



IT-Grundschutz

Informationsdienst

Workshops

**Daten schützen,
Prozesse
automatisieren,
Kosten
kontrollieren**

Seite 3



Quelle: iStockphoto/Sergey Ilin

NEWS

Passwörter raus aus dem Programmcode *Seite 2*

Anzahl neuer Computerschädlinge auf Rekordniveau *Seite 2*

Information Security Solutions Europe (ISSE) in Berlin *Seite 2*

Rubriken

Editorial *Seite 2*

Impressum *Seite 15*

Praxis und Anwendungen

Grundlagen von Managed Security Services *Seite 3*

Zugriffslisten automatisch aktualisieren *Seite 9*

Workshops

Daten schützen, Prozesse automatisieren, Kosten kontrollieren *Seite 6*

Ratgeber: Outsourcing und Informationssicherheit *Seite 11*

 **Der schnellste Weg zur IT-Sicherheit**
it-sa Nürnberg
Die IT-Security Messe
19.-21.Okt. 2010

Sicherheit in fremden Händen

Grundlagen von Managed Security Services

Guido Moezer, Product Manager Support & Managed Services, Integralis

IT-Sicherheitsbeauftragte müssen ständig mit neuen Bedrohungen, gesetzlichen Regelungen und internen Maßgaben zurande kommen. Dabei können auch große Unternehmen an ihre Grenzen stoßen. Managed Security Services sollen Firmen in dieser Situation unterstützen und entlasten.

Laut Definition sind Managed Security Services ein systematischer Ansatz, um die Sicherheitserfordernisse eines Unternehmens zu regeln. Dieser Service kann im eigenen Haus durch einen Dienstleister erfolgen, aber auch an einen Service Provider ausgelagert werden. Zu den Aufgaben eines Managed Security Service können zahlreiche Kategorien gehören: Von der Rund-um-die-Uhr Überwachung der IDS/IDP Systeme und Firewalls über Patch-Management und Security-Audits bis hin zur Intervention bei Störfällen. Dies ist besonders für Kunden interessant, die selbst kein Personal mit ausreichender Qualifizierung oder in ausreichender Besetzung bereithalten können, um diese Aufgaben zu übernehmen.

Managed Security Services (MSS) bieten die Möglichkeit, eigene Ressourcen mit den Leistungen eines Partners zu ergänzen, der mehr technische Möglichkeiten, mehr Personal und 24x7-Services besitzt. Ein Managed Security Service Provider (MSSP) verfügt im Idealfall über ein breit gefächertes Portfolio an Unterstützungsleistungen für die wichtigsten Sicherheitsaspekte sowie über eine Auswahl an Herstellern von Sicherheitstechnologien. Er bietet Verfügbarkeitsüberwachung, Auswertung von Protokolldaten (Logdaten) auf Sicherheitsvorfälle, Log-Management oder auf Wunsch Regelbasis- und Plattform-Management (Change Management). Je nach Grundlage der Überwachung sollte bei einer Auswertung der Protokolldaten auf Sicherheitsvorfälle auch ein Störfall-Management (Incident-Management) angeboten werden. Diese Bausteine kann der Kunde individuell nach Bedarf und vorhandener Technik kombinieren. Die erbrachten Leistungen sind häufig durchgehend verfügbar und mit Service Level Agreements (SLAs) abgesichert.

Um die eingesetzte Technik optimal auf die Sicherheitsanforderungen des einzelnen Kunden auszurichten, ist sie häufig im Netz des Kunden selbst installiert und speziell für diesen konfiguriert. Auch bei MSS ist es möglich,

Outsourcing, Outtasking oder Co-Sourcing zu betreiben, dabei sollten die Vorgaben für Outsourcing jedoch berücksichtigt werden und die Oberhoheit über die eigenen Sicherheitsvorgaben in der Hand des Kunden bleiben (siehe Artikel zu Outsourcing auf Seite 11).

Ein MSSP muss über eine stabile, skalierbare und erprobte Infrastruktur verfügen und diese auf Nachfrage auch nachweisen können. Idealerweise verfügt der MSSP über mehrere Security Operation Center (SOC), verteilt in verschiedene Zeitzonen, so dass kein Single Point of Failure in der Leistungserbringung auftreten kann. Dies verringert die Gefahr, dass beispielsweise eine Pandemie massive Ausfälle bei den Serviceleistungen verursacht. Die Überwachung und Auswertung der Protokolldaten erfolgt jedoch weiterhin im Netz des Kunden.

Die Ergebnisse der einzelnen Auswertungen werden über eine sichere Verbindung an die SOC übermittelt und dort für einen Überblick zusammengefasst. Auf diese Weise lässt sich umgehen, dass das Netzwerk und die Internetverbindungen unnötig mit dem Transport von Rohdaten belastet werden. Für die Datenübertragung zwischen den Datensammlern (die auch die Vorortanalyse durchführen) und den SOCs kann zusätzlich eine Out-of-Band Verbindung eingerichtet werden, sollte der primäre Transportweg unterbrochen sein.

Um den Kunden zuverlässig unterstützen zu können und um die IT-Verbindungen zwischen Kunde und Dienstleister auf ein Minimum zu reduzieren, sollte der MSSP die gleiche Vorortinfrastruktur und somit die gleichen sicheren Verbindungen nutzen. Je nach Anforderungen der Betriebsleistungen sind dabei Remote-Management-Kits als Ergänzung denkbar. Damit kann auf Video, Tastatur und Maus des zu administrierenden Systems zugegriffen werden. Auch lässt sich über solche Remote-Management-Kits ein System komplett vom Stromnetz trennen, um es bei Bedarf zu booten oder neu zu konfigurieren.

Egal wie modern die Technik ist – Hardware wird immer irgendwann ausfallen. Das Austauschsystem muss in diesem Fall auf den Konfigurationsstand des Originalsystems gebracht werden. Dies lässt sich leichter und schneller bewerkstelligen, wenn durch den MSSP regelmäßig Sicherungen der Konfigurationen durchgeführt und aufbewahrt werden.

Bedrohungen im Vorfeld ausfiltern

Einige IT-Sicherheitstechnologien sind mittlerweile soweit standardisiert, dass sie durch Cloud Technologien sicher und zuverlässig erbracht werden können, ohne dass dazu der Einsatz von eigener Hard- und Software notwendig ist. Typische Beispiele sind Email- und Web-Security sowie Schwachstellenscanner, die öffentlich erreichbare IP-Adressen überprüfen.

Solche Services können Internet-Leistungen wie E-Mail oder Web-Zugriff absichern, die grundsätzlich unverschlüsselt übertragen werden. Ein solcher Managed Secu-

Guido Moezer,
Product Manager
Support & Managed
Services, Integralis



rity as a Service (MSaaS) widerspricht trotzdem nicht den oben genannten Sicherheitsgedanken. Sie stellen einen idealen Filter für Spam, Viren, Malware oder ähnliche Bedrohungen dar, die abgefangen werden, bevor sie Gateways und Systeme des Unternehmens belasten. Die Vorteile dieser MSaaS-Technologie sind:

- Schutz vor ungewollter Schadsoftware
- Schutz vor Spam
- Entlastung von Internetbandbreite, WAN-Verbindungen und Gateways
- Keine Vorinvestition in Hardware, Software und Lizenzen
- Keine Vorhaltung von ungenutzten Kapazitäten
- Abrechnung anhand von Verbrauch

Der Servicekatalog

Ein Servicekatalog ist eine übersichtliche Darstellung aller verfügbaren Serviceleistungen und deren Eingruppierung in Technologien. Ein MSSP sollte heute mindestens die folgenden Dienste anbieten und die wichtigsten Hersteller für diese Bereiche abdecken:

Managed Perimeter Security Devices

Mit Perimeter Security Devices sind Firewalls, SSL- und VPN-Gateways gemeint, die den Eingang und Ausgang des Netzwerks zum Internet oder Partnernetzwerk absichern.

Managed Intrusion Detection & Prevention Devices

Mit Intrusion Detection & Prevention Devices sind die Vertreter von Technologien gemeint, die eine Ana-

lyse von Netzwerkdaten in Echtzeit vornehmen. Sie sollen Anomalien, Ausbrüche von Schadsoftware oder typische Angriffsszenarien erkennen und bei Bedarf den zuständigen Mitarbeiter alarmieren oder automatisch Gegenmaßnahmen einleiten.

Managed Content Security Devices

Content Security Devices untersuchen E-Mail und HTML-Daten auf Schadsoftware, Spam und andere unerwünschte Inhalte und unterbinden gegebenenfalls den Transport in das Kundennetzwerk.

Managed Authentication Devices

Authentication Devices sind Systeme, die Anmeldevorgänge durch den Einsatz von zwei Faktor-Authentifizierung absichern und somit die Identität des Anmelders überprüfen.

Managed Threat & Vulnerability Scans

Threat & Vulnerability Scanner überprüfen Netzwerkgeräte wie File-Server, Datenbanken, Web-Server oder ähnliches regelmäßig auf bekannte Schwachstellen. Sie sollen sicherzustellen, dass diese auf dem notwendigen Patch-Level sind oder keine ungewollten Zugangsmöglichkeiten entstanden sind. Solche Schlupflöcher können durch unachtsame Administration oder das Einspielen neuer Software entstehen.

Managed Network Infrastructure Devices

Network Infrastructure beinhaltet alles, was zum Aufbau eines IT-Netzwerkes gehört, also Router, Switches, Load-Balancer, DNS-Server, DHCP-Server, WAN-Optimierer und ähnliche Geräte.

In all diesen Bereichen gibt es etablierte Lösungsanbieter. Der MSP bietet die Produkte der wichtigsten Hersteller an und kann sie an die Bedürfnisse der Kunden anpassen.

Umfang des Angebots

Folgende Liste enthält die üblichen Angebote eines MSSP. Sie unterteilt sich in die Bereiche Monitoring und Alarming sowie Betrieb. An ihr kön-

nen sich potenzielle Interessenten für Managed Security Services einen Überblick verschaffen, welche Aufgaben vom Provider wahr genommen werden sollten. Zum Monitoring und Alarming gehören:

- Aktive Überwachung der Systemvitalfunktionen wie Prozessor, Festplatte, Speicher, Schnittstellen und ähnliches
- Systemfunktions- und Verfügbarkeitsüberwachung
- Trendanalyse
- Auswertung von Protokolldaten auf Sicherheitsvorfälle
- Archivierung der analysierten Informationen
- Archivierung von Protokolldaten für spätere forensische Auswertung und Dokumentation
- Korrelation der analysierten Informationen, erkennen von verdächtigen Vorgängen
- Erkennung von Anomalien
- Security Reporting
- Key Performance Indikator Reporting
- Compliance Reporting
- Alarmierung von Verantwortlichen
- Dashboard
- Backup von Konfigurationen (und deren Bereitstellung im Bedarfsfall)

Zum Betrieb rücken andere Faktoren in den Vordergrund:

- Umsetzung von Konfigurationsänderungen auf Kundenwunsch
- Installation von Patches und Updates
- Aktives Eingreifen zur Aufrechterhaltung des Sicherheitsniveaus
- Funktionswiederherstellung nach Systemaustausch
- Service Review Meetings und Beratung zur Sicherheitsoptimierung

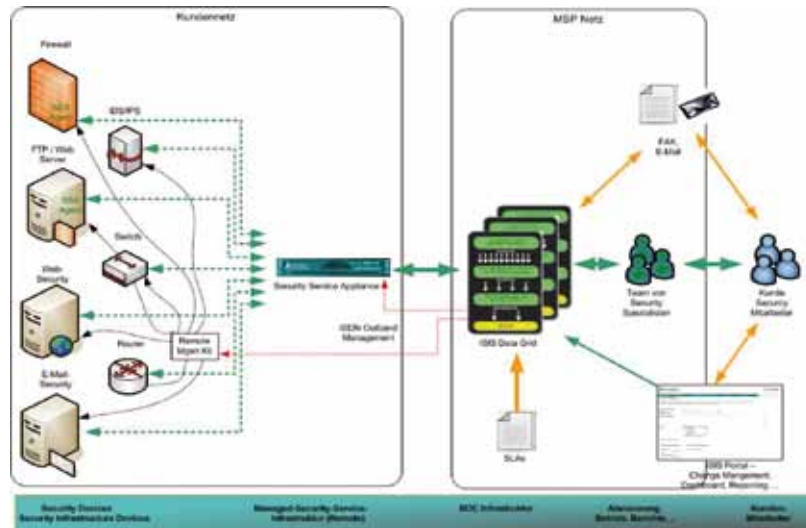
Je nach Anforderung des Kunden ist vorher vertraglich festzulegen, wann und mit welchen Reaktionszeiten diese Leistungen zur Verfügung stehen sollen. Im Prinzip stellen die oben genannten Überwachungs- und Alarmierungsmerkmale die Funktionen eines gema-

nagten SIEM (Security Information and Event Management) Systems dar. Jeder Kunde hat einen anderen Bedarf an Services und wird nicht immer alle Parameter in der gleichen Ausprägung benötigen. Nützlich ist es, wenn der MSSP auf veränderte Ansprüche seiner Kunden flexibel reagieren kann. Allerdings lässt sich nur selten jeder Service zu jedem Produkt eines Herstellers durch den MSSP realisieren.

Unternehmen, die bereits ihre IT-Services ausgelagert haben, werden darüber nachdenken, ob sie für ihre MSS den gleichen Anbieter verwenden. Die meisten großen Anbieter in der Branche haben beide Dienstleistungen im Portfolio. Eine Empfehlung der Yankee Group lautet, die beiden Sparten lieber zu trennen. So ist gewährleistet, dass es nicht zu Interessenkonflikten, zum Beispiel zwischen Kundenservice und Sicherheitsanforderungen, kommt.

Tipps zum Projektablauf

Wie bei allen Sicherheitsprojekten empfiehlt es sich auch bei der Auslagerung an einen MSS, die eigene Sicherheitsrichtlinie zum Maß aller Dinge zu machen. Sie ist Grundlage dafür, mit welchem Anbieter man zusammenarbeitet und welche Dienste ausgewählt werden.



Mögliche MSS-Infrastruktur und deren Verbindung mit dem Netz des Kunden

Wer über ein IAM verfügt, muss die im Unternehmen niedergelegten Rollen um die Rechte und Rollen erweitern, die dem außerhäusigen Sicherheitspersonal zugewiesen werden. Für einen reibungslosen Projektlauf ist es unabdingbar, jederzeit für eine ausreichende Personaldecke zu sorgen - für Vorbereitung, Durchführung und Nachbereitung der Auslagerung. Dies gilt für beide Seiten: Im Zweifelsfall ist es unter Umständen notwendig, wenn der Anbieter dem Unternehmen nachweisen kann, dass genug Personal für die kritische Zeit zur Verfügung steht, um Probleme schnell beheben zu können. Sobald die Auslagerung beendet ist und das Projekt läuft, ist regelmäßiges Monitoring zu empfehlen. Dabei

müssen nicht nur die technischen Daten, sondern auch die entstehenden Kosten überwacht werden. Fallen immer wieder zusätzliche Kosten für besondere Dienste jenseits des im Vertrag niedergelegten Budgets an, kann dies ein Hinweis sein, dass der Service-Vertrag nachverhandelt werden muss. Auch intern müssen klare Regeln für die nun ausgelagerte Sicherheitstechnik kommuniziert werden. Wenn der Service-Anbieter zum Beispiel zu zögerlich in neue Hard- oder Software investiert, als es der interne IT-Manager für angebracht hält, ist es wichtig, dass dies kommuniziert und die Reaktion darauf mit der Geschäftsführung abgestimmt wird, um unerwünschte Alleingänge zu verhindern. ■

Bankenkongress CIBI

5. Oktober 2010 in München

IT-Governance und
IT-Compliance Management
Session 4

www.cibi.de