Integration in die Prozesskette

Maßgeschneiderte Managed Security Services

Managed Security Services (MSS) überzeugen in erster Linie durch Kostenersparnisse, denn speziell die „lästige IT-Sicherheit" ist längst zu einem wunden Punkt vieler Unternehmen geworden. Diese sind aufgrund der immer weiter zunehmenden Komplexität der IT-Sicherheitsinfrastruktur kaum noch in der Lage, die notwendigen Budgets für ein angemessenes IT-Sicherheitsniveau bereitzustellen. MSS können diese Kosten unbestritten drastisch senken, Skaleneffekte einer zentralen und skalierbaren Infrastruktur sorgen für niedrige Betriebskosten. Doch IT-Sicherheit ist kein Produkt – vielmehr handelt es sich um einen stetigen Prozess. Die Herausforderung besteht also darin, arbeitsteilige Services nun sinnvoll in die Ablauforganisation zu integrieren. Hier helfen sogenannte Cloud-Services „von der Stange" kaum weiter.

Managed Security Services (MSS) werden gern als standardisierte Cloud-Lösungen verkauft – bei vielen Anbietern sind derartige Dienste längst nach Preisliste bestellbar. Klassische Vertreter wären die Antispam- und Contentfilter-Dienste, oft in Kombination mit Malware-Erkennung und weiteren Antivirus-Produkten. Endkunden können den Datenverkehr am Internetzugang über Änderungen im DNS oder forwarding Proxyserver leicht an einen beliebigen Anbieter umleiten – der behandelt die Daten dann auf seinen Produkten weiter.

Standardisierung und deren Grenzen

Die standardisierte IT-Security läuft bei den abstimmungsintensiveren Technologien an den eigentlichen Anforderungen des Betriebes vorbei. Beispiel Managed Firewall Services: Die Kommunikationsbeziehungen in dynamischen Unternehmen ändern sich laufend, weiter sind zur Beurteilung der Regelqualität Detail-Kenntnisse zu den Quell- und Zielsystemen notwendig. Die Veränderung und auch das Design der Regelwerke sind abhängig von eingesetzten Technologien, der Aufbau- und Ablauforganisation des Auftraggebers, der Unternehmenskultur, von rechtlichen Rahmenbedingungen sowie von branchenüblichen Besonderheiten zu Compliance-Richtlinien. Und nicht zuletzt auch von der internen Organisation der IT-Abteilung und den handelnden Personen. Standardisierte Produkte nach Preisliste können diesen Anforderungen nicht mehr entsprechen – hier sind maßgeschneiderte Services gefragt. Klare Kandidaten für derart spezialisierte MSS sind zum Beispiel die Managed Firewall Services, Intrusion Detection und Monitoring-Dienste.

Einzellösungen – und trotzdem Kosten sparen

Speziell auf die Kundensituation zugeschnittene Lösungen müssen von den Anbietern gut dokumentiert werden, die Integration der MSS in den organisatorischen Rahmen des Endkunden kostet zudem viel Zeit und Geld. Die Betriebsteams des MSS-Anbieters benötigen für individuelle Kundensysteme Trainings und es entsteht ein erhöhter Abstimmungsaufwand. Wieso ist eine individuelle MSS-Lösung nun oft trotzdem sinnvoller als die Alternative des Security-Eigenbetriebes? Die Wirtschaftlichkeit ergibt sich hier aus der Spezialisierung des Anbieters. MSS-Anbieter setzen bestens

- MSS-Security-Experten in Unternehmensprozesse integrieren
- Flexibilität im Betrieb erhalten

➔ erfordert individuelle Formen der Zusammenarbeit

ausgebildetes Personal ein, die Ressourcen werden dabei jedoch nicht noch für weitere Aufgaben „missbraucht". Die Ausbildung eines Security-Spezialisten ist teuer und erfordert ständig aktualisierte Trainings, was sich bei knapper Personaldecke heute kaum eine IT-Abteilung mehr leisten kann. Die eigenen Security-Spezialisten werden bei den Unternehmen abseits der Sicherheitsthemen daher oft für weitere Aufgaben eingesetzt. In der Regel bearbeiten Mitarbeiter in den IT-Abteilungen viele Themenfelder, die IT-Sicherheit wird eher nebenbei verwaltet – was den eigenen Sicherheitsansprüchen auch nicht gerecht wird. Unter Berücksichtigung von Vertreterregelungen müssten selbst bei homogener IT-Sicherheitstechnik pro Unternehmen drei trainierte Experten für die Sicherheit zur Verfügung stehen. Im 24-Stunden-Betrieb werden die Teams deutlich größer. Diese Mitarbeiter dürften dabei eigentlich nicht mit weiteren Themenkomplexen belästigt werden. Ohne ständig mit Sicherheitsvorfällen, Konfigurationen oder Event-Recherche konfrontiert zu werden, ist die Halbwertszeit des teueren Spezialistenwissens viel zu gering.

Genau hier können die Spezialisten des MSS-Anbieters den eigenen IT-Betrieb sinnvoll ergänzen. Die Security-relevanten Tasks werden mit spezialisierten, in den Prozess integrierten Technikern des MSS-Anbieters schneller, qualifizierter und so letztlich wirtschaftlicher umgesetzt. Bei komplexen oder riskanten Änderungen können die Experten mit Tests in Laborumgebung, Release Checks und Rollout-Plänen den Betrieb nachhaltig stabilisieren. Die Systemverfügbarkeit sollte bei der Beteiligung von MSS-Partnern insgesamt steigen. Die Experten stehen gesichert zur Verfügung, garantierte Reaktionszeiten werden in einem geeigneten Service Level Agreement verankert. Bei einem eng verzahnten Prozess ist der MSS-Anbieter in das Tagesgeschäft integriert, kennt zwangsläufig die aktuellen Änderungen auf den Systemen und ist somit auch jederzeit sofort handlungsfähig.

Reibungsfreie Prozesse

Wichtig sind vor allem die partnerschaftliche Zusammenarbeit und genau beschriebene Schnittstellen in der arbeitsteiligen IT-Security eines Unternehmens. Die Endkunden sollten zudem die strategische Steuerung der Sicherheit nicht aus der Hand geben und nicht unnötig auf Flexibilität verzichten. Speziell der letzte Punkt erfordert neue Denkansätze. Um bei den Managed Firewall Services zu bleiben: Die Firewall an einen MSS-Anbieter zu vergeben, geht ja fast zwangsläufig mit der Aufgabe von Flexibilität einher. Was in eigener Hand noch „auf Zuruf" möglich war, ist bei der Beteiligung unternehmensfremder Techniker schwieriger. Der Anbieter übernimmt neben der Systemverantwortung klassischerweise auch die System-Kennwörter. Statt beispielsweise für neue Testsysteme temporär und kurzfristig einmal schnell selbst eine Firewall-Policy zu ändern, müsste nun zukünftig jeweils der MSS-Anbieter kontaktiert werden – dieser benötigt für seine Task genaue Angaben und auch Zeit zur Umsetzung. Hier wird ein klassischer Outsourcing-Konflikt deutlich.

Eine flexible Lösung könnte hingegen ein Prozess der Auffangkontrolle sein. Der Kunde behält seine administrativen Systemberechtigungen, und der MSS-Anbieter verpflichtet sich, nach eigenständigen Änderungen des Kunden die Auswirkungen der neuen Policy kritisch zu überprüfen. Innerhalb im Service Level Agreement festgelegter Reaktionszeiten kann der Anbieter die Änderung dokumentieren, zurücknehmen oder seinen Kunden Optimierungsvorschläge unterbreiten. So bleibt die „Können wir mal schnell"-Flexibilität des Unternehmens zunächst erhalten, wird aber durch einen definierten Prozessablauf mit einer Qualitätssicherung der Spezialisten flankiert. Der MSS-Anbieter aktualisiert die System-Dokumentation und prüft die Auswirkungen auf Sicherheit, Verfügbarkeit und Notfallprozeduren. Das gewählte Beispiel zeigt zum einen recht deutlich, welche Vorteile Kunden aus maßgeschneiderten Services ziehen können. Zum anderen unterstreicht es die Wichtigkeit einer genauen Prozessbeschreibung bei potenziell abstimmungsintensiven Security-Technologien.

MSS-Anbieter, neue Wege

Der Gedanke ist noch jung, und die Marktteilnehmer müssen sich an die vielfältigen Möglichkeiten erst noch gewöhnen. Doch das Beispiel des Prozesses für Managed Firewall Services zeigt: Zwischen den längst bekannten Extremen „selber machen" und „Outsourcing" liegen viele weitere sinnvolle Varianten.

Um MSS individuell und effizient integrieren zu können, sollten sich Unternehmen die Anbieter genau ansehen. Wie groß ist das Unternehmen, und wie flexibel kann es agieren? Von den Skills der eingesetzten Experten bis hin zur Unternehmensführung und der verfolgten Renditepolitik des Unternehmens – alle Parameter gemeinsam sollten ein gutes und in sich stimmiges Bild ergeben.

Personalfluktuation ist aus Kundensicht in dieser Position lästig und steht einer vertrauensvollen Kommunikation auf Augenhöhe im Wege. Eine Integration in die eigenen IT-Prozesse wird noch leichter fallen, wenn selbst die handelnden Techniker persönlich bekannt sind. Gleichzeitig müssen bei MSS-Anbietern natürlich ausreichend qualifizierte Ressourcen vorhanden sein, um die Leistung auch jederzeit sicher erbringen zu können. Es empfiehlt sich, den MSS-Anbieter eher als Partner zu begreifen statt nur als einen Anbieter von IT-Leistungen.

Bei einer erfolgreichen MSS-Intergration mit individuellen Lösungen steht einer langfristigen Zusammenarbeit in der Regel nichts mehr im Wege. ■

Tim Cappelmann,
Leiter Managed Services bei der AirITSystems GmbH

Für Abonnenten ist dieser Artikel auch digital auf www.datakontext.com verfügbar

Weitere Artikel/News zum Schwerpunkt unter www.datakontext.com/mss