Handlungsfähig bleiben dank Managed Security Services

Managed Security Services (MSS) sind konkret definierte IT-Services, die ein Dienstleister für seinen Auftraggeber erbringt. Der Artikel erläutert in einer Kurzeinführung die wichtigsten Aspekte, die Banken und Sparkassen über Managed Security Services wissen sollten. Außerdem: Tipps für die Auswahl des Dienstleisters.

Autoren:
Wolfgang Kiener,
Business Development Manager, TÜV Rheinland

Haralabo Papanikolaou,
Service Manager Cyber Security Center, TÜV Rheinland

Ob Konzerne oder Mittelstand: Heute müssen alle Unternehmen damit rechnen, früher oder später Ziel von Cyberangriffen zu werden. Die Angriffe, z.B. mittels Malware, sind darauf ausgerichtet, Daten auszuspähen und zu stehlen, Prozesse zu sabotieren oder Daten zu verschlüsseln und z.B. nur gegen Lösegeld freizugeben. Einfallstor für Angreifer sind Schwachstellen in Software, IoT-Geräten und IT-Netzwerken. Vor allem die Bedrohung durch Erpresserprogramme, sogenannte Ransomware, hat sich seit 2016 deutlich verschärft, so das Fazit des Bundesamtes für Sicherheit in der Informationstechnik, BSI, im Lagebericht 2016. Die aktuelle Cyber-Bedrohungslage ist durch mehrere Faktoren charakterisiert. So schreiten Professionalisierung und Industrialisierung von Cyberangriffen weiter voran. Konventionelle Abwehr verliert immer mehr an Wirksamkeit. Schwachstellen in IoT-Geräten führen zu Sicherheitsvorfällen in bisher als abgesichert geltenden technologischen Ökosystemen wie Car-IT, Medizingeräten oder kritischen Infrastrukturen sowie Prozessleittechnik und vernetzten Industrieanlagen (Industrie 4.0). Angreifer geben sich gegenüber Mitarbeitern in anzugreifenden Unternehmen z.B. als Kollegen oder Vorgesetzte aus und fordern zur Herausgabe von Passwörtern oder zur Anweisung von Transaktionen (CEO Fraud) auf. Das Vertrauen des Opfers erschleichen sich die Angreifer durch authentisch wirkende Nachrichten per Telefon oder Email, die teilweise hochgradig an die Zielperson angepasst sind (Spear Phishing). Benötigtes Hintergrundwissen wird häufig durch gezielte Datensammlung in sozialen oder beruflichen Netzwerken beschafft. Vor diesem Hintergrund fehlt es auf Seiten der Geldinstitute und Öffentlichen Hand häufig an Spezialisten, die in der Lage sind, eine qualifizierte Abwehr zu leisten. Mehr als die Hälfte aller Unternehmen hat derzeit Probleme, Stellen in der IT mit Fachkräften zu besetzen. Bereits heute besteht eine globale Lücke von 1,2 Millionen Cyber-Security-Experten, die sich bis 2022 auf 1,8 Millionen vergrößern wird.

Aktiv gegen Fachkräftemangel und wirtschaftliche Engpässe

Angesichts der zunehmenden Komplexität der Angriffe einerseits und der IT-Infrastrukturen andererseits sind IT-Sicherheitsmaßnahmen für Geldinstitute intern kaum noch ganzheitlich abzubilden. Zu den täglichen Herausforderungen zählen z.B.:

- hohe Betriebskosten und Ressourcenbindung
- eine ständig steigende Bedrohungslage mit wechselnden Angriffsmechanismen
- ein Technologiedschungel und eine Schatten-IT
- ein bedarfsgerechter Einsatz von Hardware und Services im IT-Sicherheitsumfeld
- Fachkräftemangel und steigende Personalkosten

Managed Security Services, kurz MSS, sind für immer mehr Unternehmen eine wirtschaftlich attraktive Alternative, um Engpässe in punkto Personal und Technologie zu umgehen, die es mittlerweile in allen relevanten Bereichen der Informationssicherheit gibt: von Dienstleistungen innerhalb der Prozesslandschaft des Unternehmens bis hin zur Betriebsübernahme mit aktiver Sicherheitsüberwachung und Sicherheitschecks. Daneben steigert die Organisation auch die Qualität der Informationssicherheitsstrategie und erhöht sukzessive den Reifegrad in punkto Cyber Security.

Managed Security Services werden mit dem Kunden gemeinsam definiert und nach Möglichkeit auf die Bedürfnisse der Organisation zugeschnitten. Realisiert werden sie durch Experten, die Prozesse, IT und Sicherheitsanforderungen verstehen. Sie können Konsequenzen und Auswirkungen verschiedener IT-Szenarien abschätzen und geeignete Gegenmaßnahmen initiieren bzw. Empfehlungen an die internen Kollegen des Auftraggebers aussprechen. Managed Security Services werden in verschiedenen Sourcingmodellen angeboten.

Die Entscheidung, welches Modell am besten zu einem Unternehmen passt, hängt überwiegend vom Reifegrad des internen Sicherheitsbetriebs, vom Budget und von der Sourcingstrategie eines Unternehmens ab. Die Abgrenzung: Im Gegensatz zum typischen Outsourcing werden interne Stellen nicht überflüssig, obgleich im Rahmen von MSS operative Aufgaben vom Anbieter übernommen werden. Kunden können aber Sicherheitsrisiken nicht outsourcen und müssen vielmehr mit den vorhandenen Ressourcen dafür sorgen, dass Sicherheitsdienstleister mit entsprechend qualifiziertem Personal gesteuert und überprüft werden. MSS-Anbieter übernehmen klar abgegrenzte Teilbereiche auf der Grundlage der Service Level Agreements (SLAs).

	SOC Onsite	MSS	Hybrid
Team	Kunde Provider Cosourcing	Provider	Provider
Policy, Prozesse, Verfahren	Kunde	Provider	Provider
Use Cases, Threat Intelligence	Kunde	Provider	Provider Kunde
Plattformtechnologie	Kunde	Provider	Provider Kunde
Investment	High CAPEX[1] High OPEX[2]	Low CAPEX Predictive OPEX	Medium CAPEX Medium OPEX
Zeit für Bereitstellung	High	Low	Medium

[1] Engl.: CAPEX, capital expenditures, Investitionsausgaben für längerfristige Anlagegüter, im betriebswirtschaftlichen Sinne keine Kosten, sondern die Umwandlung in Vermögen.
[2] Engl.: OPEX, Operational expenditure, Aufwendungen für den operativen Geschäftsbetrieb.

Tabelle 1: mögliche Sourcingmodelle bei MSS *Quelle: TÜV Rheinland*

Tipps für die Auswahl eines MSS-Dienstleisters

Ist die grundsätzliche Entscheidung für eine externe Dienstleistung gefallen, sollten Unternehmen einige Punkte beachten, um den richtigen Partner für Managed Security Services zu finden.

1. Suchen Sie sich einen ausgewiesenen Spezialisten für Informationssicherheit.
Anders als ein Dienstleister mit der Generalistenperspektive sollten der MSS-Partner und sein Team einen ganzheitlichen Blick auf die Informationssicherheit haben, über branchenübergreifende Projekterfahrung verfügen und auf ein umfassendes Lösungsportfolio verweisen. Wichtig ist, dass klare Leistungsbeschreibungen vereinbart werden.

2. Entspricht der MSS-Anbieter der Compliance?
Unternehmen sind gesetzlich dazu verpflichtet, sich von den Fähigkeiten und der technischen Organisation eines MSS-Dienstleisters zu überzeugen, vor allem dann, wenn der MSS-Anbieter Zugriff auf personenbezogene Daten haben könnte. Er sollte den aktuellen gesetzlichen Anforderungen entsprechen und auch auf die Umsetzung kommender Gesetze (z. B. EU-Datenschutz Grundverordnung etc.) vorbereitet sein.

3. Der Anbieter sollte flexibel sein und ein breites fachliches Spektrum abdecken.
Managed Security Services sollten ein breites Spektrum abdecken, aus dem sich bedarfsgerecht und modular individuelle Betriebs- und Supportlösungen entwickeln lassen: von der vollständigen Betriebsübernahme mit aktiver Sicherheitsüberwachung und regelmäßigen Sicherheitschecks über Rund-um-die-Uhr-Supportunterstützung bis hin zu Dienstleistungen innerhalb der Prozesslandschaft des Unternehmens.

4. Kann der Dienstleister einen festen Ansprechpartner bieten?
Grundsätzlich sollte der MSS-Provider einen festen Ansprechpartner stellen, der mit den entsprechenden internen Abteilungen des Auftraggebers – wie z. B. der Security-Management-Abteilung oder den Bereichen Risikomanagement und Business-Fachabteilungen – in ständigem Austausch steht.

5. Versteht der Dienstleister Ihr Business?
Der Partner der Wahl sollte den technischen Hintergrund und die Geschäftsprozesse des jeweiligen Unternehmens verstehen. Nur dann kann er Konsequenzen und Auswirkungen, zum Beispiel beim Ausfall einer Komponente, abschätzen, die Folgen für das Unternehmen bewerten sowie geeignete Maßnahmen vorschlagen und treffen. Die Lösungen sollten sich an den betriebskritischen Prozessen orientieren.

6. Die Bedeutung von Service Level Agreements
Managed Security Services sind kein Ersatz für interne Sicherheitsrichtlinien, können die Compliance-Konformität allerdings um ein Erhebliches steigern. Unternehmen, die für spezielle Aufgabenstellungen rund um Informationssicherheit kein Know-how im eigenen Hause haben und qualifizierten externen Support einkaufen, können mit MSS nachweisen, ihren unternehmerischen Sorgfaltspflichten nachgekommen zu sein. Denn der Partner muss dafür sorgen, dass neue Gesetze und Vorgaben nicht nur kommuniziert, sondern auch eingehalten werden. Wichtig ist allerdings ein detailliertes Service Level Agreement, das die Verantwortung des externen Partners und die Kontrollmöglichkeiten des Kunden genau definiert.

Fazit

Die digitale Transformation und die zunehmende Konvergenz von Technologien erfordern neue Konzepte in Informationstechnologie und Cybersicherheit. In Zeiten, in denen Unternehmen, ihre Partner und Kunden immer enger vernetzt sind, gewinnt Informationssicherheit zur Absicherung der Unternehmenswerte und zur Steigerung der Wettbewerbsfähigkeit stark an Bedeutung. Moderne und innovative Sicherheitskonzepte unter Berücksichtigung neuer Sourcingmodelle im Bereich Managed Security Services ermöglichen die kosteneffiziente Steigerung des Sicherheitsniveaus in einem Unternehmen. MSS-Partner bieten standardisierte und qualitativ hochwertige Dienstleistungen in klassischen und fortgeschrittenen Feldern der Cyber Security wie z. B. der Abwehr von zielgerichteten Angriffen. Ein Schlüsselfaktor für die erfolgreiche Zusammenarbeit mit einem Managed-Security-Service-Anbieter ist die erfolgreiche Integration und Steuerung des Dienstes im Rahmen eines risiko- und prioritätenbasierten Incident- und Schwachstellenmanagements.