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).

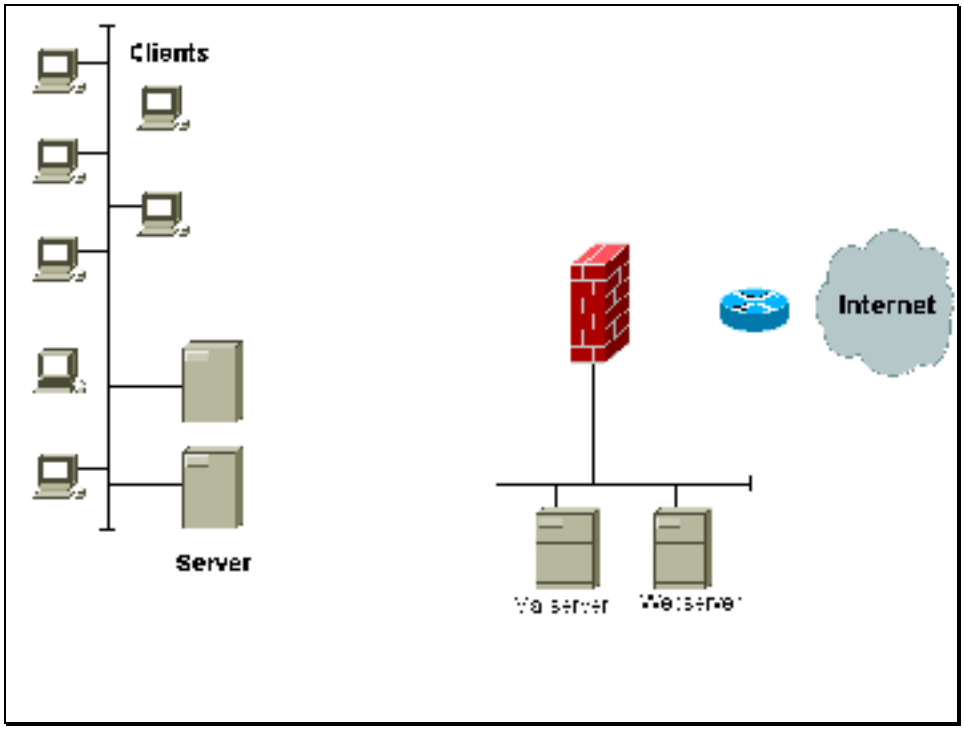

Abbildung 2.1: Einfaches IT-Netzwerk

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).

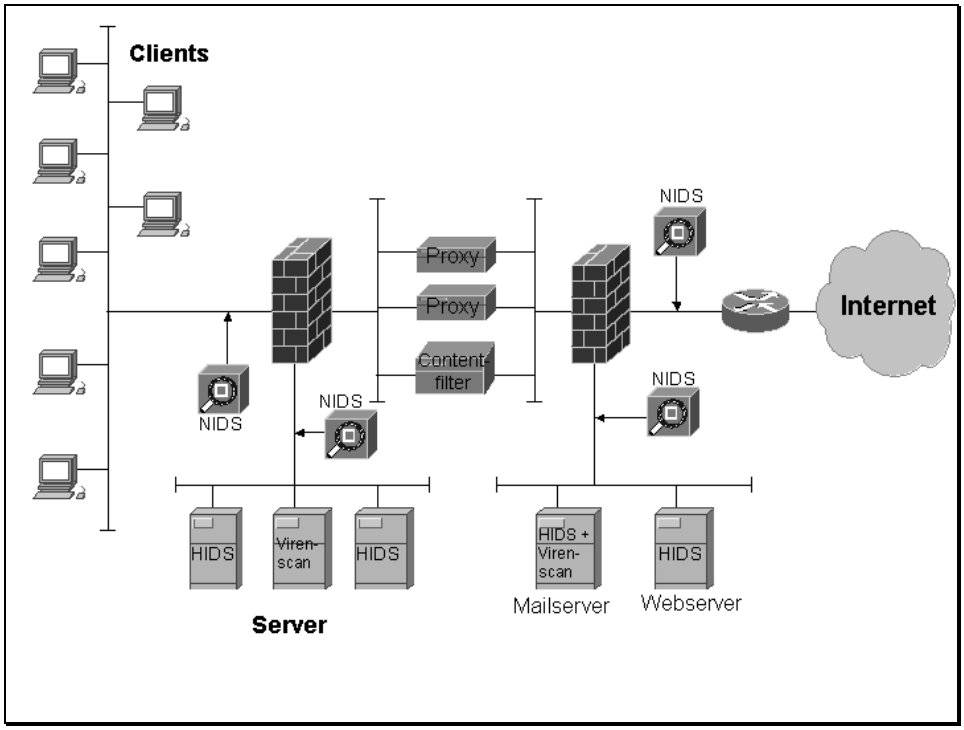

Abbildung 2.2: Komplexes IT-Netzwerk

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

Eine Informationsbasis für zeitoptimiertes Incident Management

Peter Scholz[1], Ramon Mörl[2]

[1)] Fachhochschule Landshut
Am Lurzenhof 1, D-84036 Landshut
Peter.Scholz@fh-landshut.de

[2)] SioS GmbH
Dorfstrasse 13
D-81247 München
Ramon.Moerl@sios-gmbh.de

Abstract: Ziel des Incident Managements ist die schnellstmögliche Wiederherstellung des regelmäßigen Betriebs eines Services nach Eintritt eines Vorfalls. Eine bewusst oder unbewusst produzierte Falschmeldung über einen sicherheitskritischen Vorfall kann jedoch zu schwerwiegenden Folgen führen. Um diese enttarnen zu können, ist eine profunde und rasche Einschätzung der Vertrauenswürdigkeit der Meldung und ihrer Herkunft (kurz im Folgenden „Verbindlichkeit" genannt) erforderlich. Gerade der Bewertung der Verbindlichkeit wurde bis dato aber kaum Bedeutung beigemessen. In diesem Beitrag wird ein Ansatz zur Qualitätsverbesserung und Zeitoptimierung des Incident Managements vorgestellt, der die Verbindlichkeit einer Incidentmeldung durch die Analyse von Vertrauensketten bewertet. Der Zeitvorsprung wird dabei durch Rückgriff auf eine bereits vor dem Incident aufgebaute Informationsbasis gewonnen. Darüber hinaus ermöglicht unser Modell durch eine enge Verknüpfung mit dem in einem früheren Beitrag vorgestellten aktiven Risikomanagement entlang von Wertschöpfungsketten auch die Abschätzung von Konsequenzen einer Incidentmaßnahme.

1 Einleitung und Motivation

Vielen Lesern mag das folgende hartnäckige Gerücht aus dem Jahre 2002 noch gut in Erinnerung sein: Ein Mann angeblich arabischer Herkunft warnt den angeblichen Finder seiner Brieftasche mit einer größeren Menge Bargeld vor einem bevorstehenden Attentat, indem er ihm rät, in näherer Zukunft einen bestimmten Ort zu meiden. Diese Geschichte wurde in verschiedenen deutschen Städten mit unterschiedlichen Details verbreitet, wobei vor allem die Höhe des Geldbetrags, der Ort (Kaufhäuser, Gaststätten, Menschenansammlungen) sowie der Anlass (Karneval, Halloween, Weihnachtsmarkt) variierten. Nun war aber in Hannover die Beschreibung des Finders so detailliert, dass eine Übereinstimmung mit einer lebenden Person tatsächlich gegeben war. Sie hatte tatsächlich eine Geldbörse gefunden, alles andere war aber freie Erfindung.

Sehr viele Inhaber von Incident Management-Stellen hatten sofort nach Auftreten des Gerüchts versucht, diese Person schnellstmöglich aufzufinden, um den Wahrheitsgehalt (die Verbindlichkeit) der Geschichte herauszufinden, um ggf. entsprechende Maßnahmen einleiten zu können. So konnten tatsächlich zahlreiche Sicherheitsverantwortliche mit der Person telefonisch in Kontakt treten, bis diese irgendwann aufgrund der Flut von Anfragen zu weiteren Auskünften nicht mehr bereit war.

Wir können dieses Beispiel wie folgt verallgemeinern: Ein sicherheitskritischer Vorfall wurde gemeldet und die Verbindlichkeit der zugehörigen Information sollte überprüft werden, um so schnell wie möglich die richtigen Maßnahmen einzuleiten. Dies schlug allerdings fehl, weil die Vertrauenskette zum Zeitpunkt des Vorfalls nicht mehr zurückverfolgt werden konnte, um entlang ihr den Ursprung und die Richtigkeit der Vorfallsmeldung zu überprüfen. Nicht nur dass die Überprüfung der Vertrauenskette zu lange dauerte um ein tatsächliches Attentat verhindern zu können, in diesem Szenario war sie überhaupt nicht reproduzierbar. Eine weitere, sehr wesentliche Herausforderung ist darüber hinaus das Enttarnen von Falschmeldungen.

Bei jedem Incident ist also das Vertrauen in die Richtigkeit der Vorfallsmeldung von größter Wichtigkeit: Ungerechtfertigt eingeleitete Eskalationsmaßnahmen führen im schlimmsten Fall zu kritischen Vermögensverlusten, schwächen aber in jedem Fall die Glaubwürdigkeit des Incident Managements. War die Falschmeldung sogar beabsichtigt, so war man möglicherweise durch die darauf hin eingeleitete Eskalation gezwungen, das Sicherheitsniveau derart zu senken, dass ein diese Situation ausnützender Angriff nicht schadlos überstanden werden könnte.

Um nun tatsächlich im Falle eines derartigen Vorfalls schnell die richtigen Entscheidungen zu treffen, ist eine entsprechende Informationsbasis [BDS02] erforderlich. So liegen die vier Topforderungen der deutschen Wirtschaft darin, bessere und verlässlichere Informationen für den Eigenschutz zu bekommen [WIK03]. In diesem Beitrag wollen wir aufzeigen, wie eine solche auf Basis von Vertrauensketten für sicherheitskritische Vorfälle aufgebaut werden kann.

Da eine Vorfallsmeldung meist indirekt und durch die hintereinandergeschaltete Beteiligung mehrerer Subjekte (Organisation, automatische Informationsweiterleitung in Systemen oder Owner von IT-Diensten) geschieht, muss jedes Glied der Informationskette vertrauenswürdig sein und die Verbindlichkeit der zugehörigen Nachricht als sehr hoch eingestuft werden. Bei jedem Incident sollte darum die Verbindlichkeit der Vorfallsmeldung entlang einer Vertrauenskette verfolgt und bewertet werden. Um eine schnellstmögliche Reaktion auf den Incident zu gewährleisten, sollte diese Analyse bereits im Vorfeld werkzeugbasiert und methodisch unterstützt erfolgen.

Wir schlagen daher einen Ansatz vor, der zum einen die Entscheidungszeit im Falle eines Incidents durch eine vorab erstellte Informationsbasis minimiert und zum anderen die Qualität der Entscheidung durch eine werkzeugbasierte Unterstützung beim Abschätzen der Konsequenzen analysiert. Die Voraussetzungen hierfür müssen bereits vor einem konkreten Vorfall geschaffen werden. Voraussicht zahlt sich im Notfall aus [Rie03]. Wir plädieren deshalb für eine stärkere Ausprägung der strategischen Komponente beim Incident Management, das bisher oft nur im rein operativen Bereich seinen Niederschlag findet.

Ziel unseres Ansatzes ist die Optimierung des Incident-Managements durch ein präzises mathematisches Modell, das eine automatische Verfolgung von Vertrauensketten zur Verfügung stellt und bei der Auswirkungsanalyse auf bestehenden Informationen des ebenenübergreifenden Risikomanagements [Sch03] aufbaut. Aufgrund der auf diese Weise geschaffenen direkten Anbindung an das (proaktive) Risikomanagement ist eine ganzheitliche Betrachtung von Risiko- und Incident Management möglich.

Der Rest unseres Beitrags ist wie folgt aufgebaut. In Abschnitt 2 beschreiben wir zunächst die Herausforderungen, die es im Incident Management zu lösen gilt. Wie die Verbindlichkeit einer Incidentmeldung entlang von Vertrauensketten überprüft werden kann, schildern wir in Abschnitt 3. Abschnitt 4 enthält eine Zusammenfassung unserer Ergebnisse zum proaktiven Risikomanagement entlang von Wertschöpfungsketten, das wir bereits an anderer Stelle [Sch03] erstmals beschrieben haben. Wie proaktives Risikomanagement und Incident Management zusammenwachsen, wird in Abschnitt 5 erläutert. Der Artikel schließt in Abschnitt 6 mit einer Zusammenfassung.

2 Herausforderungen des Incident Managements

Ein Vorfall (engl. incident) ist ein Ereignis (was ist wo passiert?), welches den regelmäßigen Betrieb eines IT-Services unterbricht bzw. seine Qualität deutlich mindert oder im Sinne eines Angreifers die Funktionalität verändert. Oft beschränkt man sich bei Incidents auf die Betrachtung von Störungen; wir wollen diese Einschränkung lockern und darüber hinaus alle denkbaren Arten von Vorfällen zulassen, unser Augenmerk dabei aber hauptsächlich auf sicherheitskritische Incidents lenken.

Tritt ein Incident in der eigenen Organisation auf, so ist das Ziel des Incident Managements die schnellstmögliche Behebung dieses Vorfalls und Wiederherstellung des normalen Betriebs des betroffenen Dienstes. Hierbei ist die Beseitigung der Ursache zweitrangig – auch eine Umgehung des Vorfalls ist ein valides Mittel zur Beseitigung des Incidents.

In der weitaus größeren Zahl der Fälle ist allerdings nicht die eigene, sondern eine fremde Organisation von einem sicherheitskritischen Incident betroffen, und das eigene Incident Management erfährt hiervon lediglich. Auch hier ist eine rasche Reaktion nötig, um Sofortmaßnahmen (z.B. Schutz vor einem angeblich bevorstehenden Angriff) einzuleiten.

Tritt ein Incident auf, so sollte i.d.R. wie folgt vorgegangen werden (**Ablauf des Incident Managements**):

1. Vorfall melden
2. Vorfall erfassen
3. Vorfall klassifizieren, lokalisieren und ihre Sicherheitsrelevanz sowie Dringlichkeit bzw. Wirkung auf den Geschäftsbetrieb feststellen
4. Den sicherheitskritischen Vorfall verbindlich bestätigen

5. Sicherheitskritischen Vorfall beheben in Abhängigkeit zur Einschätzung aus (3)

6. Sicherheitskritischen Vorfall schließen

Bis dato konzentrieren sich die Anstrengungen beim Incident Management auf die schnellstmögliche Wiederherstellung des betroffenen IT-Dienstes. Um eine Verkürzung der Reaktionszeit zu erzielen, wird das operative Incident Management nicht selten über ein Service Desk gesteuert. Dessen Mitarbeiter müssen in die Lage versetzt werden, im Fall eines tatsächlichen Vorfalls den oben skizzierten Ablauf so schnell wie möglich in Gang zu setzen.

Hierbei muss dem Schritt (3) eine besondere Beachtung beigemessen werden. Nur wenn der Vorfall selbst rasch lokalisiert und seine Art erkannt wird, kann eine valide Abschätzung der Dringlichkeit bzw. Wirkung auf den Geschäftsbetrieb geschehen. Dazu muss vor allem aber auch die Verbindlichkeit der Information, die einen sicherheitskritischen Vorfall meldet, eingeschätzt werden können (4). Dieser Punkt wird beim Incident Management in sicherheitskritischen Umgebungen bis dato oftmals entweder völlig außer Acht gelassen oder er verursacht zumindest ein gehöriges Maß an hektischen Aktionismus.

Als ein besonderes Problem erweisen sich zunehmend fehlerhafte oder irreführende Informationen, sogenannte Hoaxes. Sie führen in der Administration von IT-Systemen dort zu Arbeitsaufwänden, wo die Fehlinformationen nicht unmittelbar erkannt werden [BSI03]. Betrachten wir das folgende Beispiel: Der Administrator der Firewall eines Unternehmens A liest in einer fachspezifischen Newsgroup (oder in einer weitergeleiteten Email) von dem eben geschehenen Angriff auf das Unternehmensnetz eines Unternehmens B mit dem Hinweis des angeblichen Security Managers von B, welcher Patch in die Firewall eingespielt werden müsse, um den Angriff erfolgreich abzuwehren. Kann er diesem Hinweis trauen oder wurde er vielleicht arglistig getäuscht, weil der Patch den Wirkungsgrad der Firewall massiv beeinträchtigen würde (Hoax)? Um dies zu wissen, müsste er erst die Verbindlichkeit der Vorfallsmeldung überprüfen. Wie kann er dies tun? Indem er so schnell es geht Schritt für Schritt den Weg der Meldung zurückverfolgt, also telefoniert, Emails schreibt usw. Diese Recherche dauert im Zweifelsfall zu lange, und wenn er seine Entscheidung (seine Entscheidungsalternativen: nichts tun, Patch einspielen, Firewall komplett sperren) getroffen hat, ist möglicherweise der Angriff schon passiert. Darüber hinaus kann er nicht abschätzen, welche Auswirkungen jede dieser Alternativen auf die Wertschöpfung des Unternehmens haben wird? Wenn unser Administrator also erst bei dem Auftreten eines Vorfalls mit der Prüfung dessen Verbindlichkeit und Auswirkungen beginnt, ist es meist zu spät.

Die Einschätzung der Verbindlichkeit einer Information, vor allem dann, wenn sie entlang einer komplexen Vertrauenskette weitergegeben wurde, stellt eine herausfordernde Aufgabe dar. Eine adäquate Hilfestellung kann hier nur durch die Bereitstellung einer entsprechenden Unterstützung in Form von Werkzeugen, Infrastruktur- [Moe97] und Organisations-/Prozessmaßnahmen [Sch02] geleistet werden.

Als Grundlage für dieses Tool schildern wir einen Ansatz, der auf einem mathematischen Modell basiert, das auf unseren Techniken zum Risikomanagement [Sch03] aufbaut. Proaktives Risikomanagement und reaktives Incident Management wachsen somit

zusammen und können einheitlich betrachtet werden und von einem einzigen Produkt abgedeckt werden. Ein automatisierter Datenaustausch zwischen Incident- und Risikomanagement wird somit möglich.

3 Analyse der Vertrauensketten außerhalb des Unternehmens

Im Folgenden wollen wir zeigen, wie die Verbindlichkeit einer Incidentmeldung entlang von Vertrauensketten bewertet werden kann. Hierzu muss zunächst eine Reihe zentraler Begriffe definiert werden.

Definition (Verbindlichkeit): Eine Information gilt als verbindlich, wenn ihr Wahrheitsgehalt so hoch ist, dass hierauf weitreichende Entscheidungen fußen können.

Für gewöhnlich wird mit der Eigenschaft der Verbindlichkeit die Forderung nach der Abrechenbarkeit (engl. accountability) eng verbunden. Dies erfordert Maßnahmen zur Überwachung und zur Protokollierung [Eck03]. In unserem Fall ist dies allerdings von zweitrangiger Bedeutung; anstelle dessen steht eher die Frage nach der Haftung bzw. Haftbarkeit (engl. liability) im Vordergrund. So übernimmt der Überbringer einer Information keine Haftung für deren Wahrheitsgehalt – selbst das BSI CERT tut dies beispielsweise nicht. Es sollte also unser Ziel sein, auch für Nachrichten „ohne Gewähr“ eine hohe Verbindlichkeit sicherzustellen.

Den Begriff des „Subjekts“ fassen wir sehr weitläufig und definieren ihn umfangreicher als sonst in der IT-Security Community [Eck03] üblich.

Definition (Subjekt): Hierunter verstehen wir Organisationen und Organisationseinheiten genauso wie die Owner eines Service, die Benutzer eines Systems und alle Objekte, die im Auftrag von Benutzern im System aktiv sein können, wie z.B. Prozesse, Server und Dienste.

Definition (Vertrauen, Vertrauensbeziehung, Vertrauensrelation): Wir sagen, das Subjekt S1 vertraut dem Subjekt S2, wenn es die von ihm erhaltenen Informationen als mit hoher Wahrscheinlichkeit richtig einstuft. Durch dieses Vertrauen entsteht eine Vertrauensbeziehung bzw. Vertrauensverhältnis. Stehen zwei oder mehr Subjekte in einer Vertrauensbeziehung, so entsteht insgesamt eine Vertrauensrelation R (Relation auch im mathematischen Sinne):

$$(S1,S2) \in R :\Leftrightarrow S2 \text{ vertraut } S1.$$

Definition (Vertrauensqualität): Die Güte des Vertrauens (bzw. der Grad der Vertrauenswürdigkeit) innerhalb einer Vertrauensbeziehung kann durch ihre Gewichtung ausgedrückt werden, die wir als Vertrauensqualität bezeichnen.

Der Begriff der Vertrauensrelation kann auf die Vertrauensrelation mit Vertrauensqualität (= gewichtete Vertrauensrelation) wie folgt erweitert werden:

$$(S1,S2,w) \in R :\Leftrightarrow S2 \text{ vertraut } S1 \text{ mit der Vertrauensqualität } w \in W,$$

wobei W das Spektrum der Vertrauensqualität darstellt. Ein Beispiel für die Vertrauensqualität ist die Angabe des Alters bzw. der Dauer der Vertrauensbeziehung zwischen zwei Subjekten. Sie kann aber beispielsweise auch als ein Wert zwischen 0% (kein Vertrauen) und 100% (vollstes Vertrauen) angegeben werden.

Definition (Vertrauensnetz): Eine gewichtete Vertrauensrelation R kann visuell durch einen gewichteten, gerichteten Graph G=(V,E,w) mit V = Knoten, E = Kanten und w = Gewichtungsfunktion w:E→W angegeben werden, der als Vertrauensnetz bezeichnet wird.

Dass dieser Graph gerichtet ist, ist hierbei von zentraler Bedeutung: Angenommen, zwei Subjekte A und B kommunizieren per Email, wobei A seine Emails stets digital signiert, B dies aber nie tut, dann wird B Emails von A sicherlich mehr vertrauen als umgekehrt, vorausgesetzt natürlich B kann die Signatur von A diesem auch eindeutig zuordnen.

Definition (Vertrauenskette): Eine Vertrauenskette ist eine Folge bzw. Pfad von Vertrauensbeziehungen innerhalb eines Vertrauensnetzes.

Beispiel (Vertrauenskette): Die Teilnehmer eines unternehmensübergreifenden Vertrauensnetzes sind hier mit Buchstaben benannt und bezeichnen verschiedene Organisationen, die potentiell Meldungen über sicherheitskritische Incidents austauschen. Die Vertrauensqualität wird in diesem Beispiel durch die Angabe einer Prozentzahl definiert. Das Vertrauensnetz ist in Abbildung 3.1 dargestellt. Tritt ein Vorfall bei einem Knoten (= Organisation) im Netz auf, so kann eine Vorfallsmeldung entlang des Netzes verschickt werden. Zwischen zwei Knoten im Netz können somit stets durch einfache Graphenalgorithmen die kürzesten oder sichersten Pfade berechnet werden, entlang derer die Meldung transportiert werden soll.

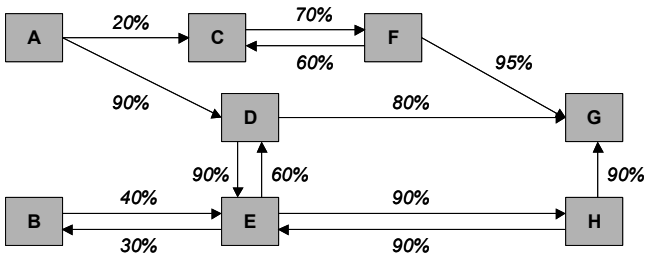

Abbildung 3.1: Organisationsübergreifendes Vertrauensnetz

Bei der Frage nach der sichersten Vertrauenskette treten sogleich interessante Fragestellungen auf, die man ohne die Modellierungen möglicherweise vernachlässigen würde. Angenommen, eine Vorfallsmeldung soll in Abbildung 3.1 von A nach G transportiert werden. Welche der folgenden Vertrauensketten ist diejenige, in die G das höchste Vertrauen setzen kann?

(a) Vertrauenskette A-C-F-G, da hier in den unmittelbaren Überbringer der Nachricht, F, das höchste Vertrauen (= 95%) gesetzt wird?

(b) Vertrauenskette A-D-G, da es sich hierbei zum einen um den kürzesten Pfad handelt (vgl. Problem der „stillen Post“: je weniger Subjekte an einer Vertrauenskette beteiligt sind, desto besser)?

(c) Vertrauenskette A-D-E-H-G, weil hier nirgends der Wert von 90% unterschritten wird?

Die gerade gestellten Fragen besitzen einen proaktiven Charakter. Tatsächlich ist es beim Incident-Management aber so, dass reaktiv gehandelt werden muss. Wir regen daher an, Entscheidungskriterien direkt in die Security Policy mit aufzunehmen, um eine Verbesserung der Vertrauenswürdigkeit externer Kommunikationsverbindungen, z.B. zu CERTs, bereits im Vorfeld anzustreben (Beispiele: Austausch von Zertifikaten, signierte Emails usw.).

Die Modellierung eines Vertrauensnetzes hilft also neben den bereits motivierten Vorteilen auch bei der Festlegung auf eine dieser Alternativen und darum insgesamt bei der Definition einer entsprechenden Vertrauenspolicy im Umgang mit verbundenen Organisationen (z.B. im Rahmen des Zulieferernetzwerks). In der Realität besteht natürlich im Regelfall mehr als nur eine einzige Vertrauensbeziehung zwischen zwei Subjekten, da unterschiedliche Ansprechpartner und Kommunikationskanäle (Email, Telefon, Fax, persönlicher Kontakt usw.) existieren.

Darüber hinaus fördert das Bilden eines Vertrauensnetzes die organisationsübergreifende Kommunikation und Transparenz, da G ohne weiteres zutun von F, D und H keine Kenntnis über die Qualität der restlichen Vertrauensbeziehungen im Netz besitzen würde. Ferner kann jedes Subjekt aktiv dazu beitragen, seine Vertrauensbeziehung zu anderen Subjekten zu verbessern, indem es Maßnahmen wie z.B. das Einführen ein PKI, das Signieren von Emails, oder auch nur die Nennung eines persönlich bekannten Verantwortlichen ergreift.

Um diesem ganzheitlichen Ansatz besser folgen zu können, werden zunächst im Abschnitt 4 die grundlegenden Wesenszüge unserer Methode des Risikomanagements entlang von Wertschöpfungsketten beschrieben.

4 Risikomanagement entlang von Wertschöpfungsketten

Betrachten wir nochmals das Beispiel des Administrators, der so rasch wie möglich die Verbindlichkeit einer Vorfallsmeldung in einer Email bewerten will. In Abschnitt 3 haben wir ein Verfahren beschrieben das ihn hierbei unterstützt. Allerdings ist der zweite Teil seiner Frage nach der Auswirkung seiner Entscheidung auf die Wertschöpfung des Unternehmens noch völlig offen. Er könnte im vorliegenden Fall die Tragweite abschätzen, wenn er eine Möglichkeit hätte, die Nicht-Verfügbarkeit der Firewall und damit des Internets und deren Konsequenzen (welche IT-Services in welchen Unternehmensebenen sind betroffen und was kostet das?) auf die Unternehmenstätigkeit zu simulieren. Diese Möglichkeit ist durch unseren Ansatz zum Risikomanagement entlang von Wertschöpfungsketten gegeben.

Wir sind derzeit bei der Entwicklung eines Werkzeugs zur softwaregestützten Erfassung und Verarbeitung (Management) von Unternehmensrisiken, insbesondere aus dem Bereich der Informationstechnologie (IT). Die wissenschaftlichen Grundlagen zu diesem Werkzeug wurden bereits in [Sch03] vorgestellt – für die Lektüre von Details sei hierauf verwiesen. Die Besonderheit des dort vorgestellten Ansatzes ist es, Kostenaspekte und Planspiele zu Kosten-/Nutzensituationen technisch unterstützt durchzuführen; er öffnet damit den „Elfenbeinturm" des Risikomanagements für die wesentlichen Geschäftsinteressen des Unternehmens.

4.1 Stand der Technik und Innovation

Der aktuelle Stand der Technik beim Risikomanagement kann wie folgt zusammengefasst werden: Zwar wird das Risikomanagement in Unternehmen bisher bereits von vielen Unternehmen prinzipiell ernst genommen und umgesetzt, jedoch erfolgt dies fast ausschließlich durch IT-Spezialisten und in Papierform. Diese konzentrieren sich bei ihrer Tätigkeit zu stark auf IT-Elemente und lassen dabei deren Verbindung zu Geschäftsprozessen bzw. zur Wertschöpfungskette des Unternehmens außer Acht. Manager dagegen orientieren sich bei ihren Investitionen entlang der Wertschöpfungskette des Unternehmens. Hier entsteht darum fast immer eine Diskrepanz; das Risikomanagement in einem Unternehmen wird deshalb derzeit auf verschiedenen Unternehmensebenen getrennt und unabhängig voneinander betrachtet.

Darüber hinaus hat sich die Realisierung des Risikomanagements mit Hilfe von Dokumenten in Papierform (oder auch formlosen elektronischen Dokumenten) einerseits als zu zeit- und kostenintensiv, andererseits als zu fehleranfällig erwiesen.

Die Idee des Werkzeugs ist die Entwicklung eines Softwareprodukts, welches das Risikomanagement (Identifikation, Analyse und Bewertung) innerhalb eines Unternehmens papierlos, automatisiert und ebenenübergreifend realisiert, damit die oben genannten Nachteile behebt und sich entlang der Wertschöpfungskette des Unternehmens orientiert. Unsere Software wird folgende Eigenschaften realisieren:

- Konzentration des Risikomanagements auf Wertschöpfungsbereiche mit hoher Wertigkeit,
- Unternehmensebenenspezifisches Modellieren von Risiken und deren Attribute als Risikoknoten (RiskNodes),
- Modellieren von horizontalen Abhängigkeiten zwischen Risiken innerhalb einer Unternehmensebene (Risikointerdependenzen) in Form von Risikodiagrammen (RiskCharts),
- Modellieren von vertikalen (unternehmensebenenübgreifenden) Abhängigkeiten zwischen Risiken (Verfeinerung eines RiskNodes durch ein RiskChart),
- Schrittweises (ebenenweises) Vorgehen führt zu einer inkrementellen (und mathematisch korrekten) Verfeinerung der Verfügbarkeitsanforderungen; entsprechende Berechnungstemplates existieren,

- Automatisierte Risikonalyse (Single Points of Failure, Gesamtverfügbarkeit),
- Planspiele zur Simulation einer veränderten Risikosituation mit automatischer Kostenanalyse per Knopfdruck,
- Automatische Benachrichtigungsfunktion (Alerting) an den Owner des RiskNodes im Falle riskanter Verfügbarkeitsschwankungen,
- Top-down Propagierung der Verfügbarkeitsanforderungen kann (formal) der Bottom-up Propagierung der Risiken gegenübergestellt werden,
- Die Arbeitsgruppe zur Verbesserung der Verfügbarkeit eines Business Services kann direkt durch die RiskNode-Owner zusammengestellt werden.

Unsere Vorgehensweise beseitigt damit auch die vielschichtigen Kommunikationsschwierigkeiten zwischen den verschiedenen Unternehmensebenen: Die am Risikomanagement beteiligten Personen aus unterschiedlichen Unternehmensbereichen verwenden bisher stets unterschiedliche Terminologien, haben unterschiedliche Ziele und definieren die auf ihrer Ebene entstehenden Risiken unabhängig voneinander und ggf. inkompatibel zueinander. Durch eine einheitliche Nomenklatur sowie ein einheitliches mathematisches Systemmodell in der Software werden Risikointerdependenzen und -aggregationen transparent und vergleichbar gemacht.

Unser Ansatz greift bereits bei der Risikoidentifikation. Die erste Stufe der Risikoidentifikation beginnt in der Regel mit der betriebsspezifischen Erfassung *aller* auf die Unternehmensziele wirkenden Risiken (Risiko-Brainstorming) – siehe Abbildung 4.1. Dabei werden im Stand der Technik quasi in einem „Rundumschlag“ alle nur erdenklichen Risiken erfasst. Bei dieser Vorgehensweise muss damit gerechnet werden, dass ein Großteil der auf diese Weise erfassten Risiken keinen oder einen nur unwesentlichen Einfluss auf die für das Kerngeschäft relevanten Wertschöpfungsketten hat. Um die Ressourcen optimal einzusetzen, beschränkt sich unsere Vorgehensweise auf solche Risiken, die eine potentielle Gefährdung von Wertschöpfungsketten darstellen; die Gefährdung selbst wird dabei technisch gestützt quantifiziert. Uninteressante Pfade können so „abgeschnitten“ werden und Schieflagen in der Wahrnehmung der Wichtigkeit von Geschäftsprozessen werden aufgezeigt und können gelöst werden (vgl. Abbildung 4.2).

Weitere Einsparpotentiale kann das Werkzeug durch die Einbindung bereits bestehender Risikoinformationen aus System Management Tools, dem Notfall- und Katastrophenplan, dem Inventory, dem Asset Management, dem Netzwerkmanagement usw. durch flexible Schnittstellen realisieren.

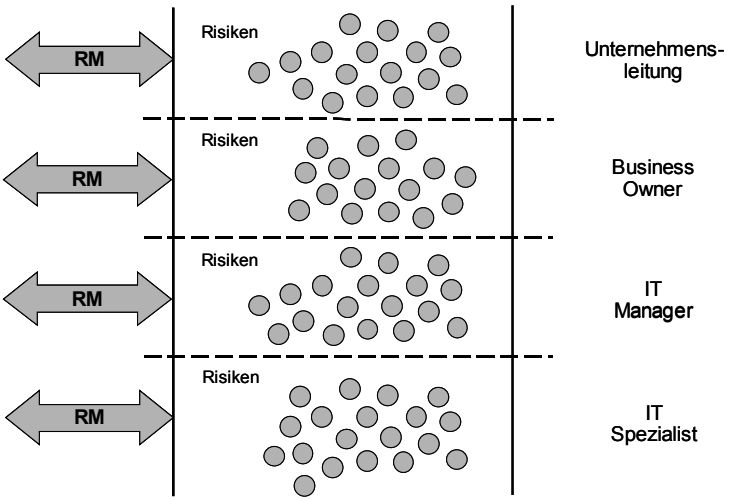

Abbildung 4.1: Stand der Technik: separates Risikomanagement verschiedener Unternehmensebenen

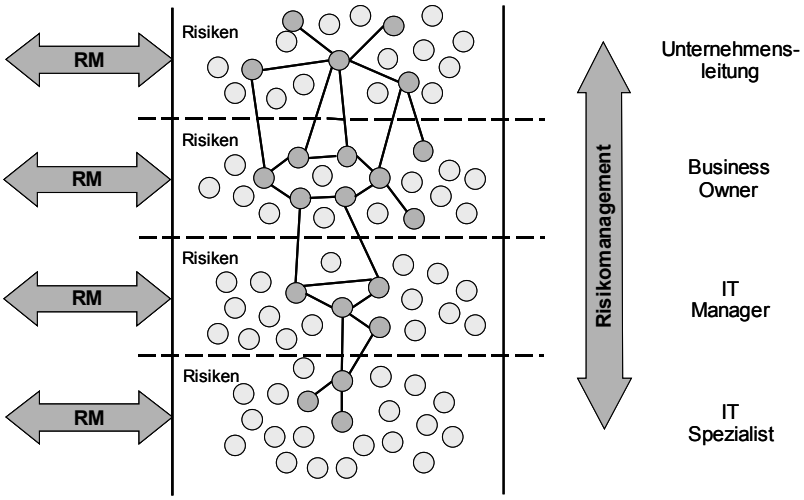

Abbildung 4.2: Innovation: Risikomanagement entlang von Wertschöpfungsketten

4.2 RiskNodes und RiskCharts

Zunächst werden diejenigen Komponenten der technischen, informationstechnischen und baulichen Infrastruktur herausgefiltert, von deren Funktionsfähigkeit die Verfügbarkeit der kritischen Geschäftsanwendungen (ebenfalls als RiskNodes modelliert) und zentralen Funktionen abhängig ist. Diese Art der Modulbildung kann bzgl. der Informa-

tionstechnologie (IT) auf jeder Unternehmensebene getroffen werden, also insbesondere auf Ebene der Geschäftsprozesse, der IT-Services sowie der Ressourcen. Bei diesen Komponenten kann es sich beispielsweise um einen Dienst, die Steuerung eines Produktionsabschnittes, einen Webserver, einen Datenbankserver, den Hauptverteiler der Telekommunikation, die Stromeinspeisung, ein automatisiertes Kleinteilelager, einen Tresorraum und vieles andere mehr handeln. Jeder RiskNode besitzt einen Verantwortlichen, den sogenannten Owner.

Ein RiskChart beschreibt die Abhängigkeiten zwischen RiskNodes und kann mathematisch als gerichteter Graph $G=(V1 \cup V2,E)$ modelliert werden, der die Abhängigkeiten verschiedener RiskNodes untereinander formal beschreibt, wobei V die disjunkte Vereinigung der Menge der RiskNodes V1 und der Menge der Verknüpfungssymbole/-operatoren $V2=\{\wedge,\vee\}$ darstellt.

Zwei Knoten i und j aus V sind durch eine Kante $(i,j) \in E$ verbunden genau dann wenn der RiskNode j vom RiskNode i abhängig ist (Beispiel: Applikationsserver hängt vom Datenbankserver oder dessen Hot-Standby ab) oder einer der beiden Knoten ein Verknüpfungssymbol aus V2 darstellt.

Um RiskNodes zu RiskCharts zu komponieren, gibt es folgende Möglichkeiten:

- Die serielle Komposition: Abhängigkeit des Knotens vom Vorgängerknoten
- Die parallele Und-Verknüpfung ($\wedge$): Gleichzeitige Abhängigkeit des Knotens von mehreren Vorgängerknoten
- Die parallele Oder–Verknüpfung ($\vee$): Alternative Abhängigkeit des Knotens von mehreren Vorgängerknoten

4.3 Ein Unternehmensebenen übergreifender Verfeinerungsbegriff

Ein RiskChart $G=(V1 \cup V2, E)$ verfeinert einen RiskNode v (Beispiel: Druckservice) genau dann wenn das Zusammenspiel aller RiskNodes aus G eine feingranularere Beschreibung von v darstellt (Beispiel: dieser Druckservice wird erzielt durch das Zusammenspiel von Druckserver, DB-Server nebst Standby-Server und Applikationsserver) und wenn die absolute Verfügbarkeit von G jederzeit mindestens die ursprünglich spezifizierte Verfügbarkeit von v erreicht. Erreicht sie diesen Wert, wird von einer korrekten Verfeinerung gesprochen. Erreicht sie diesen Wert nicht, so ist ein einfacher Indikator gefunden, der Handlungsbedarf signalisiert.

Dieser Verfeinerungsbegriff besitzt die beiden wesentlichen Eigenschaften der (a) Kompositionalität und (b) Transitivität. Sie stellen sicher, dass (a) eine lokale Verfeinerung ebenfalls global betrachtet eine Verfeinerung darstellt und (b) eine schrittweise Anwendung vieler Verfeinerungsschritte über viele Unternehmensebenen hinweg möglich ist. Die schrittweise Verfeinerung liefert als Resultat eine Hierarchie von RiskCharts, eine sogenannte **Risikolandschaft**, welche die Verfügbarkeit jeder Unternehmensebene widerspiegelt (siehe Abbildung 4.3).

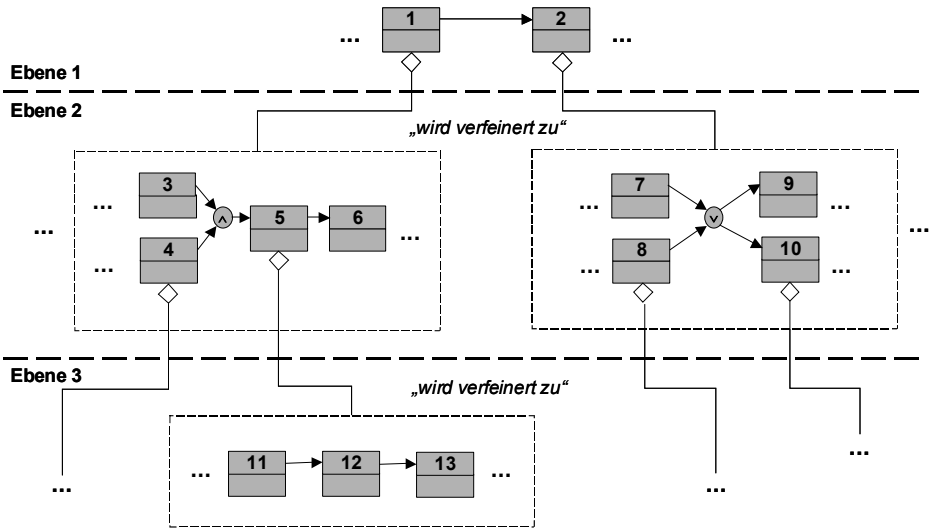

Abbildung 4.3: Verfeinerung über mehrere Unternehmensebenen hinweg

5 Analyse der Incidentauswirkungen innerhalb des Unternehmens

In diesem Abschnitt zeigen wir, wie proaktives Risikomanagement und Incident Management, also mit anderen Worten reaktives Risikomanagement, zusammengeführt und so auf Basis einer einheitlichen Plattform betrachtet werden können. Dazu gehen wir im Folgenden davon aus, dass die ebenenübergreifende Risikolandschaft eines Unternehmens bereits anhand von RiskNodes und RiskCharts sowie deren Verfeinerungsbeziehungen untereinander erfasst wurde, wie in Abbildung 4.3 skizziert. Hier wurde bewusst das Rautensymbol zur grafischen Darstellung der Verfeinerung gewählt, weil es sich zum einen bei der UML-Vererbungsbeziehung, symbolisiert durch eine Pfeilspitze, nicht um eine Verfeinerung auf semantischer, sondern nur syntaktischer Basis handelt und zum anderen unser Verfeinerungsbegriff auch als „besteht aus“-Relation, in der UML dargestellt durch ein Rautensymbol, interpretiert werden kann.

Würde nun die Firewall (z.B. linkster RiskNode 11 aus Ebene 3 in Abbildung 4.3) komplett gesperrt werden müssen, so könnte man die Auswirkungen auf die davon abhängigen IT-/Business-Services simulieren und sogar kostenmäßig bewerten. Außerdem werden alle betroffenen Owner dieser Services automatisch, beispielsweise per Email oder SMS, über den Incident bzw. die eingeleitete Maßnahme verständigt. In diesem konkreten Fall könnte man anhand der ebenenübergreifenden Risikolandschaft leicht feststellen, dass von der Sperrung der Firewall auch die RiskNodes 12, 13 (Ebene 3) und 5, 6 (Ebene2) sowie 1, 2 (Ebene 1) betroffen wären.

6 Zusammenfassung

Wir haben einen Ansatz zur Optimierung des Incident-Managements vorgestellt, der zur Bewertung der Verbindlichkeit von Vorfallsmeldungen bereits im Vorfeld des Incidents organisationsübergreifende Vertrauensketten analysiert. In einem zweiten Schritt können die Auswirkungen des Incidents auf alle abhängigen Services in allen betroffenen Unternehmensebenen simuliert werden. Dieser Teil des Verfahrens basiert auf einer Vorgehensweise zum Risikomanagement entlang von Wertschöpfungsketten [Sch03] und verbindet damit Risiko- und Incident Management zu einer ganzheitlichen Lösung, sodass wir in Summe folgende Ziele erreichen:

- Sicherstellung der Vorfallsaufnahme und deren Dokumentation,
- Weiterleiten von Vorfallsinformationen über entweder die kürzesten oder die sichersten Vertrauensketten,
- Verbesserung der Vorfallsbearbeitung und –kontrolle,
- Verbesserung der Vorfallsklassifikation und -bewertung (Vorfallsart, -ausmaß, -lokation und Verbindlichkeit der Vorfallsinformation) und ggf. Festlegung einer Priorisierung,
- Verbesserung der Vorfallsbeseitigung, ggf. Weiterleitung des Vorfalls über sichere Vertrauensketten,
- Monitoring zur Vorfallsbehebung, automatisches Erstellen von Incident-Statistiken und Rückführung dieser Daten ins aktive Risikomanagement,
- Einleitung verbindlicher Eskalationsstrategien und deren Bewertung,
- Benachrichtigung aller betroffenen Unternehmenseinheiten in allen Ebenen mithilfe der Informationen aus dem RiskChart.

Der erste Schritt zur Umsetzung unserer Vorschläge in einer Organisation besteht nun darin, diejenigen Partnerorganisationen, welche Informationen über Incidents liefern, explizit aufzulisten. Mit ihnen zusammen kann sodann die Verbindlichkeit von Kommunikationswegen untersucht werden um ggf. Maßnahmen zu deren Qualitätsverbesserung einzuleiten.

7 Literaturverzeichnis

[BDS02] Der Bundesbeauftragte für den Datenschutz: Tätigkeitsbericht 2001–2002, 19. Tätigkeitsbericht, Bundestagsdruckssache 15/888, Berlin, 2002.

[BSI03] BSI, CERT Bund: Handout zur Präsentation auf der CeBIT 2003, Seite 8, 2003.

[Eck03] Eckert, Claudia: IT-Sicherheit (Konzepte – Verfahren – Protokolle). Oldenbourg Verlag, München – Wien, 2003.

[Moe97] Mörl, Ramon: Chipkarten – Infrastruktur für eine Sicherheitsarchitektur. Konferenzband zur ChipCard 1997 (Computas), Seeheim-Jugenheim, 29.-30. September 1997.

[Rie03] Riedl, Thorsten: Voraussicht zahlt sich im Notfall aus. Computer Zeitung Nr. 28 vom 7. Juli 2003, Konradin-Verlag, Juli 2003.

[Sch02] Schneider, Adrian: Konzeptionelle Gestaltung von Organisationsstrukturen und Prozessmodellen in der IT-Sicherheit. Konferenzband zur OmniSecure 2002, Berlin, 18. und 19. Juni 2002.

[Sch03] Scholz, Peter: Risikomanagement entlang von Wertschöpfungsketten. Konferenzband zur Computas 2003, Fachkonferenz für Risikomanagement, Karlsruhe, 19.–20. Mai 2003.

[WIK03] WIK Security Enquete. WIK 2/2003, Zeitschrift für die Sicherheit der Wirtschaft, 2003.