verwalten lassen, auf Grundlage einer gründlichen Risiko- und Kosten-Nutzen-Analyse treffen. Hierbei sollten auch langfristige strategische Ziele, wie zum Beispiel die Skalierbarkeit und Flexibilität der Sicherheitsinfrastruktur, berücksichtigt werden. In vielen Fällen kann eine hybride Lösung, bei der bestimmte Aspekte intern und andere durch einen externen Dienstleister betreut werden, eine ausgewogene Option darstellen.

Datenschutz und Informationssicherheit

Ein SOC muss strenge Datenschutz- und Sicherheitsstandards einhalten, um die Integrität und Vertraulichkeit der Daten zu wahren. Zertifizierungen wie ISO 27001 (Informationssicherheit) und ISO 27701 (Datenschutz) sind das absolute Minimum. Es ist wichtig, dass das SOC die geltenden Datenschutzgesetze beachtet (evtl. von mehreren Ländern) und regelmässige Sicherheitsaudits durchführt. Eine offene Transparenz gegenüber den Kunden über die Resultate ist dabei sehr wichtig.

Zusammenfassung und Fazit

Ein SOC ist ein unverzichtbares Instrument für Unternehmen, um ihre Cybersecurity zu stärken. Die Vorteile reichen von verbesserter Überwachung und schneller Reaktionsfähigkeit bis hin zu spezialisiertem Fachwissen. Jedoch sollten die Kosten und die Komplexität des Betriebs nicht unterschätzt werden. Ob intern oder extern betrieben, gilt es genau abzuwägen. Bei der Auswahl eines SOCs sollte sorgfältig vorgegangen werden, um sicherzustellen, dass es den spezifischen Anforderungen des eigenen Unternehmens entspricht. Die Einhaltung und Gewährleistung von Datenschutz und Informationssicherheit ist dabei ein entscheidendes Kriterium.