Managed-Security-Services:

Verantwortung teilen – Kontrolle gewinnen

Im Zuge der Frage, wie Unternehmen mit der zunehmenden IT-Bedrohungslage Schritt halten können, ohne das eigene IT-Team an die Grenzen der Belastbarkeit zu bringen, fällt mittlerweile nahezu unausweichlich das Stichwort „Managed-Security-Services" (MSS). Der Bedarf – und auch das Angebot – an entsprechenden Outsourcing-Modellen wächst stetig. Was treibt diesen Trend und worauf sollte man bei der Auswahl eines geeigneten Dienstleisters achten?

Von Michael Haas, Seeheim-Jugenheim

Selbst wenn die Zahlen je nach Quelle abweichen, ist die Richtung klar: Das Geschäftsmodell von Managed-Security-Services (MSS) hat Auftrieb, eine Umkehr dieser Entwicklung ist nicht in Sicht. Dass sich entsprechende IT-Dienstleistungen zunehmender Beliebtheit erfreuen, verwundert im Hinblick auf die heutigen Rahmenbedingen kaum: Vielen IT-Abteilungen fällt es immer schwerer, die – nicht zuletzt durch den Anstieg von Remote- und Hybridarbeit – immer größer werdenden Angriffsflächen mit den eigenen Mitteln konsequent unter Kontrolle zu behalten.

Die Absicherung von Daten, Netzwerken und über den klassischen Perimeter hinausgehenden Infrastrukturen erfordert anders als früher vielerorts deutlich höhere Aufmerksamkeit und zusätzliche manuelle Eingriffe. Nur so kann auf aktuelle Gefahrentrends überhaupt noch adäquat und – gerade bei Zero-Day-Angriffen – kurzfristig reagiert werden. Die Konfiguration und das Management der eingesetzten, zum Teil in die Jahre gekommenen oder aufgrund neuer Anforderungen zusammengestückelten Security-Lösungen gestaltet sich enorm zeit- und ressourcenintensiv. In diesem Zusammenhang lassen sich mit der Beauftragung eines geeigneten IT-Servicepartners (Managed-Security-Service-Provider, MSSP) meist mehrere Fliegen mit einer Klappe schlagen.

M wie Mehrwert

Vor allem folgende Aspekte spielen bei der Abwägung, einen Dienstleister ins Boot zu holen, eine wichtige Rolle:

_____ *Mehr technisches und sicherheitsrelevantes Fachwissen:* Unternehmen, die jederzeit mit aktuellen Entwicklungen an der Angriffsfront Schritt halten wollen, brauchen vor allem einschlägige Expertise und/oder die Zeit, sich in die jeweiligen Fragestellungen einzuarbeiten – beides fehlt in IT-Abteilungen, gerade bei kleinen und mittleren Unternehmen (KMUs), zunehmend oft. Fachleute für IT im Allgemeinen und Cybersicherheit im Speziellen sind immer schwerer zu finden, vor allem für weniger große Unternehmen – diese haben im „War for Talents" gegenüber Konzernen aufgrund geringerer finanzieller Ressourcen allzu oft das Nachsehen. Wichtig ist im Zuge dessen nicht zuletzt die Schnittstellenkompetenz zwischen rein technischen Aufgaben und sicherheitsspezifischen Implikationen; hier bieten MSSP eine effektive Möglichkeit, diese Lücke zu schließen.

_____ *Zusätzliche betriebliche Effizienz:* Ebenso geht im Hinblick auf die reinen Lizenz- und Betriebskosten der erforderlichen IT-Security-Lösungen von Managed-Security-Services entscheidende Attraktivität aus. Denn für viele Unternehmen summieren sich die einzelnen Posten für den Kauf, die Verwaltung und die kontinuierliche Aktualisierung einer kompletten Cybersicherheitsinfrastruktur mittlerweile zu enormen Kosten. Durch die Dezentralisierung der Arbeitswelt und den Siegeszug von Cloudlösungen entstehen zusätzliche Einfallstore, die nicht zuletzt auch die Erweiterung bestehender Sicherheitsarchitekturen erfordern. Die Zusammenarbeit mit einem MSSP kann dazu beitragen, den Schutz der Unternehmensressourcen auf Basis eines „As-a-Service"-Modells zu optimieren und dabei gleichzeitig dafür sorgen, den damit einhergehenden finanziellen Aufwand zu reduzieren oder zumindest planbar(er) zu gestalten – schließlich tritt eine verbindliche Service-Pauschale anstelle der meist kaum bezifferbaren Summe vielfältiger Investitionskosten für unterschiedliche Sicherheitsfunktionen und den damit verbundenen Gesamtbetriebskosten in den eigenen Reihen.

_____ *Erhöhte Flexibilität:* Organisationen und Prozesse verändern sich, gleiches gilt für die Angriffsszenarien – somit wandeln sich die Herausforderungen im Hinblick auf IT-Security stetig. Durch die Beauftragung eines MSSP können Unternehmen nicht nur sicherstellen, dass ihre „Verteidigung" dank des Einsatzes und dem Nachrüsten zeitgemäßer Funktionalität im Rahmen der Service-Angebote immer auf dem neuesten Stand ist. Darüber hinaus lassen sich bei Veränderungen der Organisationsstruktur (Mitarbeiterwachstum, neue Standorte, mehr Homeoffice-Optionen etc.) die Spezifika der Vereinbarungen jederzeit schnell anpassen und skalieren, um neue Bedürfnisse souverän und schnell abzubilden – beispielsweise die notwendige Verankerung zusätzlicher Funktionen wie Multifaktor-Authentifizierung (MFA) oder erweiterte Endpunktsicherheit.

S wie sorgsame Auswahl

Der Markt rund um Managed-Security-Services ist in Bewegung und immer neue Angebote buhlen um die Gunst der Kunden. Doch nicht jeder Anbieter leistet das gleiche. Grundsätzlich lassen sich grob drei verschiedene Kategorien unterscheiden:

_____ Reseller, die hauptsächlich Implementierungen vornehmen und darüber hinaus Basis-Serviceleistungen anbieten (Wartung, Patch-Management etc.)

_____ Security-Manager, die sich bereits als weiterführende Dienstleister positionieren und spezifische Aufgabenbereiche als Managed-Security-Service abbilden (Managed Firewall, Managed Endpoint-Security o. Ä.)

_____ sogenannte SOC-Partner (Security-Operations-Center), welche die gesamte IT-Landschaft auf Kundenseite rund um die Uhr überwachen

Um den richtigen Partner zu finden, sollten Unternehmen vor ihrer Entscheidung den Bedarf in den eigenen Reihen exakt ausloten (Spezifika der IT-Infrastruktur, gesetzliche Rahmenbedingungen, Compliance-Vorgaben, bereits bekannte potenzielle Schwachstellen, Personalsituation). Wer Fehlinvestitionen möglichst früh einen Riegel vorschieben will, ist gut damit beraten, ebenfalls zu hinterfragen, ob ein MSSP in der Lage ist, neben den aktuellen Sicherheitsanforderungen auch künftige Bedürfnisse zu erfüllen – so individuell diese auch sein mögen.

Hier spielen sowohl Breite als auch Tiefe des Gesamtangebots an Security-Funktionalität eine nicht unerhebliche Rolle: Je mehr Themenbereiche ein MSSP aus „einer Hand abdeckt", desto höher ist die Wahrscheinlichkeit, dass er auch mit neuen Rahmenbedingungen umgehen kann, welche die Zukunft bringt. Zudem sollten die zugrunde liegenden Lösungsbausteine darauf ausgerichtet sein, Bedrohungsinformationen effektiv und im Idealfall synergetisch zu verarbeiten. Eine einheitliche Verwaltung und umfassende Berichtsoptionen sind darüber hinaus wichtige Qualitätskriterien. Es kann sich ebenfalls auszahlen, darauf zu achten, dass man als Auftraggeber nach Auftragserteilung bei Bedarf via Cloud über eine zentralisierte Oberfläche Einblick in die beauftragten Dienste hat. Letztendlich kommt es vor allem darauf an, die operative Belastung in den eigenen Reihen zu minimieren, ohne dass das mit einem (Gefühl von) Kontrollverlust einhergeht.

S wie Synergie

Viele MSSP bieten mittlerweile cloudverwaltete „Plug-and-Play"-Optionen für unterschiedlichste Security-Thematiken – von der Firewall bis hin zu Diensten wie

Multifaktor-Authentifizierung oder Endpunktsicherheit. Um den Anforderungen im Hinblick auf die Gefahrenlage und der individuellen Bedarfssituation auf Kundenseite Rechnung zu tragen, muss die Perspektive jedoch weg vom einzelnen Produkt gehen. Stattdessen zählt ein moderner, ergebnisorientierter Lösungsansatz!

Hierzu vielleicht am besten mal ein Beispiel: Ransomware. Da deren Eintrittstore bekanntermaßen an unterschiedlichster Stelle liegen, bringt ein fortschrittliches Managed-Service-Konzept für Endpoint-Security nichts, wenn gleichzeitig das Thema Netzwerkschutz brach liegt. Insofern macht es auch durchaus Sinn, dem Werkzeugkasten auf Partnerseite inklusive dessen Integrationsmöglichkeiten einen genaueren Blick zu schenken, selbst wenn man bestimmte Tools (zumindest noch) nicht benötigt. Denn je besser einzelne Funktionsbausteine zusammenarbeiten und je mehr fortschrittliche KI- oder Machine-Learning-Technologie im Sinne einer zielführenden Automatisierung zum Einsatz kommt, desto niedriger gestalten sich in der Regel auch die Verwaltungskosten – zudem bleibt mehr Zeit für Kundendienst und Support.

Synergie am Beispiel: Threat-Hunting

Fortschrittliche MSSP können durch weitgehende Automatisierung, ein gezieltes Zusammenspiel der eingesetzten Security-Mechanismen und zuverlässige Kontrolle aktueller Gefahren, Angriffstrends oder sicherheitsrelevanter Auffälligkeiten wichtigen Mehrwert stiften und dazu beitragen, dass selbst kleinere Unternehmen in Sachen Sicherheit großen Konzernen in nichts nachstehen.

Die Kür sind dabei beispielsweise auf MSSP-Seite integrierte Threat-Hunting-Services, die bislang unbekannten Gefahren proaktiv vorbeugen, indem dedizierte Sicherheitsanalysten jedweder Auffälligkeit bereits beim ersten Erscheinen nachgehen – mit einem Aufwand, der im normalen IT-Alltag von Unternehmen kaum zu stemmen ist. Auf diese Weise lassen sich unter anderem auch Brute-Force-Angriffe auf RDP, die Ausführung von In-Memory-Skripten über PowerShell oder die Installation von Remote-Dateien über „umbenannte“ msiexec-Programme frühzeitig verfolgen – für zusätzlichen Sicherheitsgewinn. In der Folge profitieren Kunden nicht nur von der Entlastung, sondern können auch auf mehr Qualität bei der Gefahrenabwehr vertrauen.

Caveat emptor

„Obacht!“ heißt es hingegen bei Anbietern, die vornehmlich auf „Silo-Lösungen“ setzen: In dem Fall ist durchaus mit mehr Sand im Getriebe zu rechnen, sollten die Kundenbedürfnisse eine Erweiterung der abgedeckten Leistungen und dadurch ein Zusammenspiel proprietärer Einzelprodukte erfordern.

Aber nicht nur hinsichtlich der funktionalen Leistungsfähigkeit geht es darum, die Spreu vom Weizen zu trennen: Es macht auch einen Unterschied, wie flexibel sich die Zahlungsmodalitäten darstellen. Wenn MSSP hier über unterschiedliche Optionen verfügen – von traditionellen Vorauszahlungen bis hin zu Abonnements oder „Pay-as-you-go“-Plänen, ist dies auf keinen Fall von Nachteil für den Kunden.

Fazit

Für Unternehmen, die Verantwortung für IT-Security „abgeben“ wollen, sind Managed-Security-Services durchaus eine spannende Möglichkeit, mit denen sich gleichzeitig auch an den Effektivitätsstellschrauben der Gefahrenabwehr drehen lässt.

Zudem werden selbst hochprofessionelle Dienstleistungen aufgrund des zunehmenden Wettbewerbs auch preislich immer attraktiver.

Ein fundiertes Bewusstsein der relevantesten Aspekte, die bei der Entscheidung für einen langfristig geeigneten Dienstleister ins Kalkül gezogen werden sollten, kann ebenfalls erheblich dazu beitragen, dass sich ein Outsourcing mit Sicherheit lohnt. ■

Michael Haas ist Regional Vice President Central Europe bei WatchGuard Technologies.

Need to know für CISO & Co

- <kes> liefert strategisches Wissen für Security-Verantwortliche
- <kes> informiert redaktionell unabhängig zu Management und Technik der Informations-Sicherheit
- <kes> enthält das amtliche Organ des Bundesamts für Sicherheit in der Informationsverarbeitung – BSI-Forum
- <kes> kostet im Jahr weniger als zwei Beraterstunden

<kes>

Die Zeitschrift für Informations-Sicherheit

Für 149,00 € jährlich (inkl. MwSt. und Versandkosten) erhalten Sie alle zwei Monate eine gedruckte Ausgabe und für bis zu fünf Mitarbeiter am belieferten Standort Online-Zugriff auf alle aktuellen Beiträge sowie das <kes>-Archiv.

Online bestellen: datakontext.com/kes
oder per Mail: abo@kes.de

DATAKONTEXT