SOC
AS A SERVICE

sure[secure]

00 INHALT

01 WAS IST DAS SOC?

Das **S**ecurity **O**peration **C**enter ist die zentrale Sicherheitsabteilung eines Unternehmens oder einer Organisation, in der Cybersicherheitsbedrohungen überwacht, erkannt, analysiert und notwendige Maßnahmen zur Behebung dieser getroffen werden – in der Regel 365 Tage im Jahr, rund um die Uhr.

Hier gehen alle sicherheitsrelevanten Meldungen und Notrufe der IT-Infrastruktur eines Unternehmens oder einer Organisation ein – und von hier aus werden alle nötigen Maßnahmen und Schritte eingeleitet, um den jeweiligen Sicherheitsvorfall möglichst schnell beheben zu können.

Das SOC kann als Zusammenspiel von Personen, Prozessen und Technologien für die Überwachung der Sicherheit von IT-Netzwerken betrachtet werden, in dem es darum geht, **proaktiv** Cyberangriffe zu verhindern oder zu erschweren und **reaktiv** Angriffe abzuwehren und den jeweiligen Schaden möglichst gering zu halten.

Unser SOC-Team behandelt also IT-infrastrukturelle Probleme in Echtzeit und sucht gleichzeitig konstant nach Möglichkeiten, den jeweiligen Sicherheitsstatus kontinuierlich zu optimieren.

02 WIESO SOC AS A SERVICE?

Wir leben in einer Welt und Zeit, in der Cyberangriffe zum Alltag gehören. Sie passieren immer häufiger und sind im immer größeren Umfang erfolgreich.

Dies betrifft längst nicht mehr nur große Konzerne. Auch mittelständische und kleine Unternehmen werden immer häufiger Opfer von Hackerangriffen, verschlüsselten Systemen und Daten sowie von erpresserischen Lösegeldforderungen.

Die meisten Angriffe sind finanziell motiviert. Denn so gesehen; lässt sich anhand von Datendiebstahl und Spionage alles zu Geld machen: Passwörter, Geschäftsgeheimnisse, Patente, Betriebs- und Produktionsausfälle sowie Imageschäden.

Die meisten Cybersicherheitsverletzungen werden durch menschliches Versagen verursacht – und nicht selten über das Öffnen eines unbekannten E-Mail-Anhangs.

- **Im Jahr 2021 wurden dem Bundesamt für Sicherheit in der Informationstechnik (BSI) durchschnittlich 394.000 neue Schadprogramm-Varianten pro Tag gemeldet.**
- **Täglich wird in den Medien über neue und immer größere, zielgerichtete Angriffe bzw. Angriffskampagnen berichtet.**
- **Die jährlichen weltweiten Kosten der Cyberkriminalität werden auf geschätzt $ 10.5 Billionen bis 2025. (Cybersecurity Ventures).**

02 WIESO SOC AS A SERVICE?

Viele Unternehmen haben glücklicherweise inzwischen erkannt, dass Sie selbst keine Möglichkeit besitzen, einen Sicherheitsvorfall frühzeitig zu erkennen. Regelmäßig fehlen Informationen, Prozesse und Ressourcen – und so erfolgt die Reaktion auf einen Cyberangriff meist viel zu spät und nicht zielgerichtet.

Angreifende haben es vor allem bei Personen ohne technisches Vorwissen im Bereich IT leicht – denn Ransomware, also Schadsoftware bzw. Erpressungssoftware, lässt sich schnell und einfach an eine E-Mail anhängen und muss für einen erfolgreichen Angriff lediglich von einer anderen Person in der anvisierten Infrastruktur geöffnet werden. Schon kann die Ransomware Daten verschlüsseln und die Angreifenden können ein Lösegeld für die Entschlüsselung verlangen. Ein recht effizienter Weg für Kriminelle, schnell und anonym Unternehmen auszurauben.

Vielen Unternehmen ist daher mittlerweile bewusst, dass sich nicht die Frage stellt, **ob** ein Angriff auf Unternehmen erfolgreich wäre, sondern **wann** ein erfolgreicher Angriff stattfindet.

WER KEIN EIGENES SOC BETREIBEN KANN, ERHÄLT EIN SOC AS A SERVICE.

Durch ein SOC as a Service von suresecure können Angriffe frühzeitig erkannt und der entstehende Schaden minimiert werden. Eine zentrale Grundlage hierfür bildet das SIEM – das Security Information and Event Management – um jegliche Aktivitäten im jeweiligen Netzwerk überwachen zu können und kontextbasierte Protokollereignisse sowie automatisierte Bedrohungsabwehr bereitstellen zu können.

Mithilfe dieses Sicherheitsmanagementsystems werden Meldungen und Logfiles verschiedener Systeme gesammelt, ausgewertet und aufbereitet. So lassen sich verdächtige Ereignisse, Richtlinienverstöße oder gefährliche Trends in Echtzeit erkennen – und darauf reagieren.

03 HERAUSFORDERUNG

Obwohl vielen Unternehmen inzwischen bewusst ist, dass ein Security Operation Center mit einer SIEM Lösung unbedingt notwendig ist, um die IT-Infrastruktur des jeweiligen Unternehmens oder der Organisation gegen Angriffe abzusichern, scheitert das Projekt jedoch oft bereits vor der Konzeptionierung.

In der Regel liegt das an den folgenden Gründen:

- Es existieren unzählige Angriffs-Modelle und Use Cases
- Die notwendigen Log-Quellen können nicht identifiziert werden
- Das Log-Volumen wird falsch eingeschätzt
- Für den Betrieb und die Wartung steht kein geschultes Personal zur Verfügung
- Die Einführung einer SIEM Lösung bedarf eines zu langen Zeitraums
- Fehlendes oder realitätsfernes Sicherheitsbewusstsein
- Die Kosten für die Einrichtung und den Betrieb erscheinen zu hoch

04 SURESECURE KONZEPT

FÜR ALL DIESE PROBLEME HAT DIE SURESECURE LÖSUNGEN ENTWICKELT UND ERMÖGLICHT SOMIT DEN KOSTENEFFIZIENTEN EINSATZ EINES SOC AS A SERVICE FÜR EINE VOLLUMFÄNGLICHE IT-SICHERHEIT.

Bereits bei dem konzeptionellen Entwurf des Service wurde unter Berücksichtigung einer optimalen Skalierung auf vorhandene Industriestandards gesetzt.

Die bereitgestellten Erkennungen orientieren sich an dem MITRE ATT&CK Framework. Dieses Framework beschreibt gängige Techniken, welche durch Angreifende genutzt werden und teilt diese in abstrakte Kategorien ein. Daher kann bereits mit einer einzigen Erkennung eine Vielzahl an Angriffsvarianten identifiziert werden.

Das MITRE ATT&CK Framework beschreibt diese Techniken auch in Form von IoC (Indicators of Compromise) – also in Form digitaler Spuren, die Angreifende nach einem IT-Sicherheitsvorfall hinterlassen.

04 SURESECURE KONZEPT

4.1 Unsere Leistungen

Das SOC as a Service Angebot der suresecure ermöglicht es den Unternehmen und Organisationen aus einem umfangreichen Portfolio genau die Use-Cases umzusetzen, welche benötigt werden. Somit ist es möglich, in einem kleinen Umfang zu starten und das IT-Sicherheitsniveau immer weiter auszubauen.

4.1.1 Network-Monitoring

Firewalls sind gut, sie allein bieten jedoch keinen ausreichenden Schutz für das gesamte Netzwerk. Sobald Angreifende auf die Netzwerkumgebung zugreifen können, steht die Firewall außen vor.

Im suresecure Network-Monitoring werden Sicherheitsvorfälle im Rahmen einer 24/7/365 Überwachung zeitnah entdeckt.

4.1.2 Endpoint Monitoring

In nahezu allen Sicherheitsvorfällen sind Endpoints – also Endgeräte wie Laptops, Tablets, Handys etc. – für Angreifende der Eintrittspunkt in eine IT-Landschaft. Daher ist es unerlässlich in einem SOC umfassende forensisch relevante Logs auf dem Endpoint zu sammeln.

Im suresecure Endpoint Monitoring wird hier unter anderem die Anpassung von Registry-Werten, das Starten von verdächtigen Prozessen oder auch das Ausführen von codierten Powershell Befehlen erhoben, um einen Angriff auf das System zu identifizieren.

04 SURESECURE KONZEPT

4.1.3 Vulnerability Scanning

Im Vulnerability Scanning wird das jeweilige Zielsystem auf Schwachstellen und Sicherheitslücken überprüft, über welche ansonsten beispielsweise Schadcode ausgeführt und somit Systeme ausspioniert, Daten gestohlen, manipuliert oder gelöscht werden könnten.

Ultimatives Ziel unseres suresecure Schwachstellen-Scans ist es also, mögliche Schwachstellen innerhalb eines Systems zu identifizieren.

4.1.4 Authentication Monitoring

Für die sichere Nutzung eines Systems müssen alle User ihre Identität nachweisen können. Die Multifaktor-Authentifizierung über verifizierte Benutzerkennungen und Passwörter wird eine immer beliebtere Methode zum Sichern von Benutzerkonten und Zugängen.

Das System handelt hier nach festgelegten Regeln. Nur wenn sich die Identität des Users 100%ig bestätigen lässt, wird die Nutzung gestattet. Wenn die Anmeldung eines Accounts beispielsweise innerhalb von 10 Sekunden 100-mal fehlschlägt, stellt dies ein auffälliges Ereignis dar.

Unser SOC-Team verfügt hierbei über spezialisiertes und zertifiziertes Know-how!

4.1.5 SIEM

Das SIEM (Security Information and Event Management) sammelt sämtliche Log-Informationen. Es ist in der Lage eine große Menge an Log-Daten unterschiedlichster Systeme einzubinden, auszuwerten und bei Bedrohung selbstständig einen Alarm auszulösen oder mit einer Aktion zu reagieren.

04 SURESECURE KONZEPT

4.2 Log-Volumen

In der Konzeptionierungsphase ist es von essenzieller Bedeutung alle relevanten Log-Quellen zu identifizieren und das mögliche Volumen zu schätzen.

Die suresecure bietet hier einen erheblichen Mehrwert. Zum einen durch die Auswahl der am besten geeigneten Schnittstellen bezogen auf das Quell-System, zum anderen aber auch durch die Reduzierung des Log Volumens.

Durch effiziente Filtertechniken werden nur die sicherheitsrelevanten Logs verarbeitet, dadurch wird die Bandbreite geschont, die Menge der irrelevanten Meldungen minimiert, die Effizienz gesteigert – und nebenbei werden die Kosten minimiert.

4.3 Betrieb und Wartung

Der personelle, finanzielle und zeitliche Aufwand, ein eigenes SOC zu betreiben, ist für die wenigsten Unternehmen tragbar.

Die Bedrohungslage ist immer dynamisch, dementsprechend viel Wartungsaufwand fließt in die kontinuierliche Entwicklung neuer Erkennungsmechanismen mit ein.

Für unser SOC-Team ist die Analyse sowie Beseitigung von Sicherheitsvorfällen Alltag. Unsere Mitarbeitenden werden regelmäßig geschult, um auf jegliche Probleme unserer Partner aus unterschiedlichen Branchen rechtzeitig und richtig reagieren zu können.

Durch unsere enge Zusammenarbeit mit den Herstellern können Updates zeitnah implementiert werden, um die Sicherheitssysteme auf dem aktuellen Stand zu halten.
Ausgerichtet auf Ihren Bedarf, bietet Ihnen unser SOC-Team eine 24/7 Betriebszeit und Rufbereitschaft sowie eine Helpdesk Servicezeit von täglich 7 – 19 Uhr.

05 SURESECURE GMBH

Wir, die suresecure, verstehen uns als Beratungsunternehmen und Reseller von hochspezialisierten IT-Sicherheitslösungen. Besonders wichtig ist uns dabei nicht nur zu vermitteln was wir tun, sondern vor allem auch, wie wir etwas tun.

Durch die Überzeugung, dass der alleinige Einsatz von Sicherheitsprodukten noch keine sichere Umgebung schafft, spielt die Konzeptionierung von Sicherheitsstrategien und Beratung in Fragen der IT-Sicherheit für uns eine tragende Rolle. Wir entwickeln leidenschaftlich Standards zu IT-Sicherheitsprüfungen für den Mittelstand und engagieren uns enthusiastisch im Aufbau von Managed Security Services, Security Operation Center, Professional Security Services, Incident Response Management Konzepten und Cloud Security Lösungen.

Wir haben uns auf die Kernthemen in der IT-Sicherheit spezialisiert und sind darauf ausgelegt, flexibel und zeitnah zu reagieren. Dies ist notwendig, da sich nicht sowohl die Anforderungen an die IT-Sicherheit als auch die Angriffsmuster von außen kontinuierlich verändern.

Also setzen wir auf kurze Entscheidungswege und hoch qualifizierte Mitarbeitende, welche in ihrem Bereich tief in der Materie der IT-Sicherheit verwurzelt sind. Besonders am Herzen liegt uns dabei die Zusammenarbeit mit unseren Partnern. Im Fokus steht die enge und ehrliche Kommunikation untereinander, statt der kurzfristigen Profitmaximierung.

Unsere Mission ist es, die digitale Welt jeden Tag ein Stück sicherer zu machen. Gerne laden wir Sie ein, diese Mission mit uns gemeinsam zu verfolgen.

suresecure GmbH
Dreischeibenhaus 1
40211 Düsseldorf

Telefon: +49 (0) 2156 974 90 60
Telefax: +49 (0) 2156 975 49 78

E-Mail: kontakt@suresecure.de
www.suresecure.de