Jens Nedon, Sandra Frings, Oliver Göbel (Hrsg.)

IT-Incident Management & IT-Forensics

Erste Tagung der Fachgruppe SIDAR der Gesellschaft für Informatik

24. – 25. November 2003 in Stuttgart, Deutschland

Gesellschaft für Informatik 2003

Lecture Notes in Informatics (LNI) - Proceedings
Series of the Gesellschaft für Informatik (GI)

Volume P-39

ISBN 3-88579-368-7
ISSN 1617-5468

Volume Editors
Jens Nedon
ConSecur GmbH
Schulze-Delitzsch-Strasse 2, D-49716 Meppen
Nedon@consecur.de
Sandra Frings
Fraunhofer-Institut für Arbeitswirtschaft und Organisation IAO
Nobelstraße 12, D-70569 Stuttgart
Sandra.Frings@iao.fhg.de
Oliver Göbel
RUS-CERT (Universität Stuttgart)
Breitscheidstr. 2, D-70174 Stuttgart
Goebel@CERT.Uni-Stuttgart.DE

printed by Köllen Druck+Verlag GmbH, Bonn

IT-Incident Management durch externe Dienstleistung – Die Lösung aller IT-Incident Management Probleme?

Roland Wagner

Internet/eSecurity-Systeme Datev eG
Paumgartnerstraße 6-14
D-90329 Nürnberg
Roland.Wagner@datev.de

Abstract: Aufbau, Organisation und Betrieb von IT-Incident Management-Prozessen erfordert einen hohen Aufwand an Personal und Ressourcen. Jede Organisation, die Security-Komponenten in ihrem Netzwerk betreibt, muss sich mit der Frage auseinander setzen, wie die anfallenden Datenmengen behandelt werden sollen. Die Spanne reicht von Ignoranz bis zur vollständigen manuellen Analyse jedes einzelnen Events, wobei letzteres aufgrund der Vielzahl von Meldungen sicherlich den Idealzustand darstellt. Bei all den dabei auftretenden organisatorischen, technischen und finanziellen Problemen stellt sich auch die Frage, inwieweit IT-Incident Management im eigenen Hause durchgeführt werden kann oder an einen externen Dienstleister vergeben werden soll. Mit der wachsenden Komplexität des IT-Netzwerkes, insbesondere durch eine steigende Anzahl von Security-Komponenten und die steigende Bedrohung aus dem Internet, wächst auch die Anzahl der sicherheitsrelevanten Meldungen. Diese Meldungsflut lässt sich nur noch durch automatisierte Werkzeuge beherrschen. Anhand einiger Beispiele von InHouse verwendbaren Software-Systemen mit ihren Vor- und Nachteilen soll die Möglichkeit aufgezeigt werden eine Reduktion der Meldungsflut zu erreichen. Bei allen diesen Software-Systemen ergeben sich Probleme, die dann zur Frage führen, ob nicht ein externer Dienstleister die Aufgabe besser erledigen könnte. Bei der Evaluierung verschiedener professioneller Dienstleistungen im Bereich „Managed Security Services“ (MSS) zeigen sich Stärken und Schwächen der einzelnen Anbieter. Durch theoretische Betrachtungen, Anforderungen im Betrieb und aus den praktischen Erfahrungen sowie Diskussionen mit den verschiedenen Anbietern ergibt sich dann ein Anforderungskatalog an ein externes MSS-Center, beziehungsweise an die Dienstleistung „Managed Security Service“ im Allgemeinen. Diese Anforderungen sollen – zunächst ohne Gewichtung – aufgezeigt werden. Danach findet eine subjektive Gewichtung statt, die sicherlich in vielen Punkten an die eigene Security-Policy der Organisation angepasst werden muss. IT-Incident Management umfasst Prozesse, die für jede Organisation unterschiedlich sind. Die im Titel gestellte Frage kann daher nicht universell beantwortet werden.

1 Motivation

Jede Organisation, die eine oder mehrere sicherheitsrelevante Techniken einsetzt, wird sich mit dem Problem des IT-Incident Managements auseinander setzen müssen. Immer mehr Systeme im IT-Netzwerk erzeugen sicherheitsrelevante Daten. Dazu zählen die Logfiles einer Firewall und Datenbanken mit Events aus dem host- oder netzwerk-

basierenden Intrusion Detection System. Aber auch Virenscanner oder Contentfilter liefern Daten in Form von Logfiles, Syslog oder Traps, die bearbeitet werden müssen. Bei vielen Firmen und Institutionen wird diese Aufgabe gar nicht oder nur sehr sporadisch durchgeführt. Eine Analyse von Logfiles oder die Auswertung von Events aus dem Intrusion Detection System bindet Ressourcen, die von den Systemadministratoren und Verantwortlichen anderweitig benötigt werden. Da Sicherheitskomponenten, die nicht überwacht werden und bei denen dann auch keine Alarmierung im Notfall erfolgt, nicht sehr sinnvoll sind, bleibt die Frage, ob diese Überwachung und Alarmierung im eigenen Hause realisiert oder an einen externen Dienstleister vergeben werden soll. Bei einer näheren Betrachtung von Werkzeugen für das IT-Incident Management und den technischen und organisatorischen Problemen führt dies dazu, sich näher mit externen Firmen zu beschäftigen, die eine Dienstleistung „Managed Security Service“ anbieten.

Wir betrachten zunächst in Kapitel 2 den Aufbau eines IT-Netzwerkes mit Sicherheitskomponenten so wie dies früher realisiert wurde oder heute bei wenig Anspruch an Sicherheit immer noch realisiert wird. Im Vergleich dazu ist ein modernes IT-Netzwerk heute mit einem hohen Anspruch an Sicherheit erheblich komplexer. Kapitel 3 zeigt dann anhand von Werkzeugen, wie die durch die komplexen Sicherheitstechniken erzeugte Meldungsflut an Informationen im eigenen Hause reduziert werden kann. Dies führt dann zu der Überlegung, die Überwachung der sicherheitsrelevanten Meldungen an einen externen Partner zu vergeben. Beispiele für solche Dienstleistungen werden in Kapitel 4 vorgestellt. Bei den Überlegungen zur Auswahl eines geeigneten Partners ergeben sich Fragen, die in Kapitel 5 zusammengefasst und in einer Bewertungstabelle aufgelistet werden. Bei entsprechender Konfiguration der Parameter und Anpassung an die eigene Security Policy soll diese Bewertungstabelle als Entscheidungskriterium für die Auswahl eines Dienstes dienen. Kapitel 6 fasst dann die gewonnenen Erkenntnisse zusammen.

2 Sicherheitsstruktur von IT-Netzwerken

Die Sicherheitsstruktur eines IT-Netzwerkes befindet sich in ständigem Wandel. Nahezu täglich werden nicht nur neue Sicherheitslücken, sondern auch neue Techniken zum Einbruch in Computernetze bekannt. Im folgenden Beispiel wird der Aufbau eines sehr einfachen IT-Netzwerkes betrachtet (Abbildung 2.1).

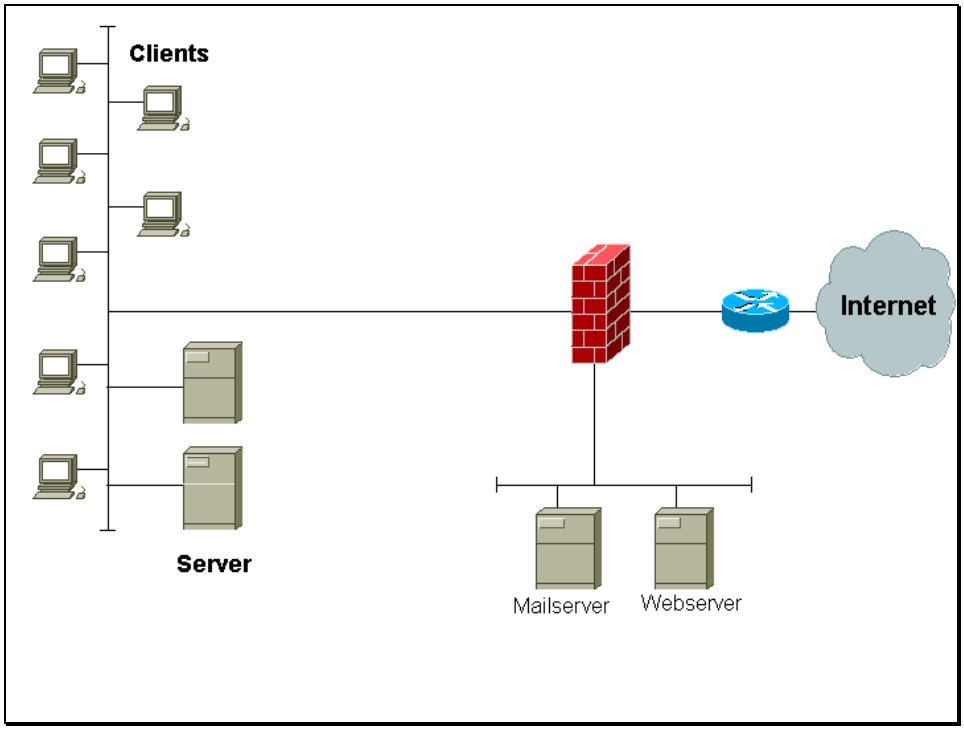

Abbildung 2.1: Einfaches IT-Netzwerk

Die Verbindung zum Internet wird durch eine Firewall geschützt. Der Webserver, der Mailserver und gegebenenfalls weitere Dienste stehen in der demilitarisierten Zone (DMZ). Dieser Aufbau war vor einigen Jahren der Standard bei vielen Firmen. Mit der steigenden Bedrohung aus dem Internet wurde der Aufbau eines sicheren Netzes immer komplexer.

Stellt man höhere Anforderungen an die Sicherheit, beispielsweise im Finanzbereich bei Banken, werden die Sicherheitskomponenten innerhalb der IT-Infrastruktur immer umfangreicher und das Gesamtbild immer komplexer (Abbildung 2.2).

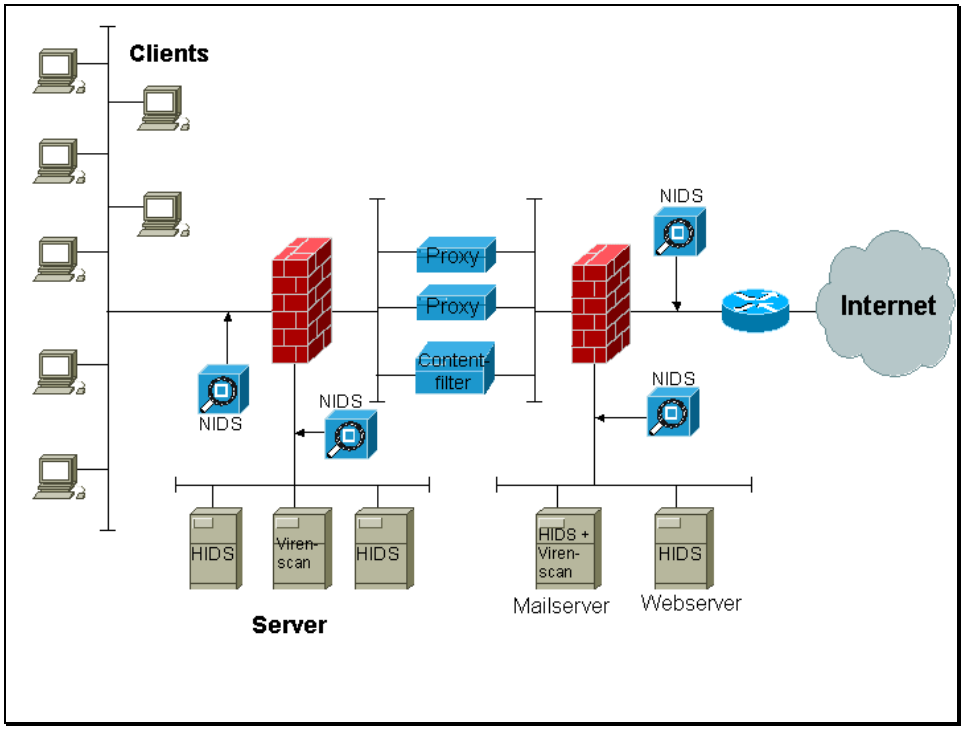

Abbildung 2.2: Komplexes IT-Netzwerk

Man benutzt mehrstufige Firewallsysteme, Virenscanner, Contentfilter und Proxy-Systeme. Ein netzwerkbasierendes Intrusion Detection System (NIDS) sucht nach Angriffen auf der Netzwerkebene. Ein hostbasierendes Intrusion Detection System (HIDS) überwacht die kritischen Server. Application Level Gateways sollen die Anwendungen vor Programmierfehlern schützen. Jedes dieser genannten Systeme erzeugt Daten, die Informationen über Sicherheitsvorfälle enthalten. Die Daten werden in Logfiles lokal gespeichert oder besser auf dedizierten Systemen zentral gesichert. Einige Systeme, wie zum Beispiel Intrusion Detection Systeme sichern die Events in eigenen Datenbanken. Jedes dieser Systeme benutzt ein eigenes Datenformat, so dass eine Korrelation zwischen mehreren Events von verschiedenen Quellen schwierig ist. Selbst verschiedene Produktklassen vom gleichen Hersteller verwenden oft unterschiedliche Formate für die Ablage der aufgezeichneten Ereignisse. Zur Verbesserung der Sicherheit werden oft Sicherheitssysteme von unterschiedlichen Herstellern betrieben. Auch wenn sich bei vielen Systemen aufgrund von definierbaren Ereignissen Traps erzeugen lassen, die an ein einziges Managementsystem gesendet werden können, bleibt das Problem der unterschiedlichen Formate.

Bei der Betrachtung der Anzahl von möglichen Eventquellen (Abbildung 2.2) und der steigenden Bedrohung durch Angriffe aus dem Internet zeigt sich eine wachsende Meldungsflut, die es zu beherrschen gilt. Obwohl es sich in nahezu allen Fällen nur um abgewehrte Angriffe handelt, die keinen Schaden anrichten, bleibt das Problem, die sprichwörtliche Nadel im Heuhaufen zu finden, d.h. einen erfolgreichen Einbruch in das

eigene Netzwerk aus der Flut der Meldungen herauszufiltern. Dass dies nur mit automatisierten Werkzeugen sinnvoll möglich ist, ist selbstverständlich.

Mit der bisherigen Darstellung wurde das Problem der Erkennung eines kritischen Sicherheitsvorfalls von der technischen Seite aus betrachtet. Viele aktive Systeme liefern sicherheitsrelevante Daten über unterschiedliche Wege mit unterschiedlichen Formaten. Allein diese Meldungsflut kann in einem Netzsegment mittlerer Größe von einer Person nicht ohne weitere Hilfsmittel qualifiziert betrachtet und bewertet werden. Dabei wurde der nach einer Bewertung folgende organisatorische Aufwand noch nicht berücksichtigt. Die im folgenden Kapitel 3 aufgeführten Werkzeuge unterstützen den Sicherheitsverantwortlichen im Unternehmen bei der Unterscheidung zwischen falschen Alarmmeldungen und einem realen Einruch ins IT-Netzwerk. Zu jedem Produkt wird eine stichpunktartige Bewertung angegeben, in der die Vor- und Nachteile aufgeführt sind. Diese subjektive Bewertung sollte bei eigenen Betrachtungen kritisch überprüft und gegebenenfalls angepasst werden.

3 Werkzeuge zur Datenreduktion

Im Folgenden werden vier verschiedene Software-Systeme kurz vorgestellt, mit denen eine Verringerung der Meldungsflut möglich ist. Jedes Produkt korreliert in gewissen Grenzen die auftretenden Daten und reduziert somit die Datenflut in einem ersten Schritt. Dabei werden grundsätzlich zwei Prinzipien angewandt. Zum einen werden sehr viele gleichartige Meldungen zu einer einzigen Meldung zusammengefasst. Die Systeme erkennen gleichartige Events anhand von Quell-IP, Ziel-IP und einer durch die Software vergebenen definierten Eventklasse. Zum anderen werden Meldungen unterdrückt, wenn bekannt ist, dass das Zielsystem nicht verwundbar ist. Dies erfolgt anhand von Informationen aus einer Datenbank, die automatisch oder manuell erstellt und gepflegt werden muss und ein Abbild der Netzwerkstruktur mit allen Betriebssystemversionen und Diensten enthält. Alle Produkte verfügen über verschiedene Möglichkeiten die erkannten Angriffe weiter zu melden. Dies kann per Mail, SNMP-Trap, SMS oder über eine produkteigene grafische Bedienoberfläche erfolgen. Die Alarmierung lässt sich auch über ein benutzerdefiniertes Skript nahezu beliebig flexibel konfigurieren. Eine weitere Möglichkeit ist die automatische Reaktion auf einen Angriff durch die Umkonfiguration der Firewall.

Diese Liste mit Programmen von vier unterschiedlichen Herstellern erhebt keinen Anspruch auf Vollständigkeit.

3.1 IBM Risk Manager

Der IBM Risk Manager ist ein Framework und basiert auf der Tivoli-Architektur. Das System unterstützt eine Vielzahl von Eventquellen, darunter Firewall-Systeme von Checkpoint und Cisco (Cisco-PIX), IDS von ISS (Real Secure), Cisco (Cisco Secure IDS) und IBM (Tivoli Host IDS, Tivoli WEB IDS) und Virenscanner (Symantec, Norton Antivirus, Trend Micro). Die Liste wird ständig erweitert. Prinzipiell kann fast jedes System in den IBM Risk Manager integriert werden. Dazu muss nur ein entsprechender „Logfile-Adapter“ geschrieben werden. Diese Flexibilität des Produkts ist auch gleich-

zeitig seine Schwäche. Der Konfigurationsaufwand ist sehr groß. Die vorhandenen „Logfile-Adapter“ sind oft erst mit zeitlicher Verzögerung für die neueste Version der Security-Produkte verfügbar. In der neuesten Version kann bei der Event-Korrelation auch das Tivoli Inventory berücksichtigt werden.

Vorteile:

- sehr flexibel
- Tivoli-Inventory wird in der Event-Konsolidierung mit einbezogen

Nachteile:

- sehr hoher Konfigurationsaufwand
- teilweise zusätzliche Softwarekomponente nötig („Logfile-Adapter“)
- Tivoli-Inventory wird zusätzlich benötigt
- sehr hohe Kosten

3.2 ISS Site Protector mit Fusion Modul

Speziell für die Security-Produkte von ISS (RealSecure Network-Sensor und Host-Sensor) existiert eine Oberfläche mit der eine Korrelation der Events durchgeführt werden kann („Site Protector“). Das zusätzliche „Fusion-Modul“ benutzt den Internet-Scanner von ISS, um eine erweiterte Korrelation der Events mit den tatsächlich vorhandenen Schwachstellen zu ermöglichen. Dadurch wird die Zahl der gemeldeten Sicherheitsverletzungen reduziert, da nur noch Meldungen generiert werden wenn das Zielsystem auch verwundbar ist. Mit zusätzlichen „Third Party Modulen“ lassen sich auch Logfiles von Firewalls (Checkpoint und Cisco-PIX) integrieren. Ein Problem beim Site Protector ist die mangelnde Einflussnahme auf die Korrelation.

Vorteile:

- sehr geringer Konfigurationsaufwand
- automatisches Inventory durch ISS-Scanner
- geringe Kosten
- Integration von FW-logs

Nachteile:

- Inventory nicht änderbar

3.3 SESA von Symantec

Die Symantec Enterprise Security Architecture (SESA) ist eine Plattform, die herstellerunabhängig eine Integration verschiedener Sicherheitstechnologien ermöglicht. So sind nicht nur die Events der Produkte von Symantec auswertbar sondern auch von vielen Fremdherstellern. Bei Fremdprodukten besteht das Problem, dass zusätzliche Agenten installiert werden müssen. Außerdem ist das Produkt neu auf dem Markt und könnte noch „Kinderkrankheiten“ haben.

Vorteile:

- geringer Konfigurationsaufwand
- flexibel

Nachteile:

- teilweise zusätzliche Agenten nötig
- neues Produkt, evtl. „Kinderkrankheiten“

3.4 Netcool von Micromuse

Die Software Netcool ist flexibel konfigurierbar und kann Daten von verschiedenen Quellen (Firewall, IDS,) lesen und verarbeiten. Dabei ist auch eine offline-Verarbeitung möglich, d.h. Events, die bei einem Netzwerkausfall nicht online in die Datenbank eingetragen wurden, lassen sich im Nachhinein noch in das System einspeisen. Mit der Erweiterung „Impact“ werden die auftretenden Events – ähnlich wie das Fusion-Modul beim Site Protector – mit der Struktur des Netzwerkes korreliert. Die dazu nötigen Daten müssen manuell in die Datenbank eingetragen werden, lassen sich aber jederzeit problemlos anpassen.

Vorteile:

- sehr flexibel
- Datenbank für Inventory möglich

Nachteile:

- hoher Konfigurationsaufwand
- manuelle Pflege des Inventory
- hohe Kosten

Die bisher aufgezeigten Werkzeuge unterstützen den IT-Sicherheitsverantwortlichen beim IT-Incident Management. Es wird eine erste Korrelation der Meldungsflut erreicht. Erkannte Ereignisse (Events) können über verschiedene Mechanismen weiter gemeldet werden. Zu einem IT-Incident Management gehören aber noch weitere organisatorische Prozesse und rechtliche Fragen. Was passiert mit fehlerhaft gemeldeten Events („False Positives“)? Wer betrachtet die gemeldeten Ereignisse und liefert den Administratoren eine qualifizierte Bewertung zur effektiven Behebung der Schwachstelle? Wie wird eine 7x24x365-Überwachung realisiert? Wie wird der Informationsfluss für neue Mitarbeiter oder für das Bereitschaftspersonal bei neu erkannten Schwachstellen gesteuert? Wie sieht die rechtliche Situation aus bei einem erkannten Angriff, beziehungsweise bei einem erkannten Einbruch in das Netzwerk? Diese und weitere Fragen zusammen mit den aufgeführten Problemen bei den Werkzeugen führen zur Frage inwieweit ein externer Partner dabei unterstützen kann. Dies soll nun im Kapitel 4 näher erläutert werden.

4 Managed Security Service als externe Dienstleistung

Aufgrund der Anforderungen des Marktes bieten immer mehr Firmen die Dienstleistung „Managed Security Services“ an. Dabei unterstützen die Firmen den Kunden beim Umgang mit sicherheitsrelevanten Daten und bei der Konfiguration der IT-Sicherheitskomponenten. Das Spektrum der Dienstleistung reicht dabei von einer einfachen Analyse von Security-Events bis zu einem vollständigen Management aller Sicherheitssysteme. In einer sicher nicht vollständigen Aufzählung werden nun kurz vier verschiedene Anbieter gegenübergestellt. Alle aufgeführten Anbieter betreiben ein oder mehrere Managed Security Service Center mit einer 7x24x365-Überwachung.

4.1 Activis Managed Security Services

Activis betreibt drei “Security Management Center” (SMC) an verschiedenen Orten (Deutschland, England und USA). Bei den Firewall-Herstellern werden Cisco PIX und Checkpoint unterstützt. Ebenso ist es möglich Intrusion Detection Systeme von ISS (RealSecure) und Cisco (Cisco Secure IDS) überwachen oder managen zu lassen. Der Dienst „e-scan“ schützt den Kunden vor Viren und Spam. Das Produkt „Web Security“ unterstützt bei der URL-Filterung, dem Management und der Überwachung des Internetzugangs und bietet einen Schutz gegen schadhaften WebContent. Die Dienste können nur zur Überwachung (co-managed) oder mit vollständigem Management (fully managed) gekauft werden. Für den Datenaustausch vom Kunden zum SMC wird eine Appliance beim Kunden installiert. Die Datenübertragung erfolgt über VPN mit einer ISDN-Leitung als Backup.

4.2 Controlware Managed Security Services

Die Firma Controlware verwendet für ihr MSS das Werkzeug Netcool von Micromuse. Das MSS-Center nutzt die Flexibilität des Werkzeugs Netcool und kann Daten von verschiedenen Quellen (Firewall, IDS, etc.) lesen und verarbeiten. Das MSS von Controlware unterstützt die offline-Verarbeitung und die Erweiterung „Impact“. Die Pflege der Impact-Datenbank, die das Inventory des zu überwachenden Netzes enthält, wird als

Dienstleistung von der Firma Controlware übernommen. Durch die Verwendung von Netcool (Micromuse) wird die gleiche Flexibilität erreicht, die auch schon in Kapitel 3.4 beschrieben wurde.

4.3 IBM Managed Security Services

Unter dem Schlagwort "Managed Security Services" werden bei der Firma IBM viele verschiedene Services zusammengefasst. Neben „Management Firewall Services", „Network Intrusion Detection Services" und „Virus Alert Services" bietet IBM auch zu dem gleichen Thema eine „Security Policy Definition" oder zum Beispiel Dienste zur Überprüfung des Netzwerkes auf Schwachstellen („Vulnerabillity Scanning Service", „Internet Intrusion Test Services"). Mit den „Incident Management Services" unterstützt IBM auch den Kunden bei der Wiederherstellung der Daten nach einem Securityvorfall.

4.4 Symantec Managed Security Services

Die Firma Symantec betreibt über die ganze Welt verteilt mehrere "Security Operations Center" (SOC). Das Angebot ähnelt dem der Firma IBM sehr. Neben Firewall- und IDS-Management kann auch auf die Dienstleistungen „virus protection and content management" und „policy compliance" zurückgegriffen werden. Die 7x24x365-Überwachung wird durch die Verlagerung des aktiven SOC in verschiedene Länder realisiert. Ab September 2003 wird es voraussichtlich eine 7x24x365-Überwachung geben, die nur in Deutschland realisiert ist. Die Firma Symantec hat ihre SOC's nach dem BS7799-Standard zertifizieren lassen.

Bei allen vier Dienstleistungen kann die Überwachung von sicherheitsrelevanten Informationen an eine externe Firma vergeben werden. Bevor eine Auswahl getroffen werden kann sollte man sich darüber im Klaren sein, welche Anforderungen überhaupt an einen solchen Dienst gestellt werden und wie wichtig die einzelnen Anforderungen für die eigene Organisation sind. Damit die Angebote der verschiedenen Firmen vergleichbar und damit bewertbar sind, sollte man die Dienste gut kennen und diese Informationen auf die eigenen Anforderungen abbilden. Dazu wird im nächsten Kapitel ein Anforderungskatalog in Form einer Liste erstellt.

5 Anforderungskatalog an einen Managed Security Service

Bei der Auswahl eines geeigneten Partners für einen Managed Security Service ergeben sich Anforderungen, bei denen verschiedene Voraussetzungen zu berücksichtigen sind. Zum Einen existieren in der eigenen Organisation Regeln, die beachtet werden müssen. Darunter fallen sowohl technische Gegebenheiten, organisatorische Anweisungen als auch rechtliche Aspekte. Zum Anderen gibt es theoretische Überlegungen die bestimmte Anforderungen einschränken. Zum Beispiel benötigt man zur Übermittlung der Daten an den externen MSS eine Mindestbandbreite, die von der Anzahl der zu übertragenden Daten bestimmt wird. Als Drittes ergeben sich Anforderungen aus dem praktischen Betrieb und der Diskussion mit den Partnerfirmen. Dabei handelt es sich um Vorgaben, Regeln und Grenzen, welche die Partnerfirma vorgibt.

Die folgende Liste enthält teilweise Idealvorstellungen, die sicherlich mit den vorhandenen Grenzen konkurrieren. Das Ziel ist es einen Anforderungskatalog zunächst ohne Bewertung zu erstellen. Danach können diese Idealvorstellungen durch Gewichtung an die Bedürfnisse der eigenen Organisation im Rahmen eines Betriebshandbuches angepasst werden. Eine Bewertung des externen MSS-Dienstes kann dann anhand dieser gewichteten Liste erfolgen.

5.1 Liste mit Anforderungen

1. Erkennen von Sicherheitsverletzungen

   Das ist der offensichtlichste Punkt in der Liste. Man geht im Allgemeinen davon aus, dass dieser Punkt bei jedem MSS-Dienst vorhanden ist. Allerdings geht es darum festzustellen, ob auch neue Schwachstellen sicher identifiziert und gemeldet werden. Dieser Punkt ist nur im praktischen Betrieb zu klären.

2. Zeitnahe Reaktion

   Ein erfolgreicher Angriff auf das Unternehmen muss rechtzeitig erkannt und unterbunden werden. Der Begriff „zeitnah“ ist in diesem Zusammenhang schwierig zu definieren, da der Zeitraum für eine Reaktion von der Art der Bedrohung abhängt.

3. Unterdrückung von Fehlalarmen

   Die Reaktion auf eine Bedrohung sollte nur bei einer wirklichen Gefahrensituation erfolgen. Erfolgt zu oft ein Fehlalarm führt dies dazu, dass ein wirklicher Vorfall nicht mehr ernst genommen wird. Es wird gar nicht oder nur sehr spät darauf reagiert.

4. Überwachung 7x24x365

   Angriffe auf das IT-Netzwerk halten sich nicht an Geschäftszeiten. Durch die weltweite Erreichbarkeit erfolgen Angriffe rund um die Uhr. Die Erfahrung zeigt, dass gerade in Ferienzeiten das Bedrohungspotenzial steigt.

5. Qualifizierte Reaktion auf eine Sicherheitsverletzung

   Der Dienst MSS wird oft von Firmen angeboten, die parallel dazu ein Remote Management anbieten. Auch wenn der Managed Security Service für Firewalls schon länger praktiziert wird, ist das Know-how auf den Gebieten Intrusion Detection System oder Content Filtering noch gering. Bei einer Dienstleistung, die direkten Einfluss auf die Verfügbarkeit des Internetzugangs haben kann, ist es deshalb wichtig, auch bei einer realen Bedrohung das Ausmaß der Reaktion auf das Nötigste zu beschränken. Zum Beispiel wäre das Sperren des gesamten Internetzugangs einer Firma aufgrund einer Sicherheitsverletzung im anonym erreichbaren ftp-Servers keine adäquate Reaktion. Auch sollte dem zu alarmierenden Personal eine aussagekräftige Meldung weitergegeben werden. Dabei reicht es nicht aus, die Meldung aus dem Logfile oder den Event aus dem IDS wört-

lich zu übermitteln. Das Personal im MSS-Center muss die Meldung analysieren, auf die betroffene Netzwerkstruktur abbilden und genaue Anweisungen für sofortige Maßnahmen und eine spätere Behebung der Schwachstelle geben können.

6. Korrelation der unterschiedlichen Eventquellen

   Bei der Betrachtung einer komplexen Netzwerkstruktur mit vielen sicherheitsrelevanten Komponenten erkennt man, dass ein Angriff oder ein Einbruch in ein Rechnersystem durchaus mehrere Ereignisse gleichzeitig auslösen kann. Um eine mehrfache Alarmierung aufgrund eines einzelnen Vorfalls zu vermeiden, muss eine Korrelation der Ereignisse stattfinden. Die Zusammenfassung der Ereignisse darf natürlich nicht so weit gehen, dass wichtige Meldungen unterdrückt werden.

7. Korrelation mit der Netzwerkstruktur

   Netzwerkbasierte Sicherheitssysteme (IDS, Firewalls) melden Events anhand von Quell- und Zieladresse. Sie können normalerweise nicht unterscheiden, ob die Zieladresse für den erkannten Angriff verwundbar ist oder nicht. Die Verbreitung von Würmern erfolgt oft durch zufällig ausgewählte Adressen. Dabei ist zum Beispiel der „Code Red"-Wurm nur bei nicht gesicherten Windows-Systemen kritisch. Die Angriffe des Wurms auf ein Unix-System oder auf ein gehärtetes Windows-System sind irrelevant und sollten natürlich nicht gemeldet werden.

8. Unterstützung möglichst vieler Systeme

   Die Fähigkeit des MSS verschiedene Produkte zu überwachen sollte sich an die gängigsten Produkte am Markt orientieren. Je mehr verschiedene Arten von Firewalls, Intrusion Detection Systemen, Virenscannern und Contentfiltern unterstützt werden, desto leichter ist es, diesen Dienst für das eigene Netzwerk zu nutzen. Eine einzelne Sicherheitskomponente, die nicht unterstützt wird, kann schon dazu führen, dass die Überwachung nicht sinnvoll vom MSS-Center durchgeführt werden kann. Dabei sollte man auch beachten, dass Beschränkungen durch das gewählte MSS-Center einen späteren Ausbau oder Umbau des eigenen Netzwerkes verhindern oder zumindest behindern kann.

9. Flexibilität bei der Alarmierung

   Nahezu alle Anbieter von MSS-Diensten unterstützen die Alarmierung per Anruf, Fax, Mail und SMS oder sind flexibel genug dies mit ihrem Produkt zu realisieren. Die Flexibilität sollte aber noch weiter gehen und Meldungen an verschiedene Personen zu verschiedenen Zeiten über verschiedene Wege ermöglichen. Dabei darf es nicht nur eine beschränkte Anzahl von vorgegebenen Schablonen geben. Die genaue Abfolge bei der Alarmierung ist ein wichtiger Bestandteil des Betriebshandbuchs und sollte auch während des Betriebs änderbar sein.

10. Datenvertraulichkeit

    Alle Daten, die dem MSS-Dienstleister überlassen werden, enthalten wichtige Informationen über die Sicherheit des IT-Netzwerkes. Aus diesen Daten lassen sich leicht Rückschlüsse über Schwachstellen im eigenen Netzwerk ziehen. Diese Daten müssen bei der Übermittlung zwingend gesichert, d.h. verschlüsselt werden. Eine Übertragung über Standleitung oder VPN sollte auf jeden Fall möglich sein. Ebenso ist eine Authentifizierung wichtig, damit das MSS-Center nicht mit falschen Daten getäuscht werden kann. Auch auf den Umgang mit den Daten innerhalb des MSS-Centers sollte man achten. Beim Thema Vertraulichkeit sollte man auch die Kommunikation mit dem MSS-Center berücksichtigen. Fragen nach den Möglichkeiten der Kontaktaufnahme im Betrieb und wie diese Kommunikation gesichert und authentifiziert werden kann, müssen geklärt werden.

11. Sicherheit des MSS-Centers

    Ebenso wichtig wie die Datenvertraulichkeit ist auch die Sicherheit des MSS-Centers. Die Überwachung durch einen externen Dienstleister ist nutzlos, wenn dessen IT-Netzwerk durch einen einfachen Denial-of-Service Angriff außer Gefecht gesetzt werden kann. Wenn das MSS-Center durch einen elektronischen Einbruch kompromittiert werden konnte, besteht die Gefahr, dass sicherheitsrelevante Daten über das institutionseigene IT-Netzwerk für jedermann verfügbar sind. Natürlich besteht die Gefahr eines Einbruchs in das MSS-Center und des Datendiebstahls nicht nur in elektronischer Form.

12. Datensicherung, Beweissicherung

    Für eine spätere Auswertung der erkannten Angriffe, gegebenenfalls mit dem Anspruch auf eine juristische Beweisbarkeit, ist die Datensicherung innerhalb des MSS-Centers von Bedeutung. Es stellt sich die Frage, wie lange die Daten aufbewahrt werden und in welcher Weise sie bei Bedarf abgerufen werden können. Außerdem ist zu klären inwieweit der externe Dienstleister bei einem kritischen Vorfall die juristische Beweisbarkeit unterstützt.

13. Know-how der Mitarbeiter im MSS-Center

    Ein wichtiger Punkt für die Qualität des MSS-Centers ist die Qualität der Mitarbeiter im MSS-Center. Gerade im 7x24x365-Betrieb ist es wichtig, dass qualifizierte Spezialisten nicht nur im Tagesbetrieb ansprechbar sind und es nicht so ist, dass während der Nacht- oder Wochenendzeiten der Betrieb durch Hilfspersonal aufrecht erhalten wird. Auch sollten ständig Mitarbeiter idealerweise vor Ort oder zumindest schnell erreichbar sein, die sich mit allen zu überwachenden Techniken gut auskennen.

14. Redundanz des MSS-Centers

    Eine einzige zentrale Stelle zur Überwachung zu verwenden ist immer ein „single point of failure“. Jede Technologie hat ihre Schwächen und jedes System kann einmal versagen. Nur eine redundante Auslegung der benötigten Kompo-

nenten verhindert einen Ausfall des gesamten Systems durch den Ausfall eines einzelnen Systems. Dieses Prinzip gilt natürlich auch für ein MSS-Center. Dabei kann die Redundanz durch mehrfache Auslegung wichtiger Komponenten innerhalb eines Standortes oder durch die Verwendung von mehreren Standorten gewährleistet werden.

15. Flexible Statistiken

    Neben der schnellen Reaktion auf aktuelle Ereignisse benötigt man auch Auswertungen über einen längeren Zeitraum hinweg. Der Zeitraum und der Umfang der Auswertung sollte vom Kunden frei wählbar sein. Solche Statistiken können wertvolle Hinweise auf das aktuelle Bedrohungspotenzial geben. Dieses Bedrohungspotenzial kann sowohl temporal mit früheren Auswertungen der eigenen Institution verglichen werden, als auch im gleichen Zeitraum mit Daten von fremden Institutionen. Selbstverständlich stellt das MSS-Center diese Vergleichsdaten von anderen Kunden anonymisiert zur Verfügung. Außerdem wäre es vorteilhaft, wenn die erzeugten Statistiken mit Zahlen von bekannten Institutionen z.B. dem SANS-Institute, vergleichbar wären. Eine Veröffentlichung solcher Statistiken kann auch zu einem Imagegewinn für das Unternehmen führen. Die Aussage, welche Bedrohung im IT-Bereich durch Angriffe erkannt und somit verhindert wurde, führt bei den Kunden und Partnern des Unternehmens zu einer verbesserten Vertrauensbasis. Der Aufbau und Betrieb von Sicherheitskomponenten im Unternehmen verschlingt viel Geld, das Ergebnis jedoch ist nicht immer transparent. Mit regelmäßigen Statistiken lassen sich bereits getätigte Ausgaben rechtfertigen und sie bilden die Grundlage für weitere Investitionen in Sicherheitstechnologie.

5.2 Gewichtung der Liste

Die im Kapitel 5.1 beschriebenen Anforderungen sollen nun in einer Liste (Tabelle 5.1) zusammengefasst werden. Für jeden einzelnen Punkt in der Liste gibt es in der zweiten Spalte eine Bewertung der Wichtigkeit auf einer Skala von 0 bis 9, wobei 0 unwichtig bedeutet und die Zahl 9 den betreffenden Punkt als sehr wichtig einstuft. In einer dritten Spalte kann für jeden externen MSS-Dienst die Umsetzung der Anforderung bewertet werden. Auch hier werden die Punkte von 0 (erfüllt die Anforderung gar nicht) bis 9 (erfüllt die Anforderung in allen Punkten) vergeben. Die endgültige Bewertung ergibt sich dann aus der Summe über alle Produkte von Spalte 2 multipliziert mit Spalte 3. In einer letzten Spalte kann für die Bewertung ein kurzer Kommentar eingetragen werden. Dadurch wird das Schema nachvollziehbar. Damit lässt sich der Gedankengang bei der Bewertung gegebenenfalls wiedergeben und so Verbesserungen und Erweiterungen einbringen.

Anforderung	Wichtig-keit	Umset-zung	Kommentar
Erkennen von Sicherheitsverletzungen	9		
Zeitnahe Reaktion	8		
Unterdrückung von Fehlalarmen	6		
Überwachung 7x24x365	8		
Qualifizierte Reaktion auf eine Sicherheitsver-letzung	6		
Korrelation der unterschiedlichen Eventquellen	4		
Korrelation mit der Netzwerkstruktur	6		
Unterstützung möglichst vieler Systeme	5		
Flexibilität bei der Alarmierung	3		
Datenvertraulichkeit	7		
Sicherheit des MSS-Centers	7		
Datensicherung, Beweissicherung	3		
Know-how der Mitarbeiter im MSS-Center	5		
Redundanz des MSS-Centers	3		
Flexible Statistiken	6		

Tabelle 5.1: Anforderungsliste mit Bewertung

Die in dieser Liste angegebene Wichtigkeit ist eine subjektive Einschätzung, die aus den theoretischen Überlegungen und praktischen Erfahrungen mit Produkten aus Kapitel 3 und externen Dienstleistern aus Kapitel 4 entstanden ist. Sie spiegelt die Security Policy der eigenen Firma wider und muss an die eigene Security Policy angepasst werden. Mit dieser Liste als Grundlage kann dann für jeden in Frage kommenden Managed Security Service-Dienst die Spalte *Umsetzung* gefüllt werden. Einige der Anforderungen können effektiv nur durch einen Test bewertet werden. Andere Fragen lassen sich leicht bei Gesprächen mit Vertretern der verantwortlichen Firma beziehungsweise durch ein Angebot von der Firma beantworten. Mit der oben angegebenen Berechnungsvorschrift erhält man dann eine Gesamtpunktzahl die theoretisch maximal 9 x 9 x 15 = 1215 betragen kann. Wichtig dabei ist nur die Differenz zwischen den Gesamtpunktzahlen der einzelnen bewerteten MSS-Diensten. Der Anbieter mit der höchsten Punktzahl erfüllt die eigenen Anforderungen am besten im Vergleich zu den anderen Anbietern von MSS-Dienstleistungen.

6 Zusammenfassung

Ein komplexes IT-Netzwerk mit vielen Sicherheitskomponenten kann effektiv nur noch mit automatisierten Verfahren überwacht werden. Sicherheitssysteme ohne Überwachung und Alarmierung sind nahezu nutzlos. Diese Überwachung und Alarmierung kann durch geeignete organisatorische und technische Prozesse innerhalb eines Unternehmens durchgeführt werden. Der dazu nötige Aufwand ist hoch und die technischen beziehungsweise organisatorischen Probleme führen zu der Frage, ob dies nicht durch einen externen Dienstleister besser realisiert werden kann.

Bei der Evaluierung von externen Dienstleistern zeigte sich, dass die Anforderungen an einen Managed Security Service-Dienst zuerst genau spezifiziert werden müssen. Bei der Anzahl von Anforderungen hat sich ein Bewertungsschema in Form einer Liste bewährt. Die angeführte Liste entstand aus dem praktischen Problem heraus, die Anforderungen eines Kunden an den externen Dienstleister transparent weiter zu geben und gleichzeitig die unterschiedlichen Leistungen eines externen MSS-Dienstes bewertbar zu machen. Die Bewertung der einzelnen Punkte muss sicherlich individuell auf die Bedürfnisse des Kunden und mit einer vorhandenen Security Policy abgestimmt werden. Mit diesen Voraussetzungen ist dann die Auswahl eines geeigneten MSS-Dienstes möglich. Dabei wird zugrunde gelegt, dass aus bestimmten Gründen eine externe Vergabe der Dienstleistung angestrebt wird.

Eine bisher nicht betrachtete Alternative zu interner oder externer Verarbeitung von sicherheitsrelevanten Daten wäre die Kombination aus einem internen Softwaresystem, welches die auftretenden Events korreliert und einem externen Dienstleister, der nur noch die zusammengefassten Ereignisse betrachten und bewerten muss und im Notfall den zuständigen Systembetreuer informiert. Der Auftraggeber muss nur sehr wenige sicherheitsrelevante Daten versenden und behält die vollständige Kontrolle über seine Sicherheitssysteme. Alle notwendigen Konfigurations- und Wartungsarbeiten sind jedoch von ihm selbst durchzuführen. Ebenso muss der 7x24x365 Bereitschaftsdienst auch vom Auftraggeber gestellt werden.

In der gesamten Betrachtung blieb allerdings der finanzielle Aspekt bis jetzt weitgehend unberührt. Bei einer InHouse-Lösung muss der Aufwand für zusätzliche Systeme, Wartungsaufwand für Hard- und Software, Schulung der Mitarbeiter und gegebenenfalls der Aufbau eines 7x24x365 Bereitschaftsdienstes in eine Berechnung mit einfließen. Bei einer Überwachung durch eine externe Firma ist vor allem die Anzahl der zu überwachenden Systeme der kostenbestimmende Faktor. Eine Kombination von interner und externer Realisierung muss keine Summierung der Kosten zur Folge haben, da sowohl bei der internen als auch bei der externen Durchführung nicht die kompletten Anforderungen realisiert werden müssen.

Die Frage, ob das IT-Incident Management durch eine externe Dienstleistung die Lösung aller IT-Incident Management Probleme darstellt, kann nur durch eine Betrachtung der technischen und organisatorischen Probleme im Zusammenhang mit dem finanziellen Aufwand beantwortet werden. Sicher werden nicht alle IT-Incident Management Probleme durch eine externe Dienstleistung gelöst. Die Entscheidung, ob und welcher Dienst eingesetzt wird, ist immer von den Vorbedingungen und Gegebenheiten der Organisation abhängig, die beabsichtigt die Dienstleistung zu verwenden.

7 Literaturverzeichnis

[ACT00] Activis: Managed IDS;
URL: http://www.activis.com/de/ids/

[BSI00] BSI: BSI-Leitfaden zur Einführung von Intrusion-Detection-Systemen;
URL: http://www.bsi.de/literat/studien/ids02/index.htm

[COS00] ConSecure GmbH: Einführung von Intrusion-Detection-Systemen, 2002;
URL: http://www.bsi.de/literat/studien/ids02/dokumente/Rechtv10.pdf

[COT00] controlware communicationssystems: Managed Security Services (M.S.S);
URL: http://www.controlware.de/de/cws2/Services/Operating/index.html

[FAI00] Faile, Jonathan S.: Security Outsourcing, SANS Institute 2001;
URL: http://www.sans.org/rr/paper.php?id=223

[HES00] Hess, Dr. Sigurd: Informationssicherheit und Schutz kritischer Infrastrukturen; „European Security and Defence, No. 02-2002

[IBM00] IBM: Security Services
URL: http://www-5.ibm.com/services/de/e-business_hosting/security.html

[ISS00] Internet Security Systems: Internet Risk Impact Summary (IRIS) for April 1, 2003 through June 30, 2003, Atlanta, 2003;
URL: https://gtoc.iss.net/documents/summaryreport.pdf

[KIN00] Kinsey, William: Why MSS, SANS Institute 2001;
URL: http://www.sans.org/rr/ paper.php?id=222

[SYM00] Symantec: Managed Security Services;
URL: http://enterprisesecurity.symantec.de
/SecurityServices/content.cfm?ArticleID=2035&EID=0