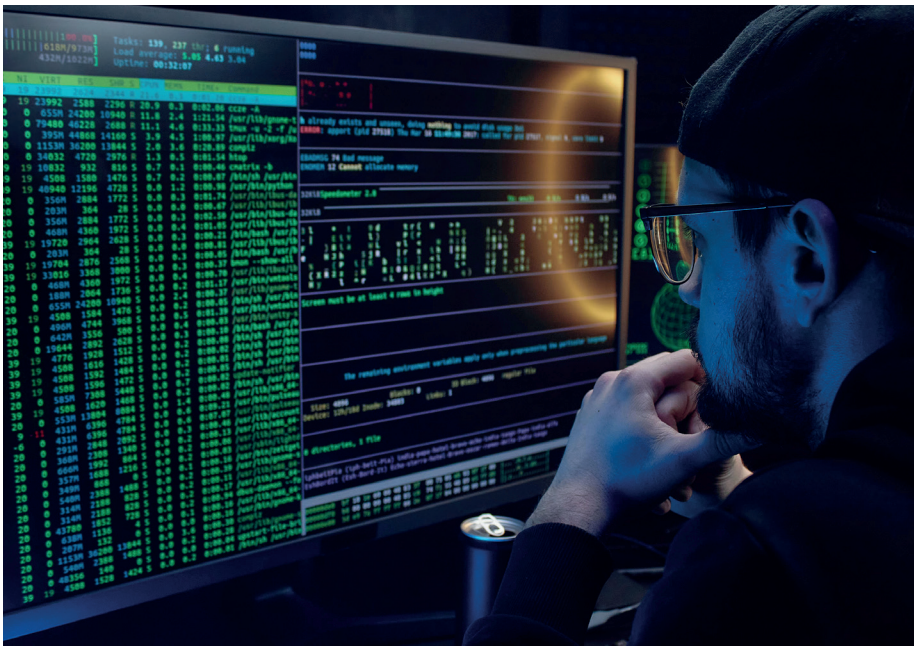
Security Operations Center als Managed Service

Wandel, Nutzen und Entscheidungsfaktoren aus Sicht der Unternehmen

Bernhard Reimann

In den letzten fünf Jahren hat sich die Bedeutung von Security Operations Centern (SOC) als Managed Services deutlich verschoben – vom optionalen Sicherheitsbaustein hin zur geschäftskritischen Komponente im IT-Betrieb vieler Unternehmen. Verantwortlich dafür sind vor allem die zunehmende Bedrohungslage, der Fachkräftemangel in der IT-, OT- und Cybersicherheit sowie die wachsende Komplexität moderner IT-Landschaften. Syserso Networks stellt durch jahrzehntelange Erfahrung mit seinem Network Operations Center (NOC) und dem Security Operations Center (SOC) den Schutz von IT- und OT-Systemen sicher.



Bei Verdacht auf einen Incident wird der Fall an das SOC Level 2 eskaliert, die tiefergehende Analysen, Maßnahmen zur Eindämmung und Abwehrmaßnahmen empfehlen oder selbstständig vornehmen (Foto: Mikhail Nilov, Pexels)

Angriffe auf IT-Strukturen werden immer komplexer und zielgerichteter. Entsprechend gewinnen Security Operations Center (SOC) als Managed Service an Bedeutung. Für den Betrieb ist jedoch weit mehr erforderlich als nur technisches Know-how und eine gute Infrastruktur. Denn selbst die beste Technik nützt wenig, wenn sie nur rudimentär und nicht vollumfänglich zum Einsatz kommt.

Komplexe Dienstleistung

Der Betrieb eines SOC zur Betreuung von Kundennetzen mit kritischer Infrastruktur ist eine komplexe Dienstleistung, bei der Sicherheitsüberwachung, Ereignisanalyse, proaktive Bedrohungserkennung und Reaktion auf Sicherheitsvorfälle zentralisiert und bedarfsgerecht skalierbar angeboten werden. „Für Unternehmen, die keine eigenen Ressourcen für eine echte 24/7-Überwachung und Incident Response bereitstellen können, bieten Managed SOCs eine flexibel erweiterbare und individuell anpassbare Lösung zur Sicherstellung der Cyber-Resilienz“, so Dirk Lukas, Head of Security Pre-Sales & Consulting bei Syserso Networks.

Die Grundlage bildet eine zentrale, leistungsfähige Analyseplattform, in der Regel ein SIEM- (Security Information and Event Management) oder Network-Monitoring-System. Sie fungiert als zentraler Knotenpunkt zur Korrelation und Analyse sicherheitsrelevanter Log-Informationen und Netzwerkkommunikation. Dieses System muss Daten aus unterschiedlichsten Quellen – wie Firewalls, Intrusion Detection/Prevention Systemen (IDS/IPS), Endpoint Detection and Response (EDR), Network Detection and Response (NDR), Cloud-Diensten sowie dem Netzwerkverkehr – in Echtzeit analysieren.

Bernhard Reimann ist Chefredakteur der NET

Technisch gesehen werden alle sicherheitsrelevanten Logs und Events von Firewalls, IDS/IPS, Windows/Linux-Servern, Netzwerkkomponenten, Authentifizierungssystemen, Cloud-Diensten und Endpoints über Syslog, Agenten oder APIs an das SIEM übergeben. Dort werden die Daten normalisiert, mit Zeitstempeln versehen, in strukturierte Form gebracht und in einem zentralen Data Lake oder Log-Archiv gespeichert. Parallel dazu greifen Korrelationsregeln, die Muster erkennen, Schwellenwerte prüfen oder Signaturen abgleichen. „Solche Ereignisse können beispielsweise das gleichzeitige Auftreten fehlgeschlagener Logins aus verschiedenen Regionen oder der Zugriff auf sensible Dateien außerhalb der Geschäftszeiten sein“, führt Lukas aus. Mit Hilfe von Network Detection and Response (NDR) werden zudem ungewöhnliche Kommunikationsmuster, neue oder veränderte Endgeräte sowie abweichendes Verhalten analysiert und für eine eventuell notwendige forensische Auswertung gesichert. Die dadurch erlangte Transparenz ermöglicht es, etwa den Einsatz unsicherer Cipher-Suiten oder veralteter Protokolle zu identifizieren und so die Resilienz der IT-Infrastruktur signifikant zu erhöhen.

Sicherheit rund um die Uhr

Neben der technischen Infrastruktur ist qualifiziertes Fachpersonal der entscheidende Erfolgsfaktor im SOC-Betrieb. Analysten, Threat Hunter, Incident Responder und Forensiker müssen rund um die Uhr einsatzbereit sein. Diese Rollen erfordern nicht nur tiefgehendes Spezialwissen, sondern auch kontinuierliche Weiterbildung und die Fähigkeit, Bedrohungen fundiert zu erkennen, zu bewerten und einzuordnen. Gleichzeitig müssen Prozesse und Playbooks klar definiert sein. Dabei spielt die Integration von SOAR-Systemen (Security Orchestration, Automation and Response) eine zentrale Rolle. Sie steigern die Effizienz und Reaktionsgeschwindigkeit signifikant, indem sie Sicherheitsmaßnahmen automatisieren und koordinieren. Ein SOAR orchestriert Playbooks: Wird etwa eine verdächtige Datei oder ein verdächtiges Verhalten erkannt, kann automatisch ein Endpoint isoliert, der Account deaktiviert, ein Ticket erstellt, ein Analyst informiert und ein Mail-Gateway blockiert werden. Moderne Plattformen wie Splunk oder Microsoft Sentinel bieten dafür Low-Code-Automatisierungen, die klassische Redaktionszeiten von Stunden auf wenige Minuten reduzieren können.

Hohe Complianceanforderungen

Ein weiteres zentrales Element ist die Einhaltung rechtlicher und regulatorischer Vorgaben. Insbesondere in der EU ist die DSGVO zu berücksichtigen, während branchenspezifische Standards wie ISO 27001, BSI IT-Grundschutz oder NIS2 zusätzliche Anforderungen definieren. Der Anbieter eines Managed SOC muss nicht nur sicherstellen, dass Daten sicher und datenschutzkonform verarbeitet werden, sondern auch vertraglich und technisch garantieren, dass Kundendaten nur autorisierten Personen zugänglich sind. Verträge, Service Level Agreements (SLAs), lückenlose Dokumentation sowie die Nachvollziehbarkeit aller Maßnahmen sind aus Compliance-Sicht zwingend erforderlich. „Die regulatorischen Anforderungen erhöhen den Druck auf Unternehmen, ihre Detektions- und Reaktionsfähigkeit nachweislich zu verbessern. Ein Managed SOC kann diese Lücke effizient schließen“, betont Dirk Lukas.

„Syserso Networks betreibt ein effektives Vorfallmanagement zur Erkennung, Meldung und Bewältigung von Sicherheitsvorfällen“, ergänzt Lukas. „Sicherheitskritische Vorfälle können in diesem Zusammenhang an zuständige Behörden wie das Bundesamt für Sicherheit in der Informationstechnik (BSI) gemeldet werden. Darüber hinaus erfolgt die Zusammenarbeit mit anderen Betreibern kritischer Infrastrukturen und den zuständigen nationalen Behörden, um Informationen über Bedrohungen und Vorfälle auszutauschen.“

Im SOC selbst arbeiten Analysten in verschiedenen Eskalationsstufen – den sogenannten SOC Levels (L1, L2 und Incident Response). Level-1-Analysten erhalten sicherheitsrelevante Alerts über ein mandantenspezifisches Security Dashboard, das Events anhand von Risikobewertungen priorisiert. Sie führen eine erste Sichtung durch, analysieren Kontextdaten, Benutzerverhalten (UEBA – User and Entity Behavior Analytics), Häufigkeiten sowie historische Zusammenhänge. Bei Verdacht auf einen Incident wird der Fall an Level 2 eskaliert. Dort erfolgen tiefergehende Analysen sowie Empfehlungen für Eindämmungs- und Abwehrmaßnahmen – oder deren unmittelbare Umsetzung.

Wird ein kritischer Sicherheitsvorfall bestätigt, kommt das Incident Response Team (IRT) zum Einsatz. Es übernimmt auf Basis organisatorischer und technischer Expertise die Koordination und Umsetzung aller notwendigen Maßnahmen zur Notfall- und Krisenbewältigung. Die Leistungen bestehen aus der Einsatzkoordination, Sachstandanalyse und Forensik, Risikoabwehr, Empfehlung von Gegenmaßnahmen, Vorfalldokumentation sowie der Unterstützung des Kunden bei der Reaktion auf den Vorfall.

Ein Managed SOC erfordert dafür eine hochverfügbare und verteilte Architektur. Entweder wird eine Multi-Region-Cloudinfrastruktur bereitgestellt – oder alternativ auf kundeneigene Rechenzentren zurückgegriffen, die mit Load Balancing, Redundanz und Disaster-Recovery-Strategien ausgestattet sind. In diesem Fall muss der Kunde sowohl die benötigte Hardware als auch die vollständige Betriebssoftware zur Verfügung stellen. Edge-Komponenten wie Log Forwarder oder Sensoren auf

Kundenseite übernehmen den sicheren Transport sensibler Daten – typischerweise über dedizierte Site-to-Site-VPNs. Ein durchgängiger Zero-Trust-Ansatz stellt dabei sicher, dass jede Kommunikation authentifiziert, autorisiert und verschlüsselt erfolgt.

Mandantenfähigkeit

Eine zentrale Herausforderung beim Betrieb eines SOC als Managed Service ist die Mandantenfähigkeit und der gleichzeitige Schutz sensibler Kundendaten. Multimandanten-Systeme bringen eine inhärente Komplexität mit sich, die bei unzureichender Segmentierung oder fehlerhafter Rechteverwaltung zu schwerwiegenden Datenschutzverstößen führen kann. Auch die Kommunikation mit Kunden erfordert besondere Sorgfalt – insbesondere, wenn Sicherheitsvorfälle zeitnah kommuniziert, abgestimmt und bearbeitet werden müssen, während gleichzeitig individuelle Kundenprozesse zu berücksichtigen sind. Ein weiteres zentrales Element ist ein skalierbares und leistungsfähiges Log-Management, das große Datenmengen effizient verarbeitet. Werden mehrere Kunden betreut, muss sichergestellt sein, dass Daten strikt getrennt, Zugriffsrechte sauber definiert und sämtliche Sicherheits- und Datenschutzanforderungen zuverlässig eingehalten werden. Nicht zu unterschätzen ist auch das Thema False Positives: Ein überempfindlich konfiguriertes SIEM- oder NDR-System kann eine wahre Flut an Meldungen erzeugen, wenn es nicht optimal abgestimmt ist. SOC-Analysten verbringen dann wertvolle Zeit mit der Bewertung harmloser Aktivitäten und riskieren dabei, echte Sicherheitsvorfälle zu übersehen. Der Betrieb eines Managed SOC erfordert deshalb ein sorgfältiges Baselining, kontinuierliches Feintuning, intelligente Regelwerke sowie eine laufende Automatisierung/Validierung – etwa durch Machine Learning und erklärbare KI. Nur so lassen sich tatsächliche Bedrohungen zuverlässig aus dem Grundrauschen herausfiltern. Ergänzend dazu ist beim Einsatz von IDS-Systemen die Nutzung permanent aktualisierter Signaturen unerlässlich, um neue Angriffsvektoren zeitnah detektieren zu können.

Dirk Lukas

Die regulatorischen Anforderungen erhöhen den Druck auf Unternehmen, ihre Detektions- und Reaktionsfähigkeit nachweislich zu verbessern. Ein Managed SOC kann diese Lücke effizient schließen

Fazit

Ein Managed SOC bietet signifikante Vorteile für Unternehmen. Sie erhalten Zugang zu hochspezialisierten Sicherheitsdiensten, ohne selbst in kostenintensive Infrastruktur, Personal und Know-how investieren zu müssen. Besonders kleine und mittelständische Unternehmen profitieren davon, da sie auf diese Weise ein professionelles Sicherheitsniveau erreichen, das intern kaum realisierbar wäre. Durch den 24/7-Betrieb und das konsolidierte Wissen aus verschiedenen Kundenumgebungen profitieren sie zudem von Frühwarnsystemen und Kollektiverfahrung. Für IT- und OT-Sicherheitsteams bedeutet die Auslagerung an ein Managed SOC vor allem eines: Fokus. Die externe Einheit übernimmt Routineaufgaben wie Log-Analyse, SIEM-Management, Alert-Triage und Eskalation - intern bleibt Raum für strategische Aufgaben wie Risikobewertung und Maßnahmenentscheidung. Die technische Infrastruktur – von Threat Intelligence über Automatisierung bis hin zur Forensik – wird vom Dienstleister bereitgestellt, gewartet und aktuell gehalten.

Moderne SOC-Anbieter liefern längst mehr als nur Tickets: Sie bringen Playbooks, automatisierte Workflows, orchestrierte Response-Mechanismen und aussagekräftiges Reporting mit, die sich in bestehende Prozesse integrieren lassen und Nachweise für Audits liefern. Auch die Anbindung an bestehende EDR/XDR-Systeme sowie Cloud-/Netzwerk-Monitoring sind heute Standard.

Das passende Managed SOC

Die Auswahl eines geeigneten Managed Security Operations Centers sollte sorgfältig und anhand klar definierter Kriterien erfolgen:

- Reaktionszeit und Servicequalität: Wie schnell werden sicherheitsrelevante Vorfälle erkannt, bewertet und gemeldet?
- Transparenz und Kontrolle: Erhalten interne Teams ausreichend Einblick in Analysen, Prozesse und Kennzahlen? Ist das Reporting nachvollziehbar, detailliert und revisionssicher?
- Integration in bestehende Prozesse: Lässt sich das SOC nahtlos in vorhandene IT- und OT-Prozesse integrieren? Werden Schnittstellen zu bestehenden Plattformen (z. B. DER, SIEM, CMDB) unterstützt?
- Datenschutz und Compliance: Wo und wie werden Daten verarbeitet? Entspricht der Anbieter relevanten gesetzlichen und branchenspezifischen Vorgaben (z. B. DSGVO, ISO 27001, NIS2)?
- Skalierbarkeit und Zukunftssicherheit: Kann der Service mit dem Unternehmen wachsen? Ist die Lösung flexibel genug, um zukünftige Anforderungen und technische Entwicklungen abzubilden?

www.syserso.com