Beste Reaktion

Security Operations Center intern oder als Managed Service

Die Funktionen eines Security Operation Center sind für die Abwehr von Angriffen auf die Unternehmens-IT unverzichtbar. Doch was tun, wenn im eigenen Unternehmen nicht genug Know-how steckt? Dienstleister können hier unterstützen – auch teilweise.

Bekanntlich stellt sich heutzutage nicht mehr die Frage, ob, sondern nur noch, wann ein Unternehmen Opfer eines Angriffs wird. Daher sind umfassende Vorkehrungen für die Cybersicherheit, auch in Form eines SOC (Security Operations Center), ein Muss, um Angriffe überhaupt erkennen und dann schnell und angemessen reagieren zu können. Die Frage ist, ob das SOC intern betrieben, an einen Dienstleister ausgelagert oder hybrid gemanagt wird.

SOC als eigene Sicherheitsleitstelle

Das SOC stellt eine eigene Organisationseinheit im Unternehmen dar, die meistens außerhalb der IT- oder OT-Abteilungen (Operational Technology) angesiedelt ist. Wichtig ist bei der organisatorischen Zuordnung, die Nähe zur Technik zu wahren und gleichzeitig dem Prinzip der Aufgabentrennung zu folgen. Daher sollte das SOC dem CISO (Chief Information Security Officer) untergeordnet sein. Als Sicherheitsleitstelle werden im SOC alle digitalen Netzwerke, Server, digitalen Geräte und Informationen und auch der Datenfluss überwacht.

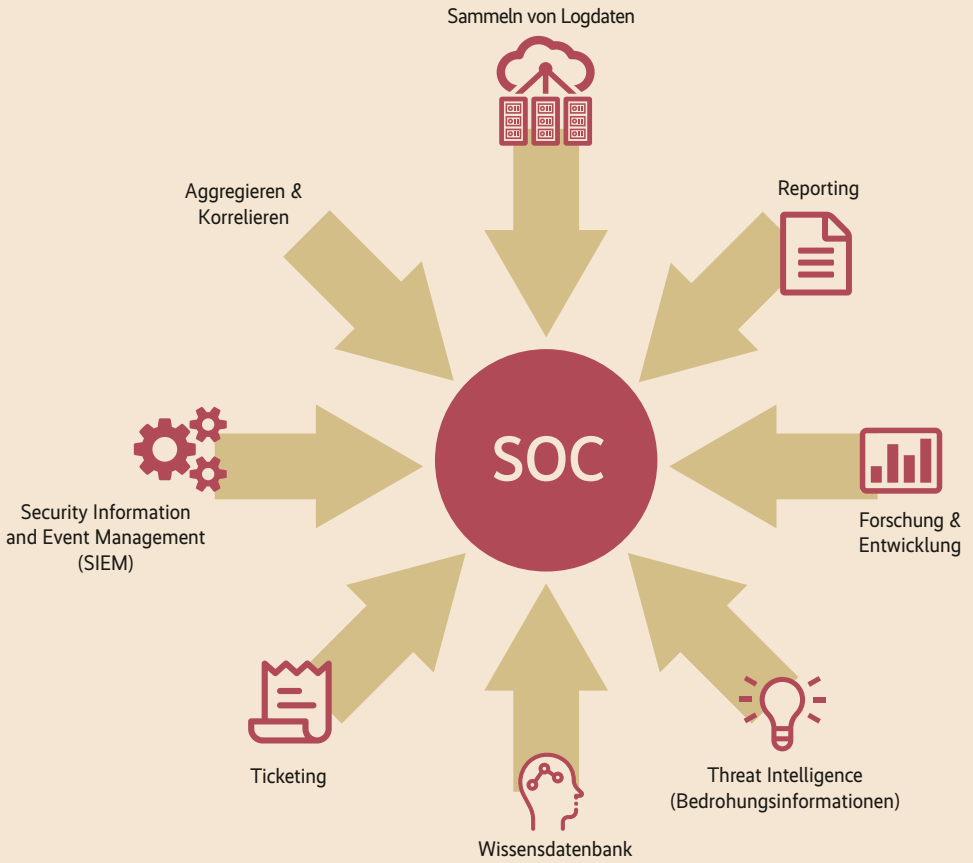
Monitoring, Erkennung und Reaktion (durch ein Computer Emergency Response Team, CERT, oder ein Computer Security Incident Response Team, CSIRT) liegen so vereint unter einem Dach. Weil IT und OT immer stärker zusammenwachsen, sollte dies für beide Welten stattfinden. Bei Auffälligkeiten leitet das SOC Gegenmaßnahmen ein, die die Betriebsteams umsetzen. Das SOC berichtet über seine Aktivitäten an den CISO beziehungsweise das Topmanagement.

Häufig sind SOCs als Kommandostand aufgebaut, an dem Mitarbeiter auf Monitoren die IT- und OT-Systeme überwachen. Sie agieren einerseits proaktiv und suchen mögliche Schwachstellen in den Systemen oder Bedrohungen aus der Außenwelt. Andererseits reagieren sie auf Angriffe und Eindringversuche. Hierfür ist es wichtig, ein sogenanntes „Security Playbook“ zu erstellen, damit es möglich ist, standardisiert und teamübergreifend auf Vorfälle zu reagieren. Die eingesetzten Schutzmaßnahmen sind sowohl technischer Natur, beispielsweise Optimierung von Firewalls, Aufsetzen eines IPS/IDS oder einer Proxy-Infrastruktur, von Identity and Access Management oder die Härtung von Systemen, als auch organisatorischer Art, wie etwa die Anpassung von Nutzerrechten oder Prozessen.

Frühe Erkennung eines Angriffs

Infolge des permanenten Monitorings der Datenflüsse, der Schwachstellen und des Sicherheitsniveaus lassen sich Angriffe frühzeitig erkennen und oft bereits im Vorfeld verhindern. Die Verantwortlichkeiten müssen klar geregelt sein und Maßnahmen schnell und umfassend auf den Weg gebracht werden. Im Krisenfall arbeitet das SOC eng mit dem Krisenstab zusammen.

Mitarbeiter im SOC sind als Spezialisten bestens mit den Eigenheiten der Unternehmens-IT und -OT vertraut, sind aber wegen des Fachkräftemangels oft schwer zu finden. Auch bedeutet das Einrichten eines eigenen SOC viel Aufwand und „Tuning“ der Systeme sowie die Erstellung von Regeln, die Alarme auslösen, auch Use Cases genannt. Struk-



Die vielfältigen Aufgaben eines SOC kann sich ein Unternehmen auch mit dem Dienstleister teilen – nur sinnvoll muss es sein.

turen und Prozesse müssen grundlegend aufgesetzt und Überwachungssysteme angeschafft werden. Der zunehmende Bedarf an KI und Automatisierung zur Erkennung und Behandlung von Sicherheitsvorfällen stellt Unternehmen vor weitere Herausforderungen bei der Rekrutierung geeigneter Mitarbeitender.

SOC als Managed Service – Hilfe von außen

Der Betrieb eines SOC kann auch als Managed Service an einen Dienstleister ausgelagert werden. Externe Anbieter übernehmen dann die Überwachung der Datenflüsse und die Kontrolle des Schutzniveaus. Je nach Vereinbarung kann der Dienstleister auch Anpassungen an den IT- und OT-Systemen vornehmen, wobei hier die Aufgabentrennung äußerst wichtig ist. Zugriffe müssen genau geregelt sein und auf einem Vertrauensverhältnis beruhen.

Das Level des Sourcing kann auch so zugeschnitten sein, dass das Monitoring zwar an einen Dienstleister gegeben, die Behandlung von Sicherheitsvorfällen aber intern durchgeführt wird. So kann der Dienstleister den vollen Leistungsumfang eines SOC erbringen, und gleichzeitig bleibt die „Intelligenz", also das Wissen, im Unternehmen. Bei diesem sogenannten hybriden Ansatz werden feste Incident-Response-Prozesse etabliert, die klar regeln, wie mit Vorfällen umzugehen ist, und die eine Brücke zwischen externem Dienstleister und interner Organisation schlagen.

SOC as Managed Service (SOCaMS) ist besonders für kleinere Unternehmen mit weniger Ressourcen eine gute Alternative, bietet aber auch grundsätzliche Vorteile, da ein Lernen aus der Erfahrung von anderen Unternehmen möglich ist. Nach Bedrohungen, die bei einem Kunden bekannt werden, kann der Dienstleister auch bei anderen Kunden suchen oder Use Cases einfach übernehmen. Beide Ansätze haben Vor- und Nachteile, deshalb wählen die meisten Unternehmen hybride Ansätze.

SOC versus SOCaMS

Für ein SOC im Unternehmen spricht die Tatsache, dass die Mitarbeiter im Idealfall mit der eigenen IT und OT bestmöglich vertraut sind. Das Management hat so für alle Cybersicherheitsfragen klare Ansprechpartner direkt vor Ort. Durch die Dokumentation aller digitalen Vorgänge im SOC können Synergien zu Compliance- und Datenschutzthemen geschaffen werden. Eigene SOCs haben allerdings begrenztere Ressourcen und oft nur das eigene Unternehmen im Blick. Auch ist es, bedingt durch den Fachkräftemangel, schwierig, Mitarbeiter im Unternehmen zu halten.

Externe Dienstleister, die mehrere Kunden absichern, haben hingegen einen besseren 360-Grad-Blick auf aktuelle Bedrohungen und können Probleme von Kunde A auf Kunde B übertragen. Beim SOCaMS können mehr mögliche Bedrohungen und Schwachstellen identifiziert werden, da diese bereits bei anderen Kunden gefunden wurden. Die Aufbauphase erfolgt deutlich schneller, weil Systeme und Erfahrungen bereits vorhanden sind.

Auch können bei SOCaMS weniger kompliziert kurzfristig benötigte zusätzliche Services oder Ressourcen dazugebucht werden. Zudem sind Mitarbeiter eines externen Dienstleisters im Notfall häufig in der Lage, geübter zu reagieren, weil sie durch weitere Kunden mehr Erfahrung mit Notfällen haben.

Des Weiteren kann der nötige 24/7-Dienst bei einem externen Dienstleister, der extra dafür bezahlt wird, oft konstanter realisiert werden. Und schließlich liefert der Dienstleister die Management-Reports meist mit.

Ein SOCaMS hat aber auch Nachteile: Mitarbeiter, die ihre Zeit nur dem eigenen Unternehmen widmen, kennen die eigenen Systeme besser. Auch fällt die Kommunikation, besonders zum Management, durch ein internes Vertrauensverhältnis leichter. In der Praxis empfiehlt sich daher oft eine Kombination beider Ansätze, der hybride Ansatz.

Hybrider Ansatz – Vorteile beider Welten

Für die nötige 24/7-Überwachung im SOC sind mindestens acht Mitarbeiter notwendig. Die Aufgaben im SOC sind verteilt, wobei die grundlegende Überwachung der Datenflüsse meist durch ein automatisiertes Security Information and Event Management (SIEM) durchgeführt wird. Tier-1-Analysten überwachen und bearbeiten, sofern das zügig möglich ist, die Warnmeldungen des SIEM. Tier-2-Analysten bearbeiten und bewerten die SIEM-Meldungen dann, wenn diese mehr Aufwand erfordern.

Zudem gibt es sogenannte Threat Hunter, die gezielt nach Schwachstellen und Bedrohungen suchen, und Konfiguratoren, die basierend auf der Arbeit der Analysten und Threat Hunter Anpassungen an den IT- und OT-Systemen vornehmen lassen. Dazu koordiniert zumeist ein SOC-Manager die Arbeit und vertritt sie gegenüber dem Management oder dem Kunden. Wichtig ist, dass die einzelnen Aufgaben von unterschiedlichen Personen ausgeführt werden. Ein Konfigurator sollte nicht die Sicherheit seiner eigenen Anpassungen testen und die Schwachstellensuche sollte außerhalb des Analyserahmens laufen.

Bei der Kombination beider Ansätze bietet es sich an, die Aufteilung der Aufgaben grob anhand der Trennlinien der Mitarbeitergruppen vorzunehmen. Eigene Analysten können durch externe Threat Hunter oder Threat Reports unterstützt werden, um so den Vorteil einer unvoreingenommenen Außensicht zu nutzen. Das externe SOC spielt dabei seine Expertise beim Erkennen und das interne SOC beim Abarbeiten aus. Die Anpassungen eines internen Konfigurators lassen sich gut durch externe Analysten überwachen.

In der Praxis werden häufig Routinearbeiten wie das Auswerten von Logdateien und die Ereignisprüfung (Tier 1) ausgelagert. Tier 2 erfolgt dann durch interne und externe Kräfte gemeinsam, da hierfür viel internes Wissen nötig ist. Die Umsetzung der Maßnahmen wiederum verbleibt dann komplett intern. Die Schnittstelle zwischen extern und intern liegt daher oft bei Tier 2 und die Trennung erfolgt zwischen Analysten und dem Incident Response Handling.

Um die beste Kombination der Aufgabenteilung zu finden, muss das Unternehmen die eigene Situation richtig bewerten. Welche Ressourcen und welches Know-how sind im Unternehmen selbst vorhanden? Wo ist externe Hilfe erforderlich? Das Zusammenspiel von externen und internen Kräften sollte klar geregelt sein. Kontaktnummern müssen immer zur Hand und das Vorgehen im Ernstfall durch Notfallpläne eindeutig geklärt sein.

Einige Dienstleister aus dem Bereich Incident Response

Unternehmen	Link
Avantec	https://www.avantec.ch/services/incident-response/
Airbus Cyber Security	https://airbus-cyber-security.com/de/produkte-und-services/respond/
Broadcom	https://www.broadcom.com/products/cyber-security/network/atp/network-forensics-security-analytics
Check Point	https://www.checkpoint.com/support-services/threatcloud-incident-response/
Cyber Triage	https://www.cybertriage.com/
DfN-CERT	https://www.dfn-cert.de/leistungen/incidentresponse.html
D3 Security	https://d3security.com/
Fast Detect	https://www.fast-detect.de/it-forensik/leistungen/incident-response/
Gdata	https://www.gdata.de/business/security-services/incident-response
Deloitte	https://www2.deloitte.com/de/de/pages/risk/solutions/cyber-incident-response.html
FireEye	https://www.fireeye.de/mandiant/incident-response.html
Forcepoint	https://www.forcepoint.com/cyber-edu/incident-response
Helmich	https://www.helmich.de/welt-der-it-security/irt-incident-response-team
IBM Resilient	https://www.ibm.com/de-de/marketplace/resilient-soar-platform
Nviso	https://www.nviso.eu/de/service/8/24-stunden-incident-response
One Consult	https://www.oneconsult.com/de/cyber-security-incident-response/
R-tec	https://www.r-tec.net/incident-response-service.html
Schutzwerk	https://www.schutzwerk.com/de/40/Incident-Response-Management.html
Secudor	https://secudor.de/incident-response/
Splunk	https://www.splunk.com/de_de/cyber-security/incident-response.html
SYSS	https://www.syss.de/leistungen/schulung/secu2-incident-response/
touringpoint	https://turingpoint.de/consulting/incident-response-management/
8 Com Cyber Security	https://www.8com.de/incident-response

Best Practices

Oberste Priorität beim Betrieb eines SOC in der Praxis muss sein, dass die Einheit tatsächlich Zugriff auf alle Daten im Unternehmen hat. Laut einer Studie des Ponemon Institute gibt die deutliche Mehrheit von über 500 befragten IT-Sicherheitsverantwortlichen an, dass dieser Zugriff nicht ausreichend umgesetzt ist. Auch müssen SOCs gut in den Rest des Unternehmens eingebunden sein. Der Nutzen des SOC für das Unternehmen muss deutlich sein und entsprechende Unterstützung vom Management kommen.

Die Nähe zur Technik ist wichtig, um keinen Elfenbeinturm zu bauen. Nur wenn ausreichend Transparenz und die Bereitschaft zur Verantwortungsübertragung auf das SOC vorhanden sind, kann ein effizientes Funktionieren des SOC gewährleistet sein. Zudem ist es wichtig, im SOC interoperable Technik einzusetzen. Bei der Aufteilung des SOC-Betriebs auf intern und extern müssen alle Anwendungen gut ineinandergreifen.

Ein weiteres Praxisproblem besteht im Finden und Halten der SOC-Mitarbeiter. SOC-Spezialisten sind sehr begehrt, gleichzeitig sind sie einem hohen Stresslevel ausgesetzt. Vorhandene Mitarbeiter müssen daher gut unterstützt werden und ein Plan für Backups sollte vorhanden sein. Letztlich wird die Arbeit eines SOC durch den regelmäßigen Austausch mit anderen SOCs deutlich erleichtert. Über Organisationsgrenzen hinweg können Schwachstellen und Bedrohungen besser erkannt werden.

Fazit

Durch SOC und SOCaMS wird das Cybersicherheitsniveau eines Unternehmens auf ein neues Level gehoben. Vorfälle und Schwachstellen werden

Einige Anbieter von EDR-Produkten (Endpoint Detection and Response)

Anbieter	Produkt	Link
Bitdefender	Gravity Zone	https://www.bitdefender.de/business/smb-products/advanced-business-security.html
CrowdStrike	Falcon	https://www.crowdstrike.de/endpoint-security-produkte/falcon-plattform/
DriveLock	Endpoint Detection & Response	https://www.drivelock.de/endpoint-detection-response-plattform-mehr-als-nur-protection
Kaspersky	Endpoint Detection and Response	https://www.kaspersky.de/enterprise-security/incident-response
McAfee	MVISION DER	https://www.mcafee.com/enterprise/de-de/products/mvision-edr.html
Microsoft	Defender Advanced Threat Protection	https://www.microsoft.com/de-de/microsoft-365/windows/microsoft-defender-atp
Palo Alto	Cortex XDR	https://www.paloaltonetworks.de/cortex/cortex-xdr
Trend Micro	XDR	https://www.trendmicro.com/de_de/business/products/detection-response/xdr.html
Varonis	Threat Detection & Response	https://www.varonis.com/solutions/threat-detection-response/
VMware	Carbon Black Cloud	https://www.carbonblack.com/resources/vmware-carbon-black-cloud-endpoint-protection-that-adapts-to-your-business/

viel schneller erkannt und der Umgang damit erleichtert. Gänzlich verhindern können sie Hackerangriffe aber nicht, da sie trotz der Schwachstellenanalyse oft nur reaktiv arbeiten. Durch das grundsätzlich asymmetrische Setting zwischen Angreifer und Verteidiger sind Angreifer immer im Vorteil. Eingesetzte KI- oder Machine-Learning-Anwendungen können zwar immer mehr Daten filtern und Angriffe erkennen und abwehren, einen 100-prozentigen Schutz können aber auch sie nicht bieten. Daher gilt es auch hier, angesichts begrenzter Ressourcen abzuwägen, inwiefern eine Anschaffung solcher eigener Tools sinnvoll ist oder ob diese über externe Anbieter genutzt werden. Auch Lösungen in der Cloud bieten hier Vorteile hinsichtlich der Skalierbarkeit und Flexibilität.

Dennoch ist der proaktive Umgang mit dem Thema Cybersicherheit für alle Unternehmen ein Muss. Alle digitalen Abläufe, Systeme und Daten müssen ständig überwacht und angepasst werden. Durch frühzeitige Reaktionen kann man viele Risiken umgehen und abmildern und so viel Geld sparen. SOCs und SOCaMS können dies sehr gut leisten. Letztlich ist es weniger entscheidend, welcher Ansatz oder welche Kombination gewählt wird, sondern dass es auch ordentlich funktioniert, schnell zu implementieren und zu skalieren ist. Hierbei ist es wichtig, sich von dogmatischen Sichten wie „Unsere Daten sind so vertraulich, die behalten wir nur intern und on Premises“ zu lösen und rein objektive Betrachtungen vorzunehmen. (ur@ix.de)

Hans-Wilhelm Dünn
ist Mitbegründer und seit 2018 Präsident des Cyber-Sicherheitsrats Deutschland e. V. Als Fachautor ist er u. a. Mitherausgeber des Standardwerks „Cybersicherheit im Krankenhaus“.