Managed Security Services reichen viel weiter als Managed Services

Cyber-Angriffe werden immer komplexer. Um angemessen auf diese Gefahr zu reagieren, setzen Unternehmen auf Managed Security Services. Jedoch muss MSS mehr umfassen als nur den Betrieb der Sicherheitsinfrastruktur.

Managed Security Services (MSS) finden sich zumindest dem Namen nach im Portfolio bei fast allen Dienstleistern für IT-Sicherheit oder Informationssicherheit – von lokalen oder regionalen Systemhäusern über globale Netzwerkausrüster oder Telekommunikationsunternehmen bis zu Beratungsfirmen und natürlich Outsourcing-Anbietern. Die Nachfrage nach Managed Security Services ist hoch, auf dem Markt ist ein vielfältiges Angebot verfügbar.

Bei der Begriffsdefinition von MSS hapert es allerdings vielfach noch. So findet sich oft die Meinung, dass es einzig und allein um den Betrieb von IT-Security-Infrastrukturen geht. Sie ist falsch: der reine Sicherheitsbetrieb ist lediglich eine einzelne Komponente von umfassenden Managed Security Services.

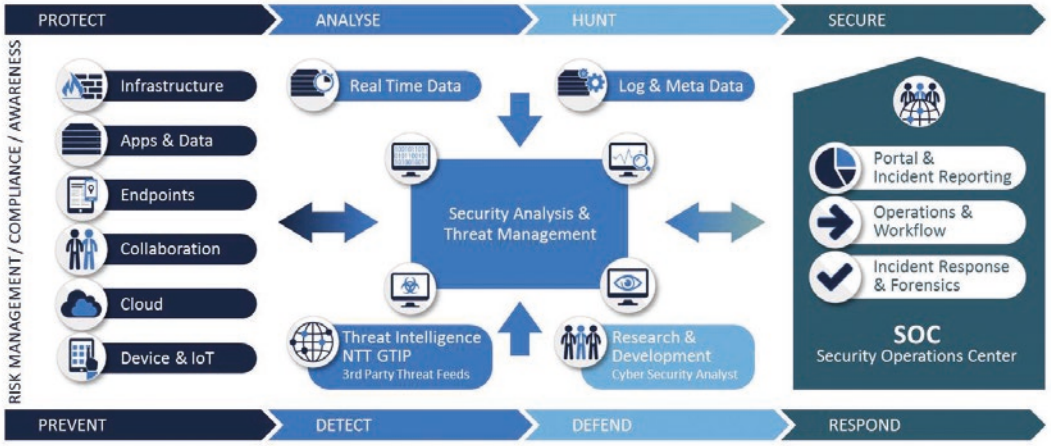
Die Fehleinschätzung, der Fokus von Managed Security Services liege auf operativen Leistungen, ist sowohl auf Anbieterseite als auch bei auslagernden Unternehmen verbreitet. Managed Security Services werden also mit Managed Services gleichgesetzt und ausschliesslich auf Betriebsthemen reduziert. Natürlich müssen Anbieter im MSS-Umfeld auch wiederkehrende Betriebsleistungen im Infrastruktur-Management erbringen. Zu den Mindestanforderungen gehören:

- Betriebsverantwortung durch den Dienstleister
- Präventive Wartung (Patch und Release Management sowie Health und Availability Monitoring)
- Change Management
- Support (Incident Management)
- Out-of-Band Management
- Service (Delivery) Management.

Diese Leistungen müssen rund um die Uhr an allen Tagen im Jahr zur Verfügung stehen und einem Service Level Agreement mit entsprechenden Messkriterien und Leistungskennzahlen (Key Performance Indicators – KPIs) unterliegen. Sie sollten nahtlos in weitere Sicherheitsleistungen des Anbieters integriert werden können.

Managed Security Services reichen viel weiter

Solche Managed Services sind aber bei Weitem noch keine Managed Security Services, sondern lediglich ein Bestandteil. Das wichtigste Unterscheidungskriterium ist, dass es bei MSS primär um einen Security Service geht und weniger um einen Managed Service. Bei MSS stehen ganzheitliche Lösungskonzepte im Mittelpunkt, die den gesamten End-to-End-Sicherheitsservice abdecken. Das heisst, bei MSS-Projekten stellen das Infrastruktur- und Technologie-Management oftmals lediglich die Basis für höherwertige Services dar.



Essenzielle Bestandteile des Security-Device-Managements im Überblick. (Quelle: NTT Security)

Ganz allgemein bedeutet das auch, dass es sich nicht um Outtasking im klassischen Sinn handelt, also die Auslagerung einzelner Betriebsaktivitäten, sondern viel umfassender um die Auslagerung von Risiken, das heisst letztlich auch um ein durchgängiges Risikomanagement.

MSS übernehmen ganz allgemein formuliert die Verantwortung für die Sicherheit von Infrastrukturen und Anwendungen durch:

- Bereitstellung (logistisch und kommerziell);
- Verarbeitung (operativ und prozessual);
- Verwaltung (organisatorisch und strategisch).

Ziel und Zweck von Managed Security Services sind die Herstellung von Sicherheit oder das Erreichen beziehungsweise Erhöhen eines Sicherheitsniveaus.

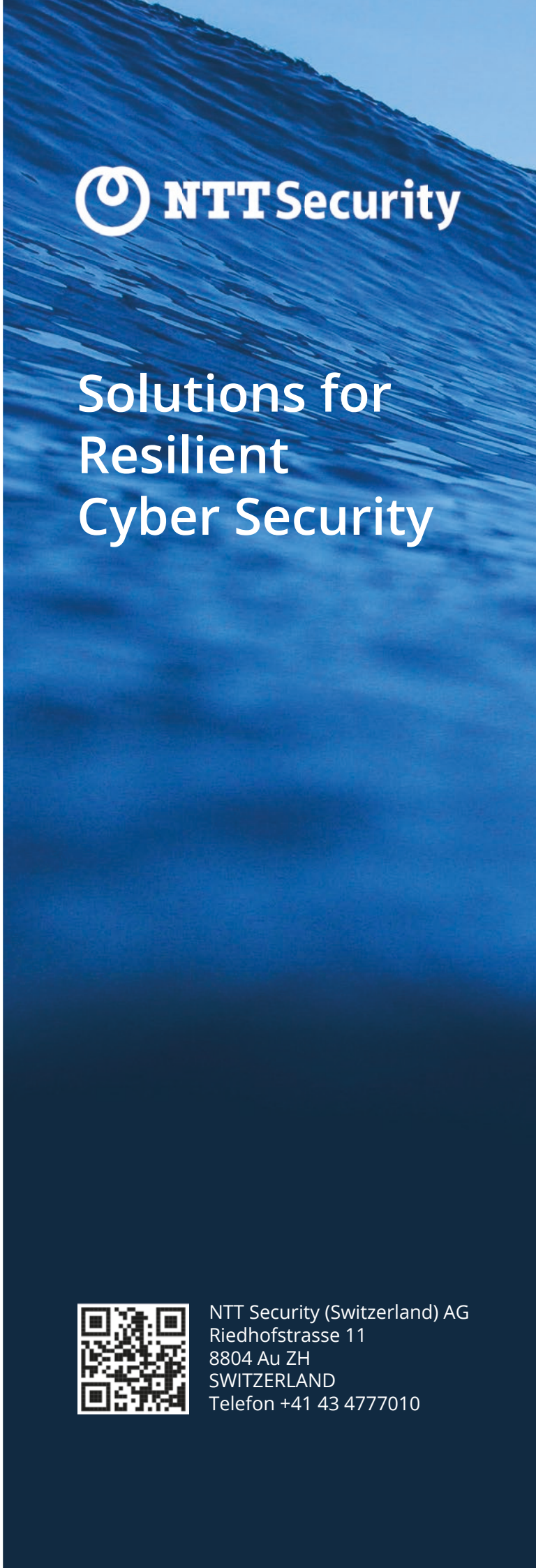
Ganzheitliche Sichtweise notwendig

Dass Managed Services allein keine Sicherheit bringen, zeigen schon zahlreiche, weiterhin erfolgreiche Cyber-Angriffe auf Unternehmen – auch wenn sie auf aktuellem Release- und Patch-Stand sind. Bei der Auswahl eines MSS-Providers sollte ein Unternehmen darauf achten, dass dieser unter technischen und fachlichen Aspekten über ein umfassendes Angebot verfügt, das den aktuellen Stand der Technik widerspiegelt. Sein Leistungsspektrum muss vor allem der Tatsache Rechnung tragen, dass herkömmliche Sicherheitsmodelle, die auf einem Perimeter-Schutz mit Firewalls, VPN-Systemen, Anti-Viren-Software, Malware-Filter oder dynamischen Sandboxing-Lösungen basieren, zwar erforderlich, aber alleine unzureichend sind.

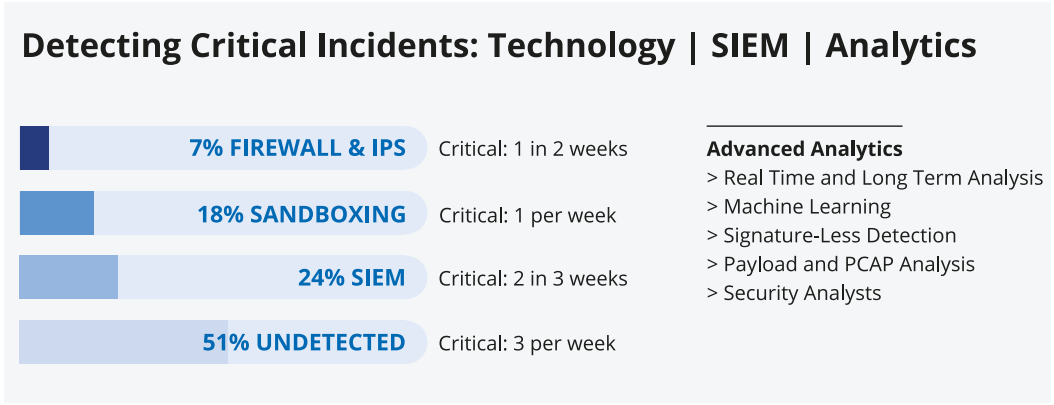
Vielfach wird auch die Meinung vertreten, dass die Einführung und Nutzung eines Security-Information-and-Event-Management (SIEM)-Systems eine hohe Sicherheit garantiert. Dazu ist anzumerken, dass SIEM eine Lösung darstellt, die auf Use Cases und Signaturen basiert. Ein traditionelles SIEM kann somit keinen Schutz vor unbekannten Attacken bieten.

Kritische und unerkannte Attaken als Sicherheitsrisiko einstufen

Analysen von NTT Security haben beispielsweise ergeben, dass die Detektionsrate von kritischen Sicherheitsvorfällen bei Firewalls und Intrusion-Prevention-Systemen bei 7 Prozent, bei Sandboxing-Lösungen bei 18 Prozent und bei SIEM-Systemen bei 24 Prozent liegt. Dieses Ergebnis ist nicht zufriedenstellend. Der Begriff Sicherheit sollte in der IT sehr weit gefasst werden – und zwar als ein Zustand, der frei ist von nicht vertretbaren Risi-



NTT Security (Switzerland) AG
Riedhofstrasse 11
8804 Au ZH
SWITZERLAND
Telefon +41 43 4777010



Herkömmliche Sicherheitsverfahren und -technologien sind für das Aufspüren kritischer Incidents unzureichend. (Quelle: NTT Security)

ken. Und als nicht vertretbare Risiken sollten auch kritische und unbekannte Attacken eingestuft werden.

Fortschrittliche Analysetechnologien bieten hohe Sicherheit

Der Anbieter eines Managed Security Services muss folglich, abgesehen von Basisleistungen wie Betrieb oder Nutzung traditioneller Sicherheitslösungen, weitere Leistungen bereitstellen, die als Advanced Security Analytics zu klassifizieren sind. Dazu zählen Echtzeit- und Langzeitanalysen, der Einsatz von Lösungen, die auf künstlicher Intelligenz und maschinellem Lernen basieren oder signaturlose Detektionsverfahren.

Darüber hinaus sollte das Leistungsspektrum und Serviceangebot eines MSS-Providers unter anderem Folgendes umfassen:

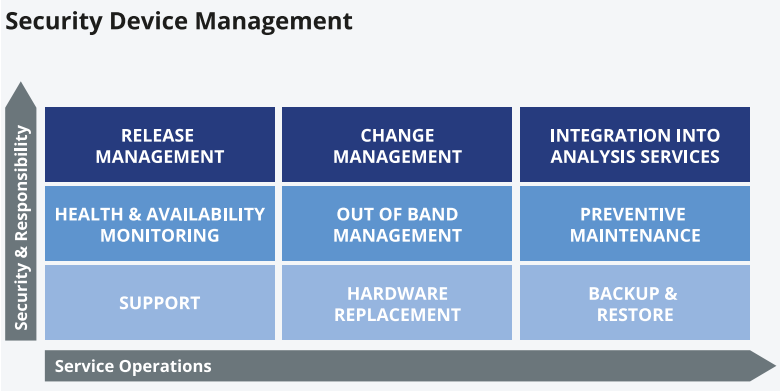
- Betrieb mehrerer Security Operation Center (SOC) weltweit
- Beschäftigung von Security-Analysten und Bereitstellung eines Computer-Security-Incident-Response-Teams (CSIRT)
- Incident Management, Incident Response und Incident Reporting
- Global Threat Intelligence und Nutzung von Threat Intelligence Feeds
- Kundenübergreifende Erfahrungen und Korrelationen
- Device Management (Authentifizierung, Privileged Identity Management, Key Management)
- Security Monitoring
- Vulnerability Management
- SIEM as a Service.

Auch diese Leistungen müssen rund um die Uhr und an allen Tagen im Jahr zur Verfügung stehen, da für kritische Sicherheitsvorfälle kurze Reaktionszeiten zwingend erforderlich sind.

Die skizzierten hohen Sicherheitsanforderungen sind hinsichtlich Art und Umfang selbst für grosse Konzerne kaum zu erfüllen und damit für mittelständische Unternehmen quasi ein Ding der Unmöglichkeit. Folglich ist auch eine dynamische Marktentwicklung im MSS-Bereich erkennbar.

Schlägt ein Unternehmen den MSS-Weg ein, ergeben sich zahlreiche Vorteile. Zu nennen sind etwa der zuverlässige Schutz geschäftskritischer Systeme und Daten, die rechtzeitigen und aussagekräftigen Sicherheitsanalysen auf Basis zusammenhängender Kontextdaten oder die proaktive Risikominderung durch die Behebung identifizierter Bedrohungen und Schwachstellen. Zu berücksichtigen ist lediglich, dass das auslagernde Unternehmen nicht durch eine extrem lange Vertragslaufzeit in Abhängigkeit eines bestimmten MSS-Anbieters gerät. Nicht zuletzt ist dabei auch darauf zu achten, dass eine praktikable Exit-Strategie vereinbart wird.

Das MSS-Angebot von NTT Security basiert auf einem Cyber-Defense-Ansatz mit den vier Grundkomponenten Prävention, Erkennung, Abwehr und Reaktion. (Quelle: NTT Security)



Autor: Kevin Eisele
ist GTM Advanced Services bei NTT Security.