symantec.

Management der Unternehmenssicherheit

Überlegungen zu internen Security Management-Lösungen und externen Managed Security Services

INHALT

INHALT

Inhalt

Einführung

Sicherheit ist ein Bereich, der für ein modernes Unternehmen heute mehr und mehr an Bedeutung gewinnt. Durch die Verbreitung des Internets und die zunehmende Akzeptanz von E-Business, E-Commerce und E-Retailing wird Sicherheit im Unternehmen zum unverzichtbaren Faktor. Noch nie zuvor wurde ihr eine so wichtige Stellung für die Überlebensfähigkeit eines Unternehmens, für den entscheidenden Wettbewerbsvorteil und für den Erhalt seines Stakeholder-Wertes beigemessen wie heute. Ein effektives Sicherheitsprogramm muss daher mehr leisten, als nur Geräte und Technologien bereitzustellen – es muss auch Menschen und die Abläufe innerhalb des Unternehmens integrieren.

Effektive Sicherheitsprogramme werden oftmals jedoch in ihrer Umsetzung und Verwaltung behindert. Zu diesen Hindernissen gehören u. a.:

- Der Mangel an qualifizierten, ausgebildeten Sicherheitstechnikern
- Fehlende Ressourcen und Infrastruktur zur Unterstützung eines Sicherheitsprogramms, das rund um die Uhr angeboten wird (24x7)
- Zunehmende Komplexität der Sicherheitstechnologie
- Nicht genügend Zeit, um sich auf eine konsequente Sicherheitsverwaltung und auf stringente Betriebsabläufe zu konzentrieren

Viele Unternehmen, die ihre Sicherheitsverwaltung bislang intern regelten, sind deshalb auf der Suche nach Alternativen, mit deren Hilfe sie diese Blockaden von vornherein ausschalten können. Sie müssen ein stabiles Sicherheitsfundament legen, um sich ungestört auf ihr Kerngeschäft und den Ausbau umsatzfördernder Bereiche wie das E-Business konzentrieren zu können.

Ähnlich wie schon bei der physischen Sicherheit und den Informationstechnologien ganz allgemein wird das Outsourcing der verschiedenen Sicherheitsaufgaben zunehmend attraktiver. Einer Studie von Gartner Dataquest zufolge sind Managed Security Services, also die externe Verwaltung und Überwachung von Sicherheitssystemen, das am schnellsten wachsende Segment des Information Security Services-Marktes. "Managed Security Services Provider" (MSSPs) unterstützen mit hochverfügbaren Security Operation Centers (die entweder Teil ihrer eigenen Einrichtungen oder Teil eines Data-Center-Anbieters sind) Services rund um die Uhr (24x7)[i].

Diese sind dafür ausgelegt, die Anzahl der Sicherheitsmitarbeiter zu reduzieren, die von einem Unternehmen eingestellt, ausgebildet und langfristig verpflichtet werden müssen, um ein akzeptables Sicherheitsfundament zu schaffen. Für viele Unternehmen zeichnen sich zwei mögliche Alternativen ab: Ein betriebsinternes oder aber ein externes Security Management, das entweder ganz oder nur in Teilbereichen zum Einsatz kommt.

Die Frage, die sich den meisten Unternehmen im Zusammenhang mit einer Outsourcing-Entscheidung stellt, lautet: Können wir Security Management-Aufgaben effektiv über Outsourcing oder Teil-Outsourcing verwalten und dennoch kosteneffizient arbeiten?

Die Durchführung einer akkuraten Analyse und die korrekte Einschätzung der mit dem Outsourcing des Security Managements verbundenen Risiken und Vorteile ist eine äußerst anspruchsvolle Aufgabe. Die Auswahl eines Managed Security Service Providers muss daher wohl durchdacht und äußerst sorgfältig durchgeführt werden. Folgende Faktoren werden bei der Entscheidung mit einbezogen:

- Wirtschaftliche Stabilität des Unternehmens
- Fachwissen der Sicherheitstechniker
- Bandbreite und Flexibilität der Services
- Kosten-Nutzen-Analyse
- Sicherheitsphilosophie, Unternehmenskultur und Mitarbeiter
- Verpflichtung zur Einhaltung von Service-Stufen-Vereinbarungen
- Unterstützte Technologie
- Vorhandensein sicherer Betriebseinrichtungen

Von all diesen Faktoren kann sich die Analyse der mit dem Outsourcing verbundenen Kosten als schwierigste Aufgabe erweisen, denn die meisten Unternehmen können die finanziellen Konsequenzen einer solchen Entscheidung nicht in vollem Umfang abschätzen. Eine vor kurzem von InfoWorld Outsourcing durchgeführte Befragung von 100 Technologie-Fachkräften kommt zu dem Ergebnis, dass 61 Prozent der Unternehmen nicht wissen, mit welchen Einsparungen sie in den nächsten 12 Monaten durch das Outsourcing von IT-Aufgaben rechnen können[ii]. Dies gilt tatsächlich für die meisten Unternehmen, die über das Outsourcing ihrer Security Services nachdenken.

Das vorliegende Dokument hat sich zum Ziel gesetzt, Unternehmen bei der Kalkulation der Managed Security-Kosten zu unterstützen. Es enthält praxisnahe Kostenvergleiche, die Unternehmen als Grundlage für eine finanzielle Analyse verwenden können. Darüber hinaus beschreibt dieses Dokument die Vorteile, die das Outsourcing von Sicherheitsfunktionen beinhaltet, und bietet Entscheidungshilfen für die Beurteilung möglicher Managed Security Services Provider.

Herausforderungen für moderne Unternehmen

E-Commerce- und E-Business-Initiativen sind für viele Unternehmen ein Ansporn für eine offene, verteilte Netzwerkumgebung. Ein solches Umgebungsdesign wendet sich an alle Mitarbeiter, Kunden, Partner, Zulieferer und Distributoren, um Informationen gemeinsam zu nutzen und auszutauschen. Doch gerade diese vernetzten Umgebungen bieten intern wie auch extern ein leichtes Angriffsziel für verärgerte Mitarbeiter, Hacker und Angreifer, die destruktive Aktionen planen und einem Unternehmen schaden wollen. Der dabei verursachte Schaden hat oftmals verheerende Folgen für das gesamte Unternehmen. Er kann sich negativ auf das Kerngeschäft auswirken, ein positives Image zerstören und das Vertrauen der Kunden in das Unternehmen gänzlich in Frage stellen.

EIN MODERNES UNTERNEHMEN MUSS SICH DAHER FOLGENDEN HERAUSFORDERUNGEN STELLEN:

Es gibt einen sichtbaren Anstieg vorsätzlich krimineller Handlungen, die sich gezielt gegen Unternehmen richten.

Da Kunden und Geschäftspartner darauf angewiesen sind, über offene Netzwerke, wie z. B. das Internet, auf unternehmenskritische Produkt- und Service-Daten zugreifen zu können, muss jedes Unternehmen dafür sorgen, dass die Integrität dieser Informationen sichergestellt ist. Andernfalls besteht das Risiko, dass der Ruf und der Markenname des Unternehmens erheblich in Mitleidenschaft gezogen werden. Um Kerngeschäft und Image eines Unternehmens nachhaltig zu schützen, müssen sämtliche Daten und Informationen effektiv gesichert werden.

Unternehmen haben jedoch nicht nur den Wunsch, ihre Daten und physikalischen Ressourcen zu schützen, sondern müssen für ihre Mitarbeiter ein produktives Arbeitsumfeld einrichten. Es gibt eine zunehmende Akzeptanz und wachsende Anzahl von mobilen Mitarbeiterpools, Telearbeitsplätzen und Fernverwaltung von Rechnersystemen, denen traditionelle LANs und WANs jedoch längst nicht mehr gewachsen sind. In dem Maße, in dem der Fernzugriff auf Unternehmensnetzwerke zunimmt, treten auch spezielle Sicherheitsprobleme auf und somit wächst auch die Notwendigkeit, den Datentransfer an exakt diesen Zugriffspunkten zu schützen.

Wenn die Sicherheit vielleicht auch keine Kernkompetenz eines Unternehmens ist, so ist sie doch eine Kernvoraussetzung.

Unternehmen, die ihre Geschäftstätigkeit auf E-Commerce und E-Business ausgerichtet haben, müssen sicherstellen, dass ihre Informationsressourcen zu jeder Zeit adäquat geschützt sind. Die Verwaltung der Informationssicherheit setzt konstante Wachsamkeit und eine konsequente Aufzeichnung aller Statusänderungen im Netzwerk voraus. Diese Aufgabe ist äußerst komplex und gehört nur selten zur Kernkompetenz der technischen Mitarbeiter eines schnell wachsenden Unternehmens.

Für die Deckung der primären Business-Anforderungen eines Unternehmens werden nur begrenzt IT-Ressourcen benötigt.

Informations- und Technologie-Manager benötigen hier Unterstützung, um Betriebsressourcen für bedeutendere, wertsteigernde Aktivitäten, an denen Kernkompetenzen und Unternehmensstrategien beteiligt sind, freizugeben. Die Spezialisten für die Informationssicherheit in den jeweiligen Unternehmen besitzen in der Regel detaillierte Kenntnisse über die im Netzwerk ausgeführten unternehmenskritischen Anwendungen. Sie wissen auch genau, welche Auswirkungen diese Anwendungen auf die Bandbreite und den Unternehmensbetrieb insgesamt haben. Im Idealfall würden diese internen Spezialisten am effektivsten für die Planung künftiger Netzwerk-Umgestaltungen und Migrationen eingesetzt werden. Hier würden sie strategische Unternehmensinitiativen unterstützen oder neue Anwendungen implementieren, die sich auf Bereiche mit einem größeren Gewinnpotenzial konzentrieren.

Betriebsinterne IT-Abteilungen besitzen allerdings weder die notwendigen Ressourcen noch das Fachwissen, um damit den Schutz der wertvollen Informationsressourcen zu garantieren.

Sie verfügen darüber hinaus auch nicht über die Ressourcen, die zur Aufrechterhaltung des Fachwissens erforderlich wären, um zwischen echten und unbeabsichtigten Angriffen unterscheiden zu können. Als Folge hiervon könnten sie das System unabsichtlich für derartige Angriffe anfällig machen. Wenn sichergestellt sein soll, dass Mitarbeiter geschult werden und über die neuesten Technologien und Sicherheitsbedrohungen informiert sind, lassen sich hohe Aufwendungen und interne Kosten dafür nicht umgehen.

Gut ausgebildete und erfahrene Spezialisten für die Informationssicherheit sind nicht leicht zu finden, denn die Nachfrage nach diesen Fachkräften ist extrem hoch.

Darüber hinaus verursachen sie hohe Einstellungskosten und sind langfristig auch schwer an das Unternehmen zu binden. Durch den häufigen Arbeitsplatzwechsel gerade in diesem Bereich hat es ein Unternehmen heute schwer, seine gesamten Informationsressourcen effektiv zu verwalten.

Kalkulation der Security Management-Kosten

Die Total Cost of Ownership (TCO) für ein Security Management-Programm umschließen neben Mitarbeitern und Hardware auch die für den Aufbau, die Aktualisierung, die Wartung, den Betrieb und die Steuerung der Systeme benötigte Software und Ausrüstung.

Ein Unternehmen, das vor der Entscheidung steht, Managed Security Services über einen externen Provider zu beziehen, sollte in jedem Fall mehrere Variablen auf die Laufzeit des Managed Security Services-Vertrags hochrechnen. Dies betrifft im Einzelnen:

- Alle relevanten Kapital- und Betriebskosten
- Die Kosten für die MSSP-Supervision
- Möglicher Anstieg der Kosten für Gehälter, Sozialleistungen und Serviceverträge
- "Geldkosten" und Zinskosten
- Restwert der Ausrüstung und Einrichtungen
- Umstellungskosten, einschließlich Personalkosten
- Kosten für Änderungen im Hinblick auf die Ausrichtung und die Ebene von Ressourcen
- Vertragsänderungskosten

Um eine langfristige und wirtschaftlich tragbare Kalkulation der mit dem betriebsinternen Security Management verursachten Total Cost of Ownership (TCO) erstellen zu können, sind eine Vielzahl an Kostenträgern über einen Zeitraum von mehreren Jahren zu erfassen. Das Unternehmen muss sowohl offene als auch versteckte Kosten benennen und analysieren. In den folgenden Abschnitten sind etliche Kostenpunkte aufgeführt, die ein Security Management-Programm verursacht.

AUSRÜSTUNG

Ausgaben für Hardware und Software

Für das betriebsinterne Security Management müssen Unternehmen die Kosten aller Hardware- und Softwareprodukte erfassen, die für die Sicherheitsverwaltung und den Sicherheitsbetrieb benötigt werden. Dies schließt nicht nur Server, PCs, Peripheriegeräte und alle damit verbundenen Betriebssysteme mit ein, sondern auch Datenbanken sowie Anwendungs- und Sicherheitssoftware. Zu den zusätzlichen Hardware- und Softwareprodukten, die für die Aufrechterhaltung des Sicherheitsbetriebs benötigt werden, gehören System- und Netzwerkverwaltungs-Tools, Helpdesk-Systeme, integrierte Verwaltungskonsolen sowie wissensorientierte Verwaltungssysteme und Software.

Für das Outsourcing ist je nach Ansatz und Technologie des MSSP die Liste der unterstützten Sicherheitstechnologien begrenzt. Einige MSSPs verwalten nur bestimmte Sicherheitstechnologien. In einigen Fällen macht der MSSP die Anschaffung einer bestimmten Sicherheitstechnologie oder den Austausch der implementierten Unternehmenstechnologie durch die Sicherheitstechnologie des MSSP zur Bedingung. Andere MSSPs wiederum machen die Anschaffung von zusätzlichen spezifischen oder unternehmenseigenen Technologien für die Protokollierung, Ereignisaufzeichnung, Analyse und Filterung zur Auflage.

Lizenzkosten

Die Kosten aller Softwarelizenzen, einschließlich Patches, Updates und neuer Softwareversionen, sollten auf den erwarteten Lebenszyklus der Software hochgerechnet werden.

Wartung

Wartungsgebühren für Software und Ausrüstung müssen in die Kalkulation der Total Cost of Ownership (TCO) einbezogen werden. Die Softwarewartung schlägt im Allgemeinen mit 15 bis 25 Prozent der jährlichen Softwarekosten zu Buche. Ein Unternehmen, das Softwarelizenzen im Wert von 1 Million US-Dollar besitzt, bezahlt 150.000 US-Dollar an Wartungskosten (untere Preisklasse). Jedes Unternehmen sollte sich demnach ein sehr genaues Bild davon machen, welche Supportleistungen es im einzelnen hierfür erhält. Bestimmte Managed Security Services-Verträge bieten 8 bis 10 Stunden Betreuung und Unterstützung, während andere Unterstützung rund um die Uhr (24x7) bieten.

MITARBEITER

Die Auswahl und Stellenbesetzung mit Sicherheitstechnikern ist oftmals der wichtigste, schwierigste und kostspieligste Faktor eines effektiven Security Management-Programms. Die Einstellung und langfristige Verpflichtung fachkundiger Sicherheitstechniker ist dabei eine der größten Herausforderungen. Zu den Personalbeschaffungskosten gehören nicht nur die Gehälter, sondern andere zusätzliche Arbeitsentgelte (Bonuszahlungen, Aktienoptionen), Anzeigen- und Ausrüstungskosten sowie Kosten für Weiterbildung und Schulung. Die Gehälter für Sicherheitsadministratoren und Sicherheitstechniker variieren je nach Standort, Fachwissen und Erfahrung. Einer von InformationWeekresearch.com durchgeführten Umfrage zufolge beträgt das Jahresdurchschnittsgehalt eines Sicherheitstechnikers (keine Management-Ebene) in Dallas, Texas, in der oberen Gehaltsklasse US$ 88.375, im mittleren Bereich US$ 71.750 und auf der unteren Ebene US$ 64.000.

obere Gehaltsklasse	mittlere Gehaltsklasse	untere Gehaltsklasse
$88.375	$71.750	$64.000

Wenn ein Unternehmen mit einer regulären Betriebszeit von 8:00 bis 17:00 Uhr seinen Sicherheitsbetrieb auf Unterstützung rund um die Uhr (24x7) ausweiten will, muss es, um 365 Tage im Jahr präsent zu sein, die Besetzung mehrerer Schichten in Erwägung ziehen:

- Schicht 1 - Frühschicht
- Schicht 2 – Nachmittags-/Spätschicht
- Schicht 3 – Spätabendschicht/Nachtschicht bis zum frühen Morgen
- Schicht 4 – Wochenendschicht und Besetzung während der arbeitsfreien Zeit der Schichten 1, 2 und 3

Für die Besetzung eines Arbeitsplatzes in einem 24x7-Sicherheitsbetrieb würden demnach mindestens vier Mitarbeiter benötigt. Darüber hinaus müssten diese zusätzlichen Mitarbeiter ein breitgefächertes Fachwissen oder eine entsprechende Spezialisierung in unterschiedlichen Sicherheitsbelangen aufweisen.

Personalbeschaffung

Aufgrund der hohen Mitarbeiterfluktuation im IT-Sektor müssen Unternehmen auch die Einstellungskosten in ihre Kalkulation einbeziehen. Ganz gleich, ob eine betriebseigene Personalabteilung oder externe Agentur für die Personalbeschaffung zuständig ist, können die Einstellungskosten bis zu 20 und 30 Prozent der jährlich anfallenden Gehaltskosten für die zu besetzenden Stellen betragen.

Aus- und Weiterbildung

Die Aus- und Weiterbildung von Sicherheitstechnikern spielt für die Vertiefung der vorhandenen Kenntnisse eine wichtige Rolle. Eine noch wichtigere Rolle spielt sie jedoch für die laufende Unterweisung der Mitarbeiter in die sich ständig wandelnden und schnell voranschreitenden neuen Technologien. Die Weiterbildung muss sich mit den neuesten Angriffsmethoden, Sicherheits-Tools und -Technologien und einer Vielzahl an Schutzstrategien befassen. In diesem Bereich treten folgende Kosten auf:

- Produkt- oder Technologieschulungen
- Schulung in der allgemeinen Sensibilisierung für Sicherheitsbelange
- Seminare für die Vorbereitung auf Zertifizierungen
- Zertifizierungskosten
- Besuch der wichtigsten Sicherheitskonferenzen und -messen
- Bücher, Fachzeitschriften, Abonnements, Fachmagazine oder Online-Schulungen, die es Sicherheitstechnikern ermöglichen, sich hinsichtlich neuester Technologien, Tipps, Techniken, Bedrohungen und Schutzmaßnahmen auf dem aktuellen Stand zu halten.

Im Allgemeinen erstellen Unternehmen genaue Richtlinien für die Anzahl der Schulungen, die ein Mitarbeiter pro Jahr absolvieren darf bzw. kann. Das Minimum ist dabei häufig zwei Wochen, oftmals sind jedoch weitere Schulungen erforderlich. Die meisten Sicherheitsseminare dauern eine Woche, jeder Mitarbeiter ist demnach berechtigt, an zwei Sicherheitsseminaren pro Jahr teilzunehmen. Da die Kosten für eine Schulung 1500 bis 3000 US-Dollar betragen, schlagen sie pro Mitarbeiter jedes Jahr mit jeweils 5000 US-Dollar zu Buche.

EINRICHTUNGEN

Security Operations Center

Die Kosten für den Aufbau und die Besetzung eines 24x7-Sicherheitsbetriebs können extrem hoch sein. Unter dem Kostenaspekt verbietet sich für die meisten Unternehmen der Aufbau oder das Leasing eines Security Operations Center (SOC), da die Investitionsausgaben hierfür mehr als 100 Millionen US-Dollar betragen können[iii]. Wenn es bereits Einrichtungen gibt, die für Security Management- und Security Monitoring-Aufgaben etabliert wurden oder verfügbar sind, betragen die Ausbaukosten für ein SOC von akzeptabler Größe mit ca. 30 Arbeitsplätzen bis zu 1 Million US-Dollar. Addiert man diese Kosten zu den Aufwendungen für die erforderliche Ausrüstung, Redundanz, Stromversorgung, Klimatisierung und Feuerschutzsysteme für redundante Hochverfügbarkeitssysteme hinzu, so werden sie für viele Unternehmen untragbar.

Überlegungen zu den Security Management-Optionen

GEGENÜBERSTELLUNG INTERNER UND EXTERNER SECURITY MANAGEMENT-LÖSUNGEN

Angesichts der immensen Herausforderungen, mit denen Unternehmen und der Markt allgemein konfrontiert werden, überrascht es niemanden, dass Unternehmen nach Alternativen suchen. Abgesehen von den niedrigeren Kosten profitiert ein Unternehmen schon allein beim Abschluss eines professionell verwalteten Servicevertrags, der ein Team engagierter und erfahrener Sicherheitstechniker einschließt, von beachtlichen Vorteilen. Durch die Zusammenarbeit mit einem erfahrenen und etablierten MSSP lässt sich das Risiko von Cyber-Bedrohungen reduzieren. Höhere Schutzstufen, 24x7-Bereitschaft und ein solideres Sicherheitsfundament sind vielleicht die wichtigsten Vorteile, von denen ein Unternehmen profitieren kann. Einige Beispiele für diese positiven Aspekte werden in der unten angeführten Tabelle aufgezeigt.

	Traditionelle Softwarelizenz	Managed Security Services-Anbieter
Einstiegskosten	Hoch	Niedrig
Installation und Implementierung	Setzt betriebsinterne Ressourcen voraus	MSSP übernimmt Implementierung
Amortisation	Lang	Kurz
Fachkräfte	Das Unternehmen muss Fachkräfte einstellen, schulen und langfristig an das Unternehmen binden	MSSP stellt Fachkräfte zur Verfügung
Sicherheitsrisiken	Das Unternehmen übernimmt das gesamte Risiko	MSS-Partner übernimmt Mitverantwortung für Betriebsrisiken
Effizienz und Effektivität	Eingeschränkte Skalierbarkeit wirkt sich auf Effizienz und Effektivität aus	Größere Effizienz via Skalierbarkeit als Merkmal von SOC-Operationen
Sicherheitsfundament	Abhängig von Fachwissen interner Mitarbeiter, internen Abläufen, Reaktionszeiten, Sicherheitsanfälligkeit	Optimierung durch garantierte Bereitschaft und Expertenwissen der internen Mitarbeiter, kurze Reaktionszeiten, Forschung im Bereich der Sicherheitsanfälligkeit und die kumulative Erfahrung eines MSS-Teams
Reaktion	Abhängig von Fachwissen interner Mitarbeiter, internen Abläufen, Reaktionszeiten, Sicherheitsanfälligkeit	24x7-Schutz, Warnmeldung bei kritischen Vorfällen und auf die Problemstufe bezogene Gegenmaßnahmen

BEISPIEL: GEGENÜBERSTELLUNG DER KOSTEN EINER INTERNEN UND EXTERNEN MANAGED SECURITY-LÖSUNG

Bei der Betrachtung der Ausgaben und Kosten, die einem mittelständischen[iv] Unternehmen im Rahmen eines zweijährigen Programms für das betriebsinterne Security Management im Unterschied zum externen Security Management entstehen, sollten auch die Vorteile und Einsparungen eines mehrjährigen Managed Service-Vertrags für den gesamten Zeitraum berücksichtigt werden. In einigen Fällen können die Einsparungen im ersten Jahr bedeutend höher liegen als in den Folgejahren, was sich auf wachsende oder sich ändernde Sicherheitsanforderungen zurückführen lässt.

UNTERNEHMENSPROFIL Das Unternehmen Sand Pharmaceuticals hat bei der Entdeckung neuer Krankheitsbilder und Behandlungsmethoden für schwere Krankheiten Pionierarbeit geleistet und nimmt nun weltweit eine Vorreiterrolle ein. Das Unternehmen beschäftigt insgesamt 3000 Mitarbeiter. In der IT-Abteilung arbeiten 40 Mitarbeiter, von denen fünf ausschließlich für die Verwaltung der Informationssicherheit zuständig sind. Sand Pharmaceuticals hat zum optimalen Schutz des Unternehmens drei Firewalls implementiert und mit der Installation eines Intrusion Detection-Systems (IDS) begonnen. Des Weiteren wird ein netzwerkbasiertes IDS für sechs Netzwerksegmente und ein permanent aktiviertes (24x7) hostbasiertes IDS auf 10 unternehmenskritischen Servern benötigt.

Vorteile von Managed Security Services

Für die Unterstützung eines reibungslosen Betriebsablaufs sind Unternehmen auf Informationsaustausch angewiesen. Mit der Zunahme komplexer Bedrohungen und der Verbreitung ausgefeilter Angriffsmethoden sehen sich Unternehmen heute mit ernst zu nehmenden Risiken konfrontiert, die es beispielsweise vor fünf Jahren noch gar nicht gab. Viele Unternehmen besitzen weder die Ressourcen noch haben sie den Wunsch, ein Vollzeit-Security-Team zu beschäftigen, das diesen Sicherheitsbedarf deckt. Somit wird die Suche nach alternativen Lösungen immer interessanter.

Ein adäquat qualifizierter MSSP (Managed Security Services Provider) kann einem Unternehmen folgende Vorteile bieten:

Verbesserter Informationsschutz

Die Sicherheitsanforderungen, die heutige moderne Netzwerke und Informationssysteme erfüllen müssen, sind weitaus komplexer und von weitaus kritischerer Bedeutung als noch vor wenigen Jahren. Denn die Methoden und Technologien, mit deren Hilfe Hacker in Unternehmenssysteme eindringen, werden in kürzester Zeit technisch immer ausgereifter. Wenn ein Unternehmen seine Sicherheitsbelange nicht zur obersten Priorität macht, wird es sich im Hinblick auf die Bereitstellung eines umfassenden, stabilen Security Management-Programms eindeutig im Nachteil befinden.

Der Zeitaufwand ist dabei nicht zu unterschätzten. Doch nur durch umfassende Schulungen können sich die Mitarbeiter das erforderliche Expertenwissen aneignen, um mit den neuesten Strategien für den Informationsschutz Schritt zu halten.

Nutzung des kumulativen Fachwissens und der gesammelten Erfahrungen der Sicherheitsexperten

Das Fachwissen der MSSP-Sicherheitsanalysten und -Ingenieure, die sich ausschließlich mit der Verwaltung und Überwachung von Sicherheitseinrichtungen beschäftigen, ist eine wertvolle Ressource. Diese Experten müssen tagtäglich auf alle möglichen Sicherheitsbedrohungen und Angriffe reagieren. Dies bedeutet, dass sie für Sicherheitsbelange weitaus stärker sensibilisiert sind und Angriffe auf die Unternehmenssicherheit besser als betriebsinterne Mitarbeiter abwehren können.

Kenntnisse der neuesten Entwicklungen und Techniken im Sicherheitsbereich

Jeder MSSP eines Unternehmens sollte eine Forschungsgruppe damit beauftragen, sich über die neuesten Cyber-Bedrohungen, Schwachstellen, Hacker-Techniken und Entwicklungen im Sicherheitsbereich zu informieren, um mit ihnen Schritt zu halten. Die konstante Überwachung von Sicherheitswarnungen und -informationen ist wichtig, um einen optimalen Schutz vor Sicherheitsbedrohungen gewährleisten zu können.

Geteilte Verantwortung mit einem bewährten Sicherheitspartner

MSSPs bieten Service-Vereinbarungen mit unterschiedlichen Leistungspaketen an, die innerhalb eines festgelegten Zeitraums in Anspruch genommen werden können. In ihrem Portfolio bieten die Managed Security Services darüber hinaus noch weitere zusätzliche Leistungen, welche die Folgen möglicher Sicherheitsverletzungen abschwächen, die Haftbarkeit reduzieren und Unternehmen insgesamt ein größeres Gefühl der Sicherheit geben. Zusätzlich hierzu stellen MSSPs ein fundiertes Sicherheits-Fachwissen zur Verfügung, das sich durch Erfahrung auf dem Gebiet der Intrusion Detection und bei der Reaktion auf Sicherheitsvorfälle auszeichnet. Als Sicherheitspartner des Unternehmens teilt sich ein MSSP mit diesem die Last und auch die Verantwortung für das Security- und Reaktions-Management.

Zuverlässiges Sicherheits-Management rund um die Uhr

Ein Managed Security Services Provider sollte Rund-um-die-Uhr-Schutz für die wichtigsten Unternehmenssysteme bieten. Dadurch wird der Schutz des gesamten Datenbestandes gewährleistet, was vor allem in permanent verbundenen Geschäftsumgebungen eine wichtige Rolle spielt. MSSPs überwachen die Netzwerke und Infrastruktur ihrer Kunden, um genau in jenen Stunden alles abzusichern, in denen erfahrungsgemäß die meisten Hacker angreifen. Dies bedeutet auch, dass die Mitarbeiter des Unternehmens wertvolle technische Ressourcen für unternehmenskritische Projekte freigeben können, von denen ein höherer Investitionsgewinn zu erwarten ist.

Maximale Nutzung bereits vorhandener Sicherheitsprodukte.

Viele Unternehmen investieren in Sicherheitsprodukte, die nie vollständig implementiert werden. Ein qualifizierter Managed Security Services Provider sorgt dafür, dass gekaufte Lösungen installiert, implementiert und integriert werden, damit das Unternehmen den vollen Wert seiner getätigten Investitionen erhält.

Entscheidung für ein wirtschaftliches Security Management.

Wird ein MSSP zum Schutz für unternehmenskritische Datenbestände beauftragt, lassen sich hohe Personalkosten für die Einstellung, Schulung und langfristige Bindung von Sicherheitstechnikern an das Unternehmen vermeiden. Der Einsatz von Managed Security Services reduziert dabei die Total Cost of Ownership (TCO), denn die Personalkosten werden nun zu einer variablen Größe. Da Managed Services auch monatlich in Rechnung gestellt werden, lässt sich das Sicherheitsbudget besser planen und verwalten.

Auswahl eines Managed Security Services Providers

Obwohl die Kostenprognose ein wichtiger Faktor ist, spielt sie mitunter nur eine relativ untergeordnete Rolle bei der Gesamtbeurteilung eines Managed Security Services Providers. Weitere Schlüsselfaktoren, die von den Unternehmen bei der Auswahl eines MSSPs berücksichtigt werden sollten, sind:

ANBIETERANALYSE – LANGFRISTIGE UNTERNEHMENSSTABILITÄT

Laut Gartner wurden bereits mehr als 1 Milliarde US-Dollar Risikokapital in Startup-MSSPs investiert[v]. Von diesen Startup-Unternehmen werden viele nicht überleben, und bis zur Beruhigung des Marktes wird es zahllose Fusionen und Akquisitionen geben. Aus diesem Grund kann kein Unternehmen darauf verzichten, die notwendigen Vorsichtsmaßnahmen zur gründlichen Analyse potenzieller MSSPs zu ergreifen. Jedes Unternehmen sollte sich gründlich informieren und Dokumente sowie andere Informationen anfordern, die das Leistungsangebot, Erfahrungen und Erfolge eines Anbieters auf folgenden Gebieten untermauern:

- Finanzielle Stabilität
- Dauer der Geschäftstätigkeit
- MSS-Erfahrung
- Kunden
- Unternehmensimage

LEISTUNGSSPEKTRUM

Ein Unternehmen, das sich über unterschiedliche MSSPs informiert, sollte auch auf Folgendes achten:

- Vorgehensweise bei der Implementierung der Managed Security Services
- Technologien, Stärken und Schwächen im Security Services-Umfeld
- Fachwissen der MSSP-Mitarbeiter

Als weiterer wichtiger Punkt sollte unbedingt darauf geachtet werden, ob das Angebot des MSSPs flexibel und vielseitig genug ist, um dem aktuellen und künftigen Bedarf des eigenen Unternehmens zu entsprechen. Für die Beurteilung der Management-, Überwachungs- und Reaktionstechniken des MSSPs ist die Beantwortung folgender Fragen relevant:

- Welche Produkte und welche Technologie unterstützt der MSSP?
- Welche Maßnahmen ergreifen die MSSP-Mitarbeiter in Notfallsituationen?
- Ist der MSSP in der Lage, geeignete Mitarbeiter einzustellen und langfristig an sich zu binden?
- Stehen dem MSSP ausreichende Mittel zur Verfügung, um bei Bedarf spezialisierte Berater zu beauftragen?
- Sind die Service-Stufen-Vereinbarungen aufeinander abgestimmt und flexibel?

UNTERNEHMENSUNTERSTÜTZUNG

Um sich ein Bild davon zu machen, in welchem Umfang ein MSSP Unternehmensunterstützung leisten kann, sollte man sich auf jeden Fall über Folgendes informieren:

- Hat der MSSP Zugang zu einem SOC oder besitzt er ein eigenes SOC?
- Wie sieht seine Einstellungspraxis aus?
- Wie verpflichtet er Mitarbeiter langfristig und wie sieht die Gehaltsstruktur aus?
- Wie wird die Vertraulichkeit von Kundeninformationen gewährleistet?

Auch die Forschungs- und Entwicklungsabteilungen der MSSPs und die Finanzierung dieser Bereiche sollten in den Fragenkatalog für die Auswahl eines MSSP aufgenommen werden:

- Wie halten die MSSP-Mitarbeiter mit den neuesten Trends der IT-Industrie Schritt?
- Welche speziellen Kenntnisse und welches Sicherheits-Fachwissen besitzen die MSSP-Mitarbeiter?

PROFIL DER SYMANTEC MANAGED SECURITY SERVICES

Die Symantec Managed Security Services zeichnen sich durch zahlreiche Vorteile aus:

- Sicherheit ist das Kerngeschäft des MSSPs
- Langfristige finanzielle Stabilität ist nachgewiesen
- Umfassendes Paket mit MSS-Services
- Einsatz bewährter MSS-Richtlinien, -Standards und -Verfahren
- Angestellte und ausgebildete Sicherheitstechniker
- Ausgearbeiteter Plan für die Mitarbeiterschulung und für Karriereoptionen
- Mitarbeiterüberprüfung zur Gewährleistung der Vertrauenswürdigkeit
- Globaler 24x7-Betrieb mit ständiger Mitarbeiterbesetzung
- Mehrere redundante SOCs mit globaler Reichweite
- Fundiertes Fachwissen in der technischen Unterstützung und in der Sicherheitsunterstützung
- Fest zugeordnete Threat- und Schwachstellen-Forschungsgruppen
- Fest zugeordnetes Team pro Kunde
- Services unterstützen Produkte unterschiedlicher Anbieter
- Implementiert nach Bedarf Sicherheitslösungen
- Vertraglich festgelegte Übernahme von Sicherheitsrisiken und finanziellen Risiken
- Individuell zugeschnittene Service-Stufen-Vereinbarung
- Abwicklung von Vorfällen und Reaktionskapazität

Zusammenfassung

Security Management setzt ein komplexes System aus Software, Hardware, Mitarbeitern und Fachwissen voraus. Ob Security Services nun betriebsintern besetzt werden oder ein externer Managed Security Services Provider beauftragt wird, ist eine Entscheidung, die am besten erst nach einer gründlichen Analyse der Einzeldaten getroffen werden sollte. Eine Entscheidung, die für ein Unternehmen genau richtig ist, mag für ein anderes Unternehmen die falsche sein. Die fundierte Überprüfung der Kosten spielt dabei eine wichtige Rolle. Allerdings stellt sie nur einen Teilaspekt in der Gesamtanalyse dar.

Weitere wichtige Entscheidungsfaktoren für die Wahl des "richtigen" MSSPs sind neben der Stellenbesetzung die Expertise des Anbieters, die Spezialkenntnisse im eigenen Unternehmen sowie die bereits vorhandenen Systeme wie Hardware, Software und Firewalls.

Quellenangaben/Hinweise

[i] Gartner Dataquest. "The U.S. Security Services Market Forecast, 2000–2005", 1. Juni 2001

[ii] Dinley, D. "Should outsourcing be part of your IT act?" InfoWorld Outsourcing Study, InfoWorld, 12. Februar 2001

[iii] Carey, Allan und Dean, Richard. "2001 Information Security Services: A Competitive Segmentation and Analysis," IDC, Juni 2001

[iv] Die Firma ist ein Beispiel für ein mittelständisches Unternehmen. Die Kostenannahmen sind geschätzt und jederzeit ohne vorherige Ankündigung änderbar.

[v] GartnerGroup Research Note. "Surviving the Managed Service Shakeout", 15. März 2001

ALS EINER DER WELTWEIT FÜHRENDEN HERSTELLER VON INTERNET-SICHERHEITSTECHNOLOGIEN BIETET SYMANTEC EIN BREITES SPEKTRUM AN SICHERHEITSLÖSUNGEN FÜR PRIVATANWENDER UND UNTERNEHMEN. DAS ANGEBOT VON SYMANTEC UMFASST LÖSUNGEN FÜR VIRENSCHUTZ, FIREWALLS UND VPN (VIRTUAL PRIVATE NETWORK), SCHWACHSTELLENANALYSE, INTRUSION DETECTION, FILTERPROGRAMME FÜR INTERNET- UND E-MAIL-INHALTE, TECHNOLOGIEN FÜR DIE FERNVERWALTUNG UND SICHERHEITS-SERVICES FÜR UNTERNEHMEN WELTWEIT. DIE NORTON-SICHERHEITSPRODUKTE VON SYMANTEC SIND HINSICHTLICH IHRER VERKAUFSZAHLEN MARKTFÜHREND UND ERHALTEN AUSZEICHNUNGEN WELTWEIT. SYMANTEC VERFÜGT ÜBER NIEDERLASSUNGEN IN 38 LÄNDERN.

WEITERE INFORMATIONEN ERHALTEN SIE UNTER WWW.SYMANTEC.DE ODER WWW.SYMANTEC.COM.

WORLD HEADQUARTERS:
20330 Stevens Creek Blvd.
Cupertino, CA 95014 U.S.A.
001-408-253 9600
001-800-441 7234

DEUTSCHLAND:
Symantec (Deutschland) GmbH
Kaiserswerther Str. 115
D - 40880 Ratingen
Tel.: +49 (0) 69-6641 0315
E-Mail: enterprise.deutsch@symantec.com

ÖSTERREICH:
Symantec GmbH
Wipplingerstraße 34
A -1010 Wien
Tel.: +43 (0)1- 532 85 33-0
E-Mail: infolineaustria@symantec.com

SCHWEIZ:
Symantec Switzerland AG
Grindelstrasse 6
CH - 8303 Bassersdorf
Tel.: +41 (0) 1-838 49 00
Fax: +41 (0) 1-838 49 01
E-Mail: infoline@symantec.com

Symantec hat Niederlassungen in 38 Ländern. Adressen und Telefonnummern der Symantec-Niederlassungen in anderen Ländern finden Sie auf unseren Websites: www.symantec.com oder www.symantec.de