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

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.

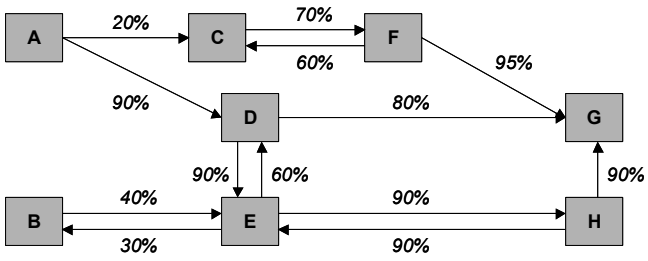

Abbildung 3.1: Organisationsübergreifendes Vertrauensnetz

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.

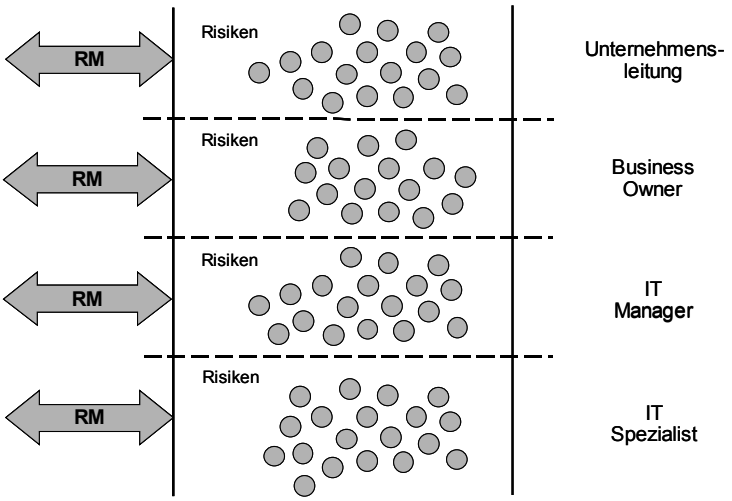

Abbildung 4.1: Stand der Technik: separates Risikomanagement verschiedener Unternehmensebenen

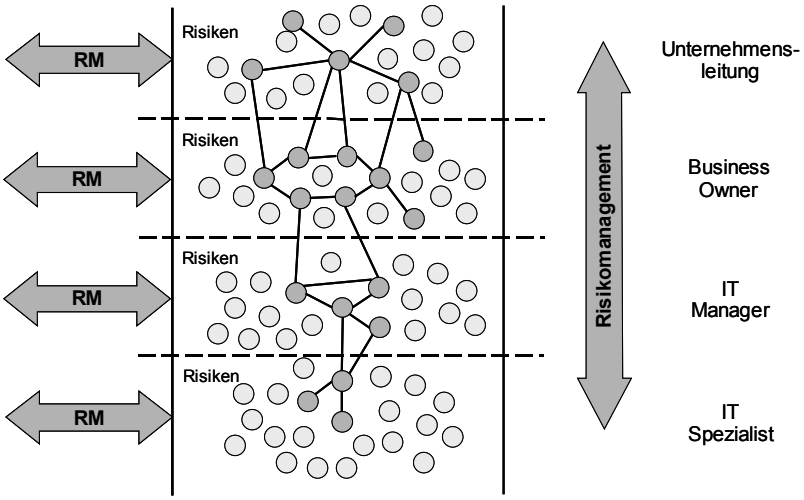

Abbildung 4.2: Innovation: Risikomanagement entlang von Wertschöpfungsketten

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).

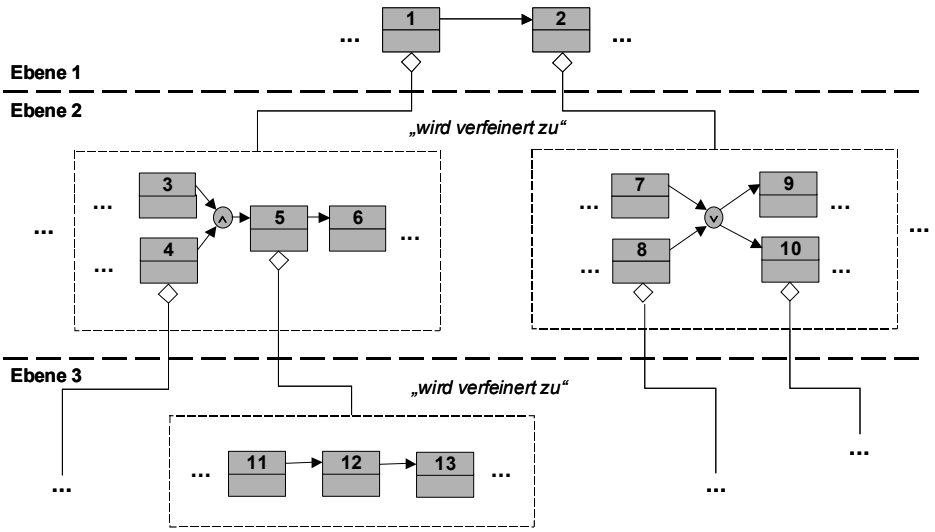

Abbildung 4.3: Verfeinerung über mehrere Unternehmensebenen hinweg

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.