Whitepaper

# Der Aufbau eines modernen SOC

**Risiken, Ressourcen, Realitätscheck**

verizon business

Im Kampf gegen immer neue Cyberbedrohungen fungiert ein Security Operations Center (SOC) als Kommandozentrale, die Warnmeldungen überwacht, akute Vorfälle in nahezu Echtzeit erfasst und alle Abwehrmaßnahmen koordiniert.

Beim Entwurf und Aufbau einer entsprechenden Cybersicherheits-Infrastruktur müssen die Entscheidungsträger im Unternehmen das akzeptable Maß an Risikotoleranz kalkulieren und gegen die verfügbaren Ressourcen und Skills abwägen. Dabei werden in einem ersten Schritt kritische Systeme, tolerierbare Risiken, Complianceanforderungen und Budgetvorgaben ermittelt, bevor schließlich die Wahl eines passenden Bereitstellungsmodells erfolgt – unternehmensintern, hybrid oder vollständig von Dritten verwaltet.

Von diesen bietet ein unternehmenseigenes SOC den Verantwortlichen einerseits die volle Kontrolle über Betriebsprozesse und Sicherheitsmaßnahmen, erfordert jedoch andererseits umfangreiche Vorabinvestitionen. Zudem entstehen bei dieser Variante laufende Kosten für qualifizierte Mitarbeiter und moderne Technologien, die das Unternehmen schützen und Risiken minimieren.

Im Unterschied dazu umfasst ein vollständig verwalteter SOC-Dienst Unterstützung durch erfahrene Analysten, die die globale Bedrohungslage überblicken und kritische Kundensysteme rund um die Uhr überwachen. Auf diese Weise profitieren Unternehmen von bereits vorhandenen Kompetenzen, Technologien und skalierbaren Lösungen – unter Vermeidung des Zeit- und Kostenaufwands, der mit dem Aufbau eines internen Teams verbunden ist.

In dem Bestreben, hier die richtige Balance zu finden, fällt die Wahl vielerorts auf einen hybriden Ansatz, der unternehmenseigenen Mitarbeitern mehr Zeit für komplexere Aufgaben und wichtige Entscheidungsprozesse verschafft, während ein vertrauenswürdiger Partner die grundlegenden Betriebsabläufe übernimmt.

## Ein unternehmensinternes SOC erfordert moderne Technologien, qualifizierte Mitarbeiter und effektive Prozesse

Moderne Technologie ist ein Grundpfeiler jeder effektiven Strategie zur Abwehr von Cyberbedrohungen. Denn erst das reibungslose Zusammenspiel diverser Sicherheitstools wie SIEM-, SOAR- und EDR-Lösungen ermöglicht die Erkennung, Untersuchung und Eindämmung akuter Gefahren.

Hierfür müssen SOCs insbesondere in der Lage sein, Fehlkonfigurationen und API-Schwachstellen sowie nicht genehmigte Zugriffsversuche auf hybride und dynamische Umgebungen zu erfassen, da viele technologische Ökosysteme mittlerweile stark auf Cloud-Services angewiesen sind. Möglich wird dies durch die Implementierung von Zero-Trust-Lösungen, die alle Benutzer, Geräte und Anwendungen verifizieren, bevor sie Zugang zu sensiblen Systemen und Daten erhalten. Mit ihrer Hilfe lassen sich Anomalien in nahezu Echtzeit erkennen und Bedrohungen automatisch eindämmen, bevor spürbare Auswirkungen auftreten.

Zugleich ist zu beobachten, dass immer mehr Angreifer künstliche Intelligenz (KI) verwenden, um ihre Attacken zu automatisieren, die Aufdeckung von Schwachstellen zu beschleunigen, Phishing-Kampagnen zu personalisieren und die Entdeckung von Malware zu erschweren. Um dem entgegenzuwirken und etwa Anomalien schneller zu identifizieren, Warnmeldungen automatisch einzustufen sowie prognostische Analysen zu erstellen, können SOCs ihrerseits KI und maschinelles Lernen einsetzen. Entsprechende Tools reduzieren unter anderem die Zahl der Fehlalarme, sodass Analysten mehr Zeit für wirklich wichtige Aufgaben bleibt.

Daneben müssen sich SOCs flexibel an neue Malwarevarianten und bisher unbekannte Bedrohungen anpassen lassen. Zunehmende Bedeutung erlangen hier Technologien für die kontinuierliche Überwachung, die die Aufdeckung von auf Deepfake-Phishing und KI-generierten Stimmimitationen basierenden Social-Engineering-Angriffen erleichtern.

Moderne SOCs können mit den hier skizzierten Bedrohungstrends Schritt halten, indem sie umfassende Bedrohungsdatenfeeds, KI-gestützte Analysen und Tools für die Verhaltensüberwachung in nahezu Echtzeit implementieren. So lässt sich sicherstellen, dass neue Angriffsmethoden aufgedeckt werden, bevor dem Unternehmen spürbare Schäden entstehen.

## Qualifizierte Fachkräfte: der Faktor Mensch

In der täglichen Praxis übernehmen SOC-Analysten und -Bedrohungsexperten die Erstreaktion auf akute Vorfälle sowie die Einstufung von Warnmeldungen. Dabei werden Fehlalarme aussortiert und komplexere Fälle eskaliert, was üblicherweise tiefergehende Analysen, Maßnahmen zur Bedrohungseindämmung und koordinierte Reaktionsprozesse nach sich zieht.

In Anbetracht dessen müssen SOC-Analysten in der Lage sein, Angriffstaktiken zu rekonstruieren, Anomalien zu erkennen und Aktivitäten zur Umgehung konventioneller Sicherheitsmechanismen aufzudecken.

Diese Skills werden derzeit stark nachgefragt, da auf dem Arbeitsmarkt ein Mangel an Experten für Incident Response, Angriffsmethoden und die Nutzung von Bedrohungsdaten herrscht.

Viele Unternehmen und Institutionen begegnen dieser Herausforderung, indem sie die eigenen IT-Mitarbeiter entsprechend schulen und weiterbilden. Doch das erfordert Zeit – und kann daher das Risiko eines erfolgreichen Cyberangriffs in der Übergangsphase erhöhen.

Erschwerend kommt hinzu, dass auch außerhalb der Geschäftszeiten Ressourcen für die kontinuierliche Sicherheitsüberwachung, die Reaktion auf akute Vorfälle und den Schutz kritischer Systeme vorgehalten werden müssen.

## Effektive Prozesse: IT-Betrieb, Bedrohungserkennung und Playbooks

Grundsätzlich sind effektive Prozesse das Bindeglied zwischen Technologien und Mitarbeitern. So werden beispielsweise im Rahmen der IT-Betriebsprozesse Risikotoleranzen, Grenzen und Zuständigkeiten für Workflows festgelegt. Das hilft den verantwortlichen Sicherheitsteams, alle nötigen Updates und Patches einzuspielen und Warnmeldungen richtlinienkonform zu eskalieren.

Zugleich sollten alle Prozesse rund um die Bedrohungserkennung dynamisch gestaltet werden und kontinuierlich laufen, damit Ihr Unternehmen jederzeit gegen neue Gefahren gewappnet ist. Ohne regelmäßige Prüfung und Pflege der entsprechenden Abläufe steigt das Risiko, dass bekannte und potenzielle Bedrohungen unerkannt bleiben.

Darüber hinaus benötigt ein modernes SOC strukturierte Playbooks, die den zuständigen Mitarbeitern die Untersuchung und Verwaltung der eingehenden Warnmeldungen erleichtern. Dabei erfordert die Verbesserung aller hier genannten Prozesse dedizierte Ressourcen, die eine effektive Abwehr und Eindämmung relevanter Bedrohungen und Schwachstellen gewährleisten.

## Outsourcing als Alternative

Wenn ein vertrauenswürdiger Partner den SOC-Betrieb übernimmt, kann dies die anfallenden Kosten senken, Sicherheitsprozesse straffen und im Ernstfall die Hinzuziehung führender Experten erleichtern. Statt große interne Teams zu managen, profitieren Unternehmen so von kontinuierlicher Überwachung, umfassender Automatisierung und der Bereitstellung von Bedrohungsdaten durch einen kompetenten Anbieter – der dann als integriertes Sicherheitsteam statt als passiver Dienstleister fungiert. Dadurch lassen sich möglicherweise die Folgen eines Cyberangriffs für das betroffene Unternehmen und seine Kunden minimieren.

Allerdings ist in diesem Zusammenhang zu beachten, dass nicht alle SOC-Anbieter über dieselben Fähigkeiten verfügen. Managed Security Services Providers (MSSPs) sind auf die Überwachung von Protokolldaten sowie Schwachstellenscans und Compliance-basierte Sicherheit spezialisiert. Diese Anbieter helfen bei Berichterstellung, Monitoring und der Umsetzung regulatorischer Vorgaben, sind jedoch üblicherweise nicht in der Lage, die Bedrohungssuche und -abwehr in nahezu Echtzeit durch aktive Maßnahmen zu unterstützen.

Dagegen schließen Anbieter für Managed Detection and Response (MDR) die personellen Lücken von Unternehmen ohne eigene Incident-Response-Teams.

## Hybride, gemeinsam verwaltete SOCs

Hybride, gemeinsam verwaltete SOCs bieten Unternehmen die Möglichkeit, die Kontrolle über kritische Sicherheitsprozesse zu behalten und Monitoring, Datenüberwachung und Automatisierung an einen Drittanbieter zu übertragen. Das steigert die Flexibilität, weil risikobehaftete Prozesse weiterhin unternehmensintern ablaufen, während entsprechend spezialisierte Experten die Erkennung und Abwehr akuter Bedrohungen übernehmen.

Indessen sollten bei der Auswahl eines passenden SOC-Anbieters unbedingt Kriterien wie dessen Branchen- und Compliance-Expertise sowie Reaktionszeiten und KI-gestützte Threat Intelligence berücksichtigt werden. Der richtige Partner passt sich an die Sicherheitsanforderungen des Kundenunternehmens an, sorgt für eine reibungslose Zusammenarbeit mit internen Teams und deckt mit seinem Leistungsangebot alle gewünschten Aspekte der Bedrohungserkennung und -abwehr in nahezu Echtzeit ab.

Deshalb sollten interessierte Unternehmen vor einem Vertragsschluss sorgfältig prüfen, ob ihr potenzieller SOC-Partner das gewünschte Maß an Flexibilität und Transparenz bietet und bestehende Prozesse und Technologien in einem ebenso effektiven wie anpassungsfähigen hybriden SOC zusammenführt.

## Wichtige Aspekte: Kosten, Expertise und Risiko

Ein internes, speziell für die Strategien und betrieblichen Anforderungen sowie das Risikoprofil und die regulatorischen Pflichten des eigenen Unternehmens konzipiertes SOC bietet den Verantwortlichen ein Höchstmaß an Kontrolle über Sicherheitsprozesse und Daten.

Doch zugleich erfordern Betrieb und Pflege eines internen SOC fortlaufende Investitionen in Technologien und Personalentwicklung. Unternehmen, die sich für diesen Weg entscheiden, müssen zum einen ihren Bestand an modernen Sicherheitstools auf dem aktuellen Stand halten, zum anderen aufwendige personelle Maßnahmen ergreifen, um qualifizierte Mitarbeiter auf einem von hartem Wettbewerb geprägten Arbeitsmarkt zu rekrutieren, fortzubilden und langfristig zu binden.

Die Zusammenarbeit mit einem SOC-Partner, der ein breites Spektrum an anpassbaren Diensten rund um das Vorfallsmanagement bereitstellt, stellt eine vielversprechende Alternative hierzu dar. Das gilt insbesondere dann, wenn Team und Lösungen des Partners als kontinuierlich verfügbare Ressourcen in die IT- und Sicherheitsprozesse integriert werden können und mit der Infrastruktur und Unternehmenskultur des Kunden kompatibel sind.

Ein internes Team kennt die eigene Infrastruktur, die ihr drohenden Risiken und die Unternehmensziele besser als jeder andere, doch der Aufbau eines solchen Teams, die Aus- und kontinuierliche Weiterbildung seiner Mitarbeiter und nicht zuletzt ihre Bindung an das Unternehmen erweisen sich oft als kompliziert, zeitaufwendig und teuer. Zudem können in der Übergangsphase Sicherheitslücken entstehen, die das Cyberrisiko erhöhen. Andererseits bietet die Outsourcing-Variante ein höheres Maß an Skalierbarkeit und spezialisierter Expertise, wenngleich sie möglicherweise das unternehmensspezifische Wissen und die Präsenz eines internen Teams vermissen lässt. Daher umfasst die Liste der bei der Wahl zwischen internen, externen und hybriden SOC-Ansätzen relevanten Kriterien unter anderem Faktoren wie die Arbeitskultur und betriebliche Flexibilität des Unternehmens sowie anbieterseitige Erfahrungen mit der Nutzung vorhandener Sicherheitstools und der Umsetzung einschlägiger Compliancevorgaben.

Letztlich sollte das gewählte SOC sowohl für die jeweils geltenden gesetzlichen Bestimmungen als auch für branchenspezifische Standards ausgelegt sein. Diese Forderung erstreckt sich auf alle regulatorischen Vorgaben, die das jeweilige Unternehmen zu kontinuierlichem Monitoring, regelmäßigen Audits und proaktiver Governance im Bereich Sicherheit verpflichten.

Nicht zuletzt deshalb ist der Aufbau eines SOC kein einmaliges Projekt, sondern ein dynamisch fortlaufender Prozess, der kontinuierliche Überwachung, Pflege und Anpassung erfordert. Letzteres gilt umso mehr, als Unternehmen derzeit mit einer sich rasch wandelnden Bedrohungslandschaft, veränderten geschäftlichen Anforderungen und einem gesteigerten Kostendruck konfrontiert sind.

Unter diesen Umständen kann selbst das modernste SOC schnell veralten und seine Effektivität verlieren – wenn fortgesetzte Investitionen in innovative Technologien, kompetente Expertenunterstützung und die neuesten Sicherheitsstrategien ausbleiben.

### Mehr zum Thema

Kontaktieren Sie Ihren Verizon Business Account Representative, wenn Sie mehr über die Wahl eines passenden SOC-Ansatzes erfahren möchten. Außerdem erreichen Sie uns per E-Mail an: info@verizonenterprise.com. Oder über unsere Website: www.verizon.com/business/de-de/contact-us