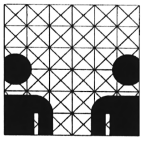
Einfluss von Incident Response auf die Erstellung von Notfallkonzepten

Diplomarbeit

Fachbereich Informatik
Universität Hamburg



Benjamin Hoherz

Betreuer:
Prof. Dr. Klaus Brunnstein
Dr. Hans-Joachim Mück

Hamburg, im September 2003

Danksagung

Während der Entstehung dieser Diplomarbeit haben mich zahlreiche Personen mit Gesprächen, Denkanstößen und Ermutigungen unterstützt. Mein Dank gilt insbesondere meinen Betreuern Professor Doktor Klaus Brunnstein und Doktor Hans-Joachim Mück. Außerdem möchte ich (in alphabetischer Reihenfolge) Karin Colsman, Jan Menne, Silvio Krüger, Karin Pape, Christian Paulsen, Kerstin Schwarze und ganz besonders meinen Eltern für ihre Unterstützung danken.

Einleitung

Seit Menschen auf der Erde leben ist ihre Existenz verschiedensten Risiken ausgesetzt. Zu Beginn der menschlichen Entwicklung bedrohte die Tierwelt, hartes Klima und Hungersnöte das Überleben der Gruppen oder des einzelnen Menschen. Später kamen Kriege, Seuchen und zahlreiche andere Einflüsse hinzu, die das Leben der Menschen bedrohten. Mittlerweile haben die moderne Technik und die extreme Ausbreitung des Menschen gewisse Risiken beseitigt und dafür neue geschaffen.

Das menschliche Leben ist eng verflochten mit der Abschätzung diverser Risiken für Leib, Leben und Besitz. Jeder Mensch sieht sich vor die Aufgabe gestellt, seine persönlichen Risiken zu kennen, mit ihnen zu leben und sie eventuell zu vermeiden oder zu reduzieren. Schafft er das nicht, können unerwünschte Ereignisse dazu führen, dass der Mensch Schaden an seiner Gesundheit, seinem Besitz, seinem Ansehen oder an anderer Stelle nimmt. Der Zusammenschluss von Menschen zu sozialen Gemeinschaften führte dazu, dass auch eine Gemeinschaft mit den Risiken klarkommen musste, die alle Mitglieder der Gruppe betrafen. Von Anfang an war und ist Risikomanagement ein wichtiger Teil des menschlichen Lebens.

Der technische und kulturelle Fortschritt der Gesellschaft hat die Lebensumstände der Menschen mit der Zeit verändert und damit auch die Menge an Risiken, denen einzelne Menschen oder Gruppen ausgesetzt waren. So hat beispielsweise die Erfindung des Speers dazu geführt, dass das Risiko des Verhungerns gemindert wurde, denn nun konnte Nahrung besser gejagt und erlegt werden. Gleichzeitig brachte der Speer das Risiko mit sich, dass Menschen nun andere Menschen leichter angreifen und töten konnten. Ähnliche Überlegungen lassen sich für zahlreiche Erfindungen und kulturellen Veränderungen anstellen. Eine Erfindung der jüngeren Geschichte hat jedoch das Risikomanagement weit stärker beeinflusst als die meisten anderen Veränderungen, die während dieser Zeit eintraten: Die Erfindung des Computers.

Mit einem Computer und später mit einem Computernetzwerk konnten viele Aufgaben, die bislang ein Mensch ausführen musste, auf eine Maschine abgewälzt werden. Die Möglichkeiten, komplizierte Berechnungen in kurzer Zeit anzustellen, große Mengen von Daten auf wenig Platz zu speichern, rund um die Welt in Echtzeit zu kommunizieren, sind nur einige Eigenschaften dieser Erfindung, die das Leben der Menschen maßgeblich erleichterten. Mit dem zunehmenden Einsatz von Computern und Computernetzwerken gerieten Menschen wie auch Organisationen zunehmend in eine Abhängigkeit von ihren IT Systemen[1]. In jüngerer Zeit gerieten sie auch in eine Abhängigkeit vom Internet. Daraus resultiert ein verheerendes Schadenspotential für die Risiken, die mit dem Einsatz von IT Systemen verbunden sind.

Aus der Evolution der menschlichen Kultur folgt bereits die Erkenntnis, dass auch die Erfindung des IT Systems ebenso wie alle Neuerungen neue Risiken schaffen musste. Das IT

[1] Der Begriff IT System wird synonym sowohl für einzelne Computer als auch für Netzwerke verwendet.

System steht in punkto Sicherheit in einer Linie mit früheren Erfindungen, da während seiner Entwicklung nur sehr wenig Augenmerk auf die Vermeidung von Risiken gelegt wurde, wie dies bei zahlreichen Erfindungen anfangs der Fall war. Dies wird heutzutage vor allem daran deutlich, dass das Internet zwar von fast allen Organisationen für sensible Operationen genutzt wird, aber kaum über Schutzmechanismen verfügt. Diese werden erst in jüngerer Zeit nachträglich in die Systeme eingebaut. Beispiele hierfür sind Firewalls, Virenscanner, digitale Signaturen, verbesserte Kommunikationsprotokolle usw.

Seit Computer von einer breiten Masse von Menschen und Organisationen genutzt werden, gibt es immer wieder Vorfälle, bei denen im Umfeld des IT Systems ein immaterieller und in selten Fällen auch ein materieller Schaden für dessen Benutzer eintritt. Vor allem seit das Internet großflächig zum elektronischen Geschäftsverkehr genutzt wird, ist das IT System geradezu die Achillesverse zahlreicher Organisationen. Denn IT Systeme werden nicht nur durch Fehler und zufällige Ereignisse bedroht. Auch Angreifer haben die „Schwachstelle Computernetzwerk“ längst erkannt und nutzen sie tagtäglich aus, um vorsätzlich Schaden anzurichten.

Wenn ein Risiko nicht komplett ausgeschaltet werden kann, bietet es sich an, im Voraus zu planen, was im Falle eines schädigenden Ereignisses getan werden soll. Maßnahmenkataloge zur Reaktion auf Schadensereignisse werden Notfallkonzepte genannt und sind schon seit langem fester Bestandteil des Risikomanagements, beispielsweise als Katalog für Sofortmaßnahmen bei einem Feuer. Seit der Ausbreitung der IT Systeme haben die Organisation zahlreiche neue Notfallkonzepte schreiben müssen, um auch auf IT Vorfälle vorbereitet zu sein.

Leider steht die Entwicklung von Notfallkonzepten für IT Vorfälle vor einer Reihe von Schwierigkeiten. Das IT System ist noch immer eine relativ neue Erfindung und noch dazu eine, die ständig weiterentwickelt wird und immer breitere Anwendung findet. Deshalb ist die Gültigkeit und Durchführbarkeit eines Notfallkonzeptes für IT Vorfälle oft nur von kurzer Dauer. Spätestens mit der nächsten Systemumstellung müssen sie neu oder umgeschrieben werden. Hinzu kommt, dass zahlreiche mögliche Vorfälle im IT Bereich entweder noch nicht bekannt sind oder die Warnungen vor ihnen (mangels technischen Verständnisses) nicht ernst genug genommen werden. Das alles führt dazu, dass es in den letzten Jahren immer wieder zu spektakulären Vorfällen im IT Bereich gekommen ist. Genannt sei hier der Internetwurm, der im Jahr 1988 als erster großflächiger IT Vorfall die gesamte Internetkommunikation in den USA für drei Tage lahm legte. Aber nicht nur großflächige Angriffe wie das Ausbreiten von Würmern treten auf, sondern auch gezielte Attacken gegen einzelne Organisationen oder Personen. Zusätzlich zu Angriffen gibt es noch die Risiken, die aufgrund anderer Ursachen für IT Systeme bestehen, etwa Stromausfälle, Fehlbedienung u.v.a.

Möglichkeiten, in Zusammenhang mit einem IT System Schaden zu erleiden, gibt es also genug. Dies steht dem Missstand gegenüber, dass das Formulieren und Umsetzen geeigneter Notfallkonzepte schwierig ist. Es stellt sich daher die Frage, ob es Möglichkeiten zur Verbesserung der Situation gibt.

Seit dem Internetwurm gibt es in der Welt der IT Systeme eine Entwicklung von Teams, die sich der Behandlung von Computervorfällen widmet. Diese als „Incident Response Teams“ bekannten Gruppen arbeiten an unterschiedlichen Stellen und bieten eine Vielzahl von Diensten an (siehe Kapitel 2 und 3). Einige von ihnen wurden von Organisationen speziell zu dem Zweck gegründet, ihre Mutterorganisation bei Computervorfällen zu unterstützen.

Die vorliegende Arbeit beschäftigt sich mit der Frage, ob und wieweit die Tätigkeiten, die als Incident Response bekannt sind und am häufigsten von Incident Response Teams ausgeführt werden, dazu beitragen zu können, auf Notfallkonzepte im IT Bereich konstruktiv einzuwirken. Es wird untersucht, welche Möglichkeiten und Grenzen ein Incident Response Team dabei hat, eine Organisation bei der Erstellung, Durchführung und Verbesserung eines Notfallkonzepts zu unterstützen. Dazu wird zunächst in Kapitel 1 das traditionelle Risikomanagement vorgestellt, von dem das Notfallkonzept einen Teilaspekt darstellt. Es wird am Ende des Kapitels gesondert vorgestellt werden. Kapitel 2 gibt einen Überblick über die Historie von Incident Response Teams und stellt die verschiedenen Typen derselben dar. Im dritten Kapitel werden die einzelnen Dienstleistungen der Incident Response Teams näher beschrieben, und einige mögliche Auswirkungen dieser Dienste werden vorgestellt. Kapitel 4 gibt einen groben Überblick darüber, in welchem Rahmen Incident Response Teams auf Notfallkonzept einwirken können und wo die Grenzen liegen. Im fünften Kapitel wird dieser grobe Rahmen anhand von Szenarien ausgefüllt. Hier werden für ausgewählte Vorfälle die Einflussmöglichkeiten des Incident Response Teams auf das Notfallkonzept untersucht und diskutiert.

1. Vom Risiko zum Notfallkonzept

In diesem Abschnitt werden zunächst die für das Verständnis von Risikomanagement und Notfallkonzepten nötigen Grundbegriffe erläutert. Außerdem werden die für die Erstellung eines Notfallkonzeptes erforderlichen Maßnahmen und Inhalte dargestellt. Vor allem die Risikoanalyse und das Risikomanagement, aus denen das Notfallkonzept letztlich hervorgeht, werden ausführlich erläutert.

1.1. Begriffsklärung: Risiko, Vorfall, Notfall, Notfallkonzept, Malware, Sicherheit

Maßgeblich für die Erstellung eines Notfallkonzeptes für ein System sind das Aufspüren und Analysieren von Risiken für das System. Deshalb muss zunächst einmal der Begriff des Risikos in seiner Bedeutung dargestellt werden. Ferner werden in diesem Abschnitt die Begriffe Vorfall, Notfall, Notfallkonzept, Malware und Sicherheit definiert.

1.1.1. Risiko

Der Begriff Risiko stammt aus dem Italienischen und bezeichnet „die mit einem bestimmten Verhalten verknüpfte Gefahr“ [Knaur]. Diese Definition ist für den hier dargestellten Kontext zu allgemein; hier soll der Begriff im Zusammenhang mit IT Systemen definiert werden. Entsprechend könnte die Definition lauten „Risiko ist die mit dem Umgang eines IT Systems verbundene Gefahr“. Worin dabei die „Gefahr“ eigentlich besteht, kann sehr unterschiedlich sein. In der Tat braucht die Gefahr sich nicht auf das IT System selber zu beziehen, sondern kann auch für das Umfeld oder den Benutzer bestehen. Ebenso muss der Begriff „Umgang“ näher bestimmt werden. Er könnte hier sowohl die „normale“ Benutzung des Systems als auch die abnormale Benutzung des Systems umfassen. Was unter normaler Benutzung zu verstehen ist, wird im Regelfall in der Sicherheitspolitik definiert. Alles andere ist das abnormale Benutzung. Unter abnormale Benutzung fallen beispielsweise Fehlbedienung, Angriffe auf das System oder zufällige Ereignisse wie etwa ein Blitzschlag. Offensichtlich muss die Definition noch konkretisiert werden, um sauber mit ihr arbeiten zu können. Um den Risikobegriff besser fassen zu können, werden die Termini Schwachstelle (vulnerability) und Bedrohung (threat) eingeführt. Eine Schwachstelle wird gemäß [RFC 2828] wie folgt definiert:

Vulnerability: A flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's security policy.

Ebenfalls nach [RFC 2828] definiert sich die Bedrohung:

Threat: A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm.

Nach [Krallmann] besteht ein Risiko aus zwei Komponenten: Einer Schwachstelle und einer Bedrohung. Dabei muss die Bedrohung mit eben gerade dieser Schwachstelle gekoppelt sein. Nur wenn beides vorliegt, ist auch ein Risiko gegeben. Nach dieser Formel besteht beispielsweise ein Risiko, wenn die Tür eines Rechenzentrums nicht verschlossen werden kann (Schwachstelle), und ein potentieller Dieb draußen vor dem Rechenzentrum herumläuft (Bedrohung). Dazu ist es nicht nötig, dass der Dieb tatsächlich die Absicht hat, etwas aus diesem Rechenzentrum zu stehlen. Allein seine Existenz reicht nach dieser Definition für eine Bedrohung aus. Hätte das Rechenzentrum hingegen eine Hochsicherheitstür, die ein Dieb nicht überwinden kann, so bestünde kein Risiko, weil es an der Schwachstelle fehlte. Gäbe es hingegen den Dieb nicht, bestünde auch kein Risiko, da die Schwachstelle durch keinerlei Bedrohung ausgenutzt würde.

Analog zu [Krallmann] und entnommen aus [RFC 2828] wird das Risiko also definiert:

Risk: An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result.

Dieser Risikobegriff spricht von einer Möglichkeit des Verlustes durch ein schädigendes Ereignis. Damit ist die Möglichkeit eines Wertverlustes durch einen Schaden gemeint. Dies entspricht im Groben dem Risikobegriff von [Moses], der neben Bedrohung und Schwachstelle auch einen bedrohten Wert voraussetzt. Mögliche Schwachstellen und Bedrohungen sind nicht nur im System selber, sondern auch in seinem Umfeld zu suchen. So gehört ein Dieb in der Regel nicht zum System dazu, sondern stammt aus seinem Umfeld. Wie weit das Umfeld dabei gefasst wird, hängt davon ab, wie umfangreich die spätere Risikoanalyse werden soll. Beispiele für mögliche Schwachstellen und Bedrohungen folgen in den Unterabschnitten 1.2. zur Risikoverteilung und 1.3. Risikoanalyse.
Die Formel Risiko = Bedrohung + Schwachstelle + Wert hat lediglich qualifizierenden Charakter. Sie sagt nichts darüber aus, worin die konkrete Bedrohung besteht oder ob und wann sie sich verwirklicht. So beschreibt das Beispiel nicht, ob ein Dieb tatsächlich durch die unverschlossene Tür eindringt oder mit welcher Wahrscheinlichkeit er dies tut. Ebenso wird nichts darüber ausgesagt, ob und was er stehlen wird. Es ist daher angebracht, aus der Kombination von Bedrohung und Schwachstelle weitere Größen zu folgern und das Risiko als Abbildung zu verstehen.

Eine aus Bedrohung und Schwachstelle zu folgernde Größe ist die Wahrscheinlichkeit, mit der sich die Gefahr für das System oder sein Umfeld verwirklicht. Diese Wahrscheinlichkeit hat dabei einen Wert, der größer als 0 ist, da die Manifestation des Risikos ansonsten nicht mehr eintreten könnte und damit kein Risiko mehr bestünde. Um ein Risiko komplett auszuschalten, müsste dieser Wahrscheinlichkeitswert also durch geeignete Maßnahmen auf 0 reduziert werden. In dem Beispiel wäre dies die Wahrscheinlichkeit, mit der ein Dieb tatsächlich durch die unverschlossene Tür in das Rechenzentrum eindringt und dort etwas stiehlt. Die zweite wichtige Größe ist der angerichtete Schaden, also im Beispielsfall der Wert der gestohlenen Sache, die Folgekosten für die Wiederbeschaffung, der Verdienstausfall, weil das Rechenzentrum nicht mehr korrekt arbeiten kann usw. Wie bereits an diesem Beispiel zu sehen ist, kann die Ermittlung der tatsächlichen Größen recht schwierig sein. Unter Umständen können sich außerdem uneindeutige Schadenswerte ergeben, wenn die Betrachtung von Bedrohung und Schwachstelle zu grob angesetzt wird. So könnte der Dieb mit Wahrscheinlichkeit p1 einen Monitor stehlen, mit Wahrscheinlichkeit p2 eine Tastatur usw. Um eine funktionale Abbildung zu erhalten muss die Betrachtung sehr genau sein. Das folgende Beispiel stellt eine Konkretisierung des Falles dar:

Wenn die Tür zum Rechenzentrum kein Schloss hat (Schwachstelle) und in diesem Rechenzentrum die CD mit der Software XYZ unbewacht und frei zugänglich auf einem Tisch liegt (Wert) und ein potentieller Dieb draußen herumläuft (Bedrohung), dann wird dieser Dieb mit Wahrscheinlichkeit ¼ (Wahrscheinlichkeit) tatsächlich in das Rechenzentrum eindringen und die Software XYZ aus dem Rechzentrum stehlen (Schaden).
Aus diesen Überlegungen folgt die Definition des Risikos als Funktion:

Risiko: (Schwachstelle, Bedrohung, Wert) → (Wahrscheinlichkeit, Schaden)

Aus dieser Definition ergibt sich insbesondere die Konsequenz, dass unterschiedliche Bedrohungen auf dieselbe Schwachstelle zu unterschiedlichen Schäden führen können, die mit unterschiedlicher Wahrscheinlichkeit eintreten. Eine einzelne Schwachstelle kann also dazu führen, dass das System gleich mehreren Risiken ausgesetzt ist.

1.1.2. Vorfall

Kommen wir nun zum Begriff des Vorfalls (engl. i*ncident)*. Dieser ist für Notfallkonzepte von Bedeutung, da der Notfall eine Sonderform des Vorfalls darstellt, für den das Notfallkonzept spezielle Folgen vorsieht. Unter einem Vorfall ist zunächst einmal jedes beliebige Ereignis zu verstehen. Bezogen auf Sicherheit für IT Systeme wird der Vorfallsbegriff mit etwas negativem behaftet. Er steht für ein Ereignis, bei dem die Sicherheit des Systems beeinträchtigt wird. [RFC 2828] definiert:

security incident: A security event that involves a security violation.

Mit dem sicherheitsrelevanten Ereignis, von dem die Definition spricht, ist die Manifestation eines Sicherheitsrisikos gemeint. Um den Vorfallsbegriff für unsere Zwecke auch mit dem Risikobegriff zu verknüpfen, wird der Vorfall noch etwas konkreter definiert. Im Kontext der Risikoanalyse und der Notfallkonzepte soll der Vorfallsbegriff wie folgt verwendet werden:

Ein Vorfall ist das Ereignis, bei dem sich die in einem (Sicherheits-)Risiko innewohnende Gefahr für das System manifestiert, d.h. das Ereignis, bei dem der Schaden (in Form einer Sicherheitsverletzung) tatsächlich eintritt.

Mit dieser Definition wurde der Vorfall an das Risiko gekoppelt. Jedes Risiko kann somit, wenn es genau bestimmt wurde und das Schadensereignis eintritt, zu genau einem Vorfall führen. Diese stark mathematisch idealisierte Darstellung wird sich in der Praxis allerdings selten bestätigt finden, da die einzelnen Risiken schwer gegeneinander abzugrenzen sind.
Oftmals fällt die Abgrenzung zwischen einer Bedrohung, einem Vorfall und der bloßen Ausnutzung einer Schwachstelle (engl. e*xploit*) schwer. Die Ausnutzung einer Schwachstelle

ist ein Konstrukt, das zeitlich zwischen Risiko und Vorfall liegt. Sie bezeichnet die Manifestation der Bedrohung. In unserem Beispiel wäre ein tatsächlicher Dieb, der sich darauf vorbereitet hat, die Tür des Rechenzentrums zu öffnen und dort etwas zu stehlen, die Ausnutzung einer Schwachstelle. Die abstrakte Bedrohung durch den möglichen Dieb hat konkrete Gestalt angenommen, aber es liegt noch kein Vorfall vor. Abbildung 1 zeigt den zeitlichen Verlauf:

Phase	Beispiele
Risiko	Unverschlossene Tür + potentieller Dieb + Software hinter der Tür Oder Schwachstelle in einer Software + potentielle Existenz eines Konzepts, wie die Schwachstelle ausgenutzt werden kann + Diese Software und sensible Daten auf dem gleichen Rechner
Ausnutzung der Schwachstelle	Konkreter Dieb, der sich darauf vorbereitet, im Rechenzentrum einzubrechen Oder Trojanisches Pferd, das eben diese Schwachstelle in eben dieser Software ausnutzt.
Vorfall	Einbruch des Diebes Oder Einsatz des Trojanischen Pferdes auf dem Rechner mit der Schwachstelle

Abbildung 1: zeitlicher Verlauf vom Risiko zum Vorfall

1.1.3. Notfall

Bei vielen Vorfällen, die in existierenden IT Systemen eintreten, ist der angerichtete Schaden minimal. Denken wir einmal an eine versehentlich in den Papierkorb verschobene Datei, die wiederhergestellt werden muss, was der Benutzer auch unverzüglich tut. Hier besteht der Schaden lediglich aus einigen Sekunden Zeitverlust.
Für solche kleinen Schäden ist keine besondere Planung vonnöten. Sie werden problemlos im Alltag abgehandelt. Für Notfallkonzepte sind sie nicht relevant. Um Vorfälle, die eine besondere „Schadensbehandlung“ nötig machen, von unwesentlichen Vorfällen abzugrenzen, wird der Notfall definiert:

Ein Notfall ist ein Vorfall mit solchem Schadensausmaß, dass bereits vor seinem Eintritt die nötigen Schritte und Maßnahmen zur Schadensbeseitigung oder Prävention geplant werden müssen.

Es ist keine rein objektive Entscheidung, ob ein Vorfall als Notfall zu klassifizieren ist. Für eine Privatperson mag das Löschen eines selbstgemalten und auf Festplatte gespeicherten Hintergrundbildes einen Notfall darstellen, für ein Unternehmen könnte derselbe Vorfall keinerlei Bedeutung haben.

1.1.4. Notfallkonzept

Der letzte in diesem Abschnitt zu definierende Begriff ist der des Notfallkonzeptes. Das Notfallkonzept ist ein Katalog von möglichen Notfällen und für den Fall ihres Eintritts vorgesehenen Maßnahmen. Für seine Erstellung müssen die Notfälle natürlich zunächst einmal dargestellt und durchdacht werden. Dies ist deshalb sehr schwierig, weil der Sinn des Notfallkonzeptes ja in der Vorausplanung liegt und deshalb im Regelfall nicht auf Erfahrungen mit dem konkreten Notfall zurückgegriffen werden kann. Allerdings gibt es mitunter zumindest Erfahrungswerte aus ähnlich gelagerten Notfällen, auf die zurückgegriffen werden kann. Es wird definiert:

Ein Notfallkonzept ist eine Sammlung von möglichen Notfällen und dazugehörigen Maßnahmen, die nach Eintritt des Notfalls ergriffen werden sollen.

Wie der Wortlaut ja schon hergibt, beinhaltet ein Notfallkonzept keine Regeln für den Normalbetrieb eines Systems. Diese sind eher in einer Sicherheitspolitik zu finden, deren Beschreibung hier den Rahmen sprengen würde.
Die Maßnahmen zu jedem Notfall werden, wie oben beschrieben, im Idealfall vor dem Eintreten des Notfalls festgelegt und eventuell anhand von Simulationen des Notfalls auf ihre Wirksamkeit überprüft. Allerdings kann erst nach dem tatsächlichen Eintritt des Notfalls mit Sicherheit gesagt werden, ob die gewählten Maßnahmen überhaupt durchführbar sind und ob sie für den Notfall angemessen waren. Das Ziel dieser Arbeit besteht darin festzustellen, in welchem Umfang ein bestehendes Notfallkonzept durch vorausgeplante oder ähnliche Notfälle verbessert werden kann.
Für die Erstellung eines Notfallkonzeptes muss zunächst eine umfangreiche Risikoanalyse durchgeführt werden. Diese Risikoanalyse umfasst auch eine Schadensabschätzung und eine hochgerechnete Wahrscheinlichkeit des Eintritts eines Vorfalls. Allerdings muss nicht nur die Art und Höhe des Schadens bestimmt werden, sondern auch die Möglichkeiten, wie er wieder zu beseitigen ist, müssen im Voraus untersucht werden. Die näheren Einzelheiten für Risikoverteilung, Risikoanalyse und Erstellung eines Notfallkonzeptes werden in den nächsten Unterabschnitten dieses Kapitels dargestellt.

1.1.5. Malware

Ein letzter noch zu definierender Begriff ist der der Malware. Dieser wird benötigt, weil zahlreiche IT Vorfälle auf Angriffen basieren, die mit Hilfe von Malware durchgeführt

wurden. Der Begriff Malware setzt sich aus den Worten malicious (engl. für „bösartig“) und Software zusammen und bezeichnet eine Software, die eine nicht spezifizierte Funktion enthält. Diese Funktion wird Dysfunktion genannt und in [Brunnstein 99] wie folgt definiert:

A software or module is called "dysfunctional" when at least one function deviates from the specification.

Eine Dysfunktion kann absichtlich oder unabsichtlich in eine Software gelangen. Eine beabsichtigte Dysfunktion wäre beispielsweise eine nicht spezifizierte Funktion zur Formatierung der Festplatte in einem Textprogramm, die automatisch alle drei Wochen angestoßen wird. Eine unbeabsichtigte Dysfunktion kann etwa durch Spezifikationsfehler oder Programmierfehler in eine Software gelangen und zeigt sich in der Regel erst beim laufenden Betrieb der Software. Damit eine Software als Malware eingestuft wird, muss die Dysfunktion absichtlich in die Software integriert worden sein. In [Brunnstein 99] wird definiert:

A software or module is called "intentionally dysfunctional", when some essential feature is not contained in the manufacturer`s specification, whether formal or informal.

Absichtliche Dysfunktionalität wird also nur angenommen, wenn eine *wesentliche* Funktion der Software nicht in der Spezifikation des Herstellers enthalten ist. Im Gegensatz zur einfachen Dysfunktion wird bei einer Abweichung zwischen Software und Spezifikation bezüglich einer wesentlichen Funktion davon ausgegangen, dass diese nicht zufällig in die Software gelangt sein kann, sondern mit Absicht eingebaut worden sein muss.
Aufbauend auf der Definition der beabsichtigten Dysfunktionalität wird nun nach [Brunnstein 99] die Malware definiert:

A software or module is called "malicious" ("malware") if it is intentionally dysfunctional, and if there is sufficient evidence (e.g. by observation of behaviour at execution time) that dysfunctions may adversely influence the usage or the behaviour of the original software.

Damit eine Software zur Malware wird, müssen also zwei Bedingungen erfüllt sein. Zunächst muss die Software eine beabsichtigte Dysfunktion enthalten. Dabei kann sie entweder von Anfang an Teil der Software gewesen, aber auch durch fremde Einwirkung in eine vorher nicht maliziöse Software gelangt sein. Ein solcher Prozess, der aus normaler Software Malware macht, wird Kontamination genannt.
Die zweite Bedingung fordert, dass die Dysfunktion das Verhalten der Software oder ihre Brauchbarkeit zum spezifizierten Zweck beeinflusst. Durch diese Forderung wird beispielsweise ein Computerspiel, das nicht spezifizierte Funktionen zum Schummeln enthält,

gerade nicht zur Malware. Denn diese Funktionen beeinflussen weder das Verhalten noch die Brauchbarkeit in maßgeblicher Weise. Würde das Spiel hingegen eine versteckte Funktion haben, mit der die Festplatte formatiert wird, so würde diese Funktion das Verhalten des Computerspiels maßgeblich beeinflussen und es damit zur Malware machen.
Es gibt zahlreiche verschiedene Arten von Malware. Für diese Diplomarbeit sind drei Arten von Belang: Viren, Würmer und Trojanische Pferde.
Ein Virus ist ein selbstreplizierendes Programm, das sich dadurch verbreitet, dass es sich an ein anderes Programm anhängt. Diese von Viren verwendete Form der Kontamination wird Infektion genannt. Viren sind keine eigenständigen Programme, sondern existieren immer nur als Teil ihres Wirtsprogramms. Für die Infektion eines Wirtsprogramms gibt es verschiedene Methoden, die hier nicht näher erläutert werden sollen. [Brunnstein 99] definiert den Virus:

" A *computer virus* is a computer program which is able to replicate itself by attaching itself in some way to other computer programs. ... (The) two main properties of the computer viruses (are) —merely that a virus is able to replicate itself and that it does it by always attaching itself in some way to another, innocent program. This process of virus replication and attaching to another program is called *infection*. The other program, i.e., the program that is infected by the virus is usually called a *host* or a *victim* program."

Würmer haben ebenfalls die Fähigkeit zur Selbstreplikation, sind aber anders als Viren selbständige Programme. Würmer verwenden keine Wirtsprogramme, sondern versenden sich aktiv weiter. Üblicherweise geschieht dies über Netzwerke. Nach [Brunnstein 99] lautet die Definition für einen Wurm:

"Programs which are able to replicate themselves (usually across computer networks) as stand-alone programs (or sets of programs) and which do not depend on the existence of a host program are called computer *worms*."

Trojanische Pferde, oder einfach nur Trojaner, haben keine Funktion zur Selbstreplikation. Ein Trojaner besitzt eine nützliche Funktion oder täuscht diese vor, während dessen er eine absichtlich eingebaute, dem User im Regelfall unbekannte Schadfunktion ausführt. [Brunnstein 99] definiert:

"A *Trojan Horse* is a program which performs (or claims to perform) something useful, while in the same time intentionally performs, unknowingly to the user, some kind of destructive function. This destructive function is usually called a *payload*."

1.1.6. Sicherheit

Zur Definition des Sicherheitsbegriffs orientiert sich die Arbeit an [Pfleeger] und [RFC 2828]. Allgemein wird unter Sicherheit ein Zustand verstanden, in dem auf ein System keinerlei Bedrohungen schädigend einwirken können. In [RFC 2828] wird definiert:

Security: The condition of system resources being free from unauthorized access and from unauthorized or accidental change, destruction, or loss.

Um diesem allgemeinen Sicherheitsbegriff Substanz zu geben, wird der Sicherheitsstand eines Systems nach [Pfleeger] über drei Größen bestimmt: Vertraulichkeit, Verfügbarkeit und Integrität. Sie werden ebenfalls nach [RFC 2828] definiert. Zunächst die Vertraulichkeit:

confidentiality: The property that information is not made available or disclosed to unauthorized individuals, entities, or processes

In einem System, das Vertraulichkeit gewährleistet, dürfen Informationen nicht für Unbefügte zugänglich sein. Die Definition der Verfügbarkeit:

Availability: The property of a system or a system resource being accessible and usable upon demand by an authorized system entity, according to performance specifications for the system

Ein verfügbares System oder eine verfügbare Systemressource ist also für autorisierte Benutzer zugänglich und für die spezifizierten Aufgaben benutzbar. Als letztes die Definition der Integrität:

Integrity: The property that [system resources have] not been changed, destroyed, or lost in an unauthorized or accidental manner

Integrität ist die Eigenschaft einer Systemressource, nicht durch unerlaubten oder versehentlichen Zugriff verändert oder zerstört worden zu sein.
Nach [Pfleeger] definieren diese drei Größen gemeinsam die Sicherheit eines Systems. Zur Beurteilung, ob ein System sicher ist, werden üblicherweise an die drei Größen gewisse Anforderungen gestellt. Werden alle Anforderungen bei allen Größen erfüllt, so gilt das System unter den gegebenen Voraussetzungen als sicher. Sicherheit ist somit ein relativer Begriff. Dasselbe System kann in einem Einsatzkontext sicher sein, in einem anderen jedoch nicht. Als Beispiel sei eine Steuerungssoftware genannt, die im Schnitt alle 10 Tage einmal abstürzt und einen Neustart des Rechners erfordert, ansonsten aber tadellos funktioniert. Der alle 10 Tage stattfindende Systemabsturz ist eine Beeinträchtigung der Verfügbarkeit der Software. Wenn ein Privatnutzer mit dieser Software seine Modelleisenbahn steuert, werden

seine Anforderungen an die Verfügbarkeit der Software erfüllt werden, denn ein Neustart alle 10 Tage ist für eine Modelleisenbahn unkritisch. Wird mit der Software hingegen ein Atomkraftwerk gesteuert, ist ein Ausfall der Verfügbarkeit alle 10 Tage nicht hinnehmbar. Somit ist das System für eine Modelleisenbahn (bezüglich der Verfügbarkeit) sicher, für ein Atomkraftwerk aber nicht.
Um die Sicherheit eines Systems zu beurteilen und mathematisch zugänglich zu machen, wird in der Praxis wird häufig der Begriff des Sicherheitsniveaus verwendet. Dieser Abschnitt orientiert sich an [Pfleeger] und [Menne].

Ein Sicherheitsniveau ist ein Vektor aus Werten für Vertraulichkeit, Verfügbarkeit und Integrität.

Das Sicherheitsniveau eines Systems gibt an, welchen Grad an Vertraulichkeit, Verfügbarkeit und Integrität das System bietet. Die durch den Einsatzkontext gestellten Anforderungen in den drei Größen werden ebenfalls in Form eines Sicherheitsniveaus angegeben. Die Werte des Systems werden dann zur Beurteilung der Sicherheit paarweise mit den Werten des geforderten Sicherheitsniveaus verglichen. Sind alle drei Werte des Systems mindestens genauso hoch wie die entsprechenden Werte in den Anforderungen, so liegt das tatsächliche Sicherheitsniveau des Systems über oder auf dem geforderten Sicherheitsniveau: Das System ist sicher. Liegt mindestens einer der Werte des Systems unter den Anforderungen, so ist das Sicherheitsniveau des Systems niedriger als das geforderte Sicherheitsniveau. Das System ist unsicher.
Wenn ein System durch einen Vorfall oder Notfall einen Schaden in Form einer Sicherheitsverletzung erleidet, so wird der Wert des Systems in einer oder in mehreren der drei Größen beeinträchtigt. Dadurch wird das Sicherheitsniveau des Systems herabgesetzt. Für eine detailliertere Betrachtung des Sicherheitsbegriffs sei auf [Menne] verwiesen. Für die Zwecke dieser Diplomarbeit reicht die dargestellte Begriffstiefe aus.

1.2. Risikoverteilung

Bevor die Konzepte zur Risikoanalyse vorgestellt werden, folgen einige Anmerkungen zur Risikoverteilung. Unter Risikoverteilung wird die Wahrscheinlichkeitsverteilung in einem Raum von mehreren Risiken verstanden. Ist für jedes einzelne Risiko die Wahrscheinlichkeit des Schadenseintritts gleich groß, so wird dies eine Gleichverteilung genannt. Wie die betrachteten Risiken dabei in Beziehung zueinander stehen, soll zunächst einmal offen gelassen werden.
Für die Risikoanalyse eines Systems ist es besonders hilfreich, wenn in Räumen von ähnlichen Risiken eine Gleichverteilung herrscht, da diese Risiken dann in der Risikobewertung zu Gruppen zusammengefasst werden können.

Als Beispiel dient ein Rechenzentrum mit zwanzig Rechnern, die nahezu identische Aufgaben haben und sich deshalb in Hardware- und Softwareausstattung fast gleichen. Jeder dieser Rechner habe dieselbe Schwachstelle in einer Software, die sich auf allen Rechnern befindet. Diese Schwachstelle werde zudem von Malware ausgenutzt, die Daten auf den Rechnern ausspioniert. Für jeden Rechner besteht dann ein Risiko, das den Risiken für die anderen Rechner nahezu gleicht. Es hat dieselbe Bedrohung und dieselbe Schwachstelle. In einem solchen Fall werden bei der Risikoanalyse die Risiken für die einzelnen Rechner oft als gleich betrachtet und somit wird eine Gleichverteilung angenommen. Dann braucht die Risikobewertung für die zwanzig Rechner nur einmal durchgeführt zu werden, anstatt das Risiko für jeden Rechner einzeln zu bewerten.
In der Praxis ist es allerdings oft so, dass eine angenommene Gleichverteilung in Wirklichkeit so nicht besteht. Unterscheiden sich im Beispielfall die Rechner etwa durch ihre Netzwerkkarte, so kann die Wahrscheinlichkeit des Schadenseintritts von Rechner zu Rechner stark variieren, da unterschiedliche Treibersoftware u.ä. Einfluss ausüben kann. Es muss also genau abgewogen werden, in welchen Bereichen eines betrachteten Systems eine Gleichverteilung der Risiken angenommen werden kann. Die Grenze des Systems oder Systemausschnitts, der untersucht wird, wird „ Security Perimeter“ genannt [Brunnstein 02]. Der Security Perimeter ist im Regelfall sehr eng zu wählen, um den Umfang der Risikoanalyse überschaubar zu halten, sodass nur selten größere Gruppen von Risiken gemeinsam bewertet werden können.

1.3. Risikoanalyse

Die Risikoanalyse ist Teil des Risikomanagements [Stelzer]. Allerdings kann sie auch ohne die weiteren Schritte des Risikomanagements durchgeführt werden, wenn die Risiken lediglich ermittelt, aber nicht bekämpft werden sollen. Dies ist vor allem für Risiken mit geringem Schadenspotential von Bedeutung, da diese eventuell tragbar sind, aber dennoch bekannt sein müssen. Deshalb wird die Risikoanalyse losgelöst vom Rest des Risikomanagements erläutert. Ihr Ziel besteht darin, Risiken im System aufzuspüren, zu klassifizieren und eventuell zusammenzufassen und schließlich zu bewerten. Bei der Risikoanalyse geht es noch nicht darum, Maßnahmen im Sinne eines Notfallkonzeptes zu ermitteln. Es werden lediglich die Risiken selbst, insbesondere ihre Schadenswirkung, betrachtet und abgeschätzt. [RFC 2828] definiert die Risikoanalyse wie folgt:

risk analysis:
A process that systematically identifies valuable system resources and threats to those resources, quantifies loss exposures (i.e., loss potential) based on estimated frequencies and costs of occurrence, and (optionally) recommends how to allocate resources to countermeasures so as to minimize total exposure.

Wie zu sehen, betrachtet [RFC 2828] die Erarbeitung von Gegenmaßnahmen als optional. Diese erfolgt nach der hier vertretenen Ansicht von [Stelzer] und [Krallmann] erst nach der Risikoanalyse, also im zweiten Teil des Risikomanagements.
Für die Risikoanalyse gelten bestimmte Grundannahmen, auf denen jede Risikoanalyse aufbaut. Nach [Stelzer] lauten sie:

- Die Struktur, die Bedeutung und das Umfeld der Informationsverarbeitung sowie die zu schützenden Werte sind in vielen Organisationen sehr verschieden.
- Selbst innerhalb komplexer Organisationen gibt es sehr unterschiedliche Sicherheitsanforderungen.
- Deshalb gibt es für die wenigsten Bereiche, in denen Informationsverarbeitung betrieben wird, Standardvorschläge für angemessene Sicherheitsmaßnahmen.
- Der Bedarf an Sicherheitsmaßnahmen muss durch eine detaillierte Analyse der Risiken ermittelt werden.
- Ein angemessenes Sicherheitskonzept lässt sich in den meisten Fällen nur durch die Analyse der Risiken und die darauf bauende Auswahl von Sicherungsmaßnahmen erzielen.

In diesem Katalog fehlt eine weitere Grundannahme, nämlich die, dass in jeder Organisation Risiken bestehen. Fügt man sie dem Katalog hinzu, so zeigen die Grundannahmen, dass jede Organisation einer Risikoanalyse bedarf, wenn sie überraschende, schädigende Vorfälle vermeiden will.

Die Risikoanalyse erfolgt in Phasen. Bei der Beschreibung der einzelnen Schritte folgt diese Arbeit im wesentlichen [Brunnstein 02], [Moses] und [Stelzer]. Zunächst werden die einzelnen Phasen aufgezählt und anschließend näher besprochen.

- Ermittlung des Security Perimeters
- Werteermittlung
- Risikoerkennung
- Risikobewertung

1.3.1. Ermittlung des Security Perimeters

Zu Beginn der Analyse müssen zunächst Inhalt und Grenzen des betrachteten Systems festgelegt werden (Ermittlung des Security Perimeters). Soll in einem Unternehmen beispielsweise nur eine Filiale oder sollen alle Filialen untersucht werden? Betrachtet man ein ganzes Rechnernetz oder nur den Gatewayrechner? Zur Abgrenzung des Systems gehört auch die Ermittlung von Schnittstellen zum nicht untersuchten Bereich der Welt. Eventuell kann eine Unterteilung in Subsysteme sinnvoll und nötig sein. Es müssen sicherheitsrelevante

Objekte ermittelt werden, wie etwa Gebäude, Rechner, Daten, Personen usw., für die später die einzelnen Risiken betrachtet werden sollen. Oft müssen hierbei auch die Wechselwirkungen zwischen diesen Objekten untersucht werden, da einige Risiken nur bei Interaktion auftreten.
Die Festlegung der Systemgrenzen ist alles andere als trivial. Werden die Grenzen zu eng gefasst, können bedeutende Risiken in ausgeklammerten Systemteilen unerkannt bleiben, die sich dennoch auf das System auswirken können. Werden die Grenzen hingegen zu weit gefasst, so kann das gesamte Vorhaben Risikoanalyse zu aufwendig und teuer werden, da die einzelnen Risiken sich zu sehr unterscheiden (siehe 1.2. Risikoverteilung). Zudem könnten hierbei Ausschnitte der Welt mitbetrachtet werden, die keine Auswirkung auf das eigentliche System haben und die Analyse unnötig verkomplizieren.

1.3.2. Werteermittlung

Nach der Festlegung der Systemgrenzen müssen die Werte ermittelt werden, die innerhalb der Organisation des Schutzes bedürfen. Als Werte sind hierbei alle materiellen oder immateriellen Dinge zu verstehen, von deren, eventuell alleinigem, Besitz die Organisation abhängt oder profitiert **(**„valuable system resources" [RFC 2828] oder auch Assets genannt). Zu den materiellen Werten gehören z.B. Immobilien, Hardware, Mobiliar oder auch die Gesundheit der Mitarbeiter. Beispiele für immaterielle Werte sind Kapital, Mitarbeiterdaten, Forschungsergebnisse, allgemeine Daten und ähnliches. Besondere Beachtung haben hierbei die Werte, von denen das Unternehmen der Alleinbesitzer ist und bleiben muss, z.B. Daten aus der Produktentwicklung. Bei ihnen können nicht nur mit Zerstörung, Beschädigung oder Diebstahl verbundene Risiken bestehen, sondern es besteht auch die Gefahr der Datenspionage.
Die ermittelten Werte müssen mit den Objekten des Systems in Beziehung gesetzt werden, um die Masse der möglichen zu untersuchenden Risiken einzuschränken. So besteht in der Kantine einer Firma (Objekt) selten ein Risiko, dass der Rechner eines Abteilungsleiters (Wert) beeinträchtigt wird. Folglich braucht die Risikoanalyse in den folgenden Schritten Risiken für den Rechner des Abteilungsleiters, die *ausschließlich* mit der Kantine zusammenhängen, nicht zu untersuchen. Betrachtet man hingegen die Gesundheit der Mitarbeiter, so könnte sie sehr wohl mit der Kantine in Verbindung gebracht werden.
Ziel dieses Schrittes ist die Beantwortung der Frage „Welche Werte stehen mit welchen Objekten in Beziehung und wo könnten sich folglich Risiken für diese Werte verbergen?".

1.3.3. Risikoerkennung

Der nächste Schritt, die Risikoerkennung, gliedert sich in zwei Unterpunkte. Gemäß der Risikodefinition sind dies:

- Ermittlung von Bedrohungen
- Ermittlung von Schwachstellen

Es ist sinnvoll, in dieser Reihenfolge vorzugehen, da sich Bedrohungen wesentlich leichter als Schwachstellen zu einem allgemeinen Katalog zusammenstellen lassen. Es ist wichtig, alle Teile der Organisation in die Risikoerkennung einzubeziehen, da ja auch in jedem Teil Risiken bestehen können. Nach [Krallmann] sind insbesondere der Datenschutzbeauftragte, die Sicherheitsgruppe, die Revision sowie das Management gefordert. Allein die Geschäftsleitung ist an der Risikoerkennung nicht beteiligt, da sie für den Gesamtüberblick über die Organisation zuständig ist und in die einzelnen Prozesse selten Einblick hat. Ihr kommt jedoch eine wichtige Rolle bei der Risikobewertung zu, wenn für die Risiken das Schadenspotential ermittelt wird. Nützlich für die Risikoerkennung können auch externe Berater sein, die einen objektiveren Blick auf die Organisation haben als die Mitarbeiter.

Ermittlung von Bedrohungen

Zur Ermittlung von Bedrohungen untersucht das Analyseteam die Umgebung des Systems und das System selber auf mögliche Bedrohungen und stellt diese zusammen. Analog zu [Moses] müssen insbesondere die folgenden Bedrohungen geprüft werden:

- Natürliche Ereignisse

Hierzu zählen Brände, Wassereinbruch, Unwetter, Ausfall von Mitarbeitern wegen Krankheit, Vulkanausbrüche, Erdbeben u.ä. Da diese Bedrohungen zum Bereich der höheren Gewalt zählen, müssen sie für jedes System betrachtet werden.

- Menschliches Fehlverhalten

Zu diesem Punkt zählen alle unerwünschten, bedrohlichen Eingriffe, die Menschen unabsichtlich am System vornehmen. Dies könnte beispielsweise das Herunterstoßen einer Vase oder das Stolpern über ein Kabel sein. Auf IT Systeme bezogen müssen insbesondere mögliche Fehler von Softwareprogrammierern, Systemadministratoren, Operatoren, Anwendern und Wartungsingenieuren betrachtet werden.

- Fehlfunktionen von Ausrüstung und Software

Unter den Punkt Fehlfunktionen fallen alle zufälligen Ausfälle und Fehler. So können beispielsweise einzelne Rechner oder Rechnerteile wie CPU, Speicher oder Netzverbindung ausfallen. Gleiches gilt für Software oder auch für Einrichtungen, die nicht direkt zum IT System gehören, deren Beeinträchtigung aber für dieses von Belang wäre, wie etwa die Klimaanlage. Teilweise schwieriger als Ausfälle sind die Fälle zu handhaben, in denen die Teile nicht ausfallen, sondern fehlerhaft weiterarbeiten. Hier ist eine genaue Untersuchung der möglichen Fehler jedes Teils nötig.

- Eindringen ins System

Als Eindringen ins System (Infiltration) wird das absichtliche und unerlaubte Bearbeiten von Systemteilen bezeichnet, beispielsweise Manipulation an der Klimaanlage oder Vergiften des Essens durch Außenstehende. Im IT Bereich fallen hierunter alle Angriffe auf Rechner, Netze und Daten mit dem Ziel, Daten auszuspionieren, zu löschen, zu modifizieren oder für legale Anwender unzugänglich zu machen.

- Missbrauch von Ressourcen

Beispiele für den Missbrauch von Ressourcen sind unerlaubte private Telefongespräche oder Surfen im Internet am Arbeitsrechner. Unter diese Kategorie fallen alle absichtlichen Missbräuche von Systemressourcen, durch die diese Ressourcen für autorisierte Prozesse nicht mehr oder nur noch begrenzt zur Verfügung stehen. Auch die unerlaubte Produktion von Netzlast in einem LAN fällt unter den Missbrauch von Ressourcen.

- Diebstahl

Diebstahl ist die mutwillige Entfernung von Systemteilen oder Ausrüstung aus dem System.
Bezogen auf Daten ist Diebstahl bereits dann gegeben, wenn unerlaubter Besitz an Daten erlangt wird.

- Vandalismus

Unter Vandalismus wird die mutwillige Beschädigung oder Zerstörung von Systemteilen verstanden, worunter auch Datenträger fallen können. Im Gegensatz zur Infiltration steht beim Vandalismus die Zerstörung oder Beschädigung der Systemteile im Vordergrund, nicht die einfache Manipulation.

Der Bedrohungskatalog muss so vollständig wie möglich sein, da übersehene Bedrohungen in der weiteren Risikoanalyse und dem daraus entstehenden Notfallkonzept unbeachtet blieben. Der Bedrohungskatalog an sich ist abstrakt, er stellt nur Klassen von möglichen Bedrohungen dar. Für die spätere Wahrscheinlichkeits- und Schadensermittlung müssen die Bedrohungen konkreter ausgestaltet werden. Nach [Brunnstein 02] und [Moses] muss zunächst geklärt werden, welche Werte im Einzelnen bedroht sind. Auf diesen Überlegungen fußen später die Schadensberechnungen. Eine abstrakte Bedrohung wie beispielsweise Diebstahl kann natürlich eine Vielzahl von Werten treffen, weshalb die Bedrohungen weiter untergliedert werden müssen, etwa in der Form „Bedrohung 1: Diebstahl von Büroausstattung, Bedrohung 2: Diebstahl von Hardware...“. Wie weit untergliedert werden muss, hängt davon ab, wie stark die bedrohten Werte sich in ihrem Wesen unterscheiden.
Ebenso sollte für jede Bedrohung der Kreis der Personen ermittelt werden, von dem diese Bedrohung ausgehen könnte. Nach [Krallmann] ist zu untersuchen:

- Wer sind mögliche Täter?

In den Kreis möglicher Täter gehören alle Personen, denen das Umsetzen der Bedrohung einen Vorteil bringen würde. Zudem müssen potentielle Täter die Gelegenheit zur Tat haben. Zu beachten ist auch die Einstellung der Person gegenüber der Organisation.

- Wie könnte ein Täter vorgehen?

Diese Frage gehört systematisch eigentlich in den Bereich der Schwachstellenermittlung, es liegt jedoch nahe, die möglichen Vorgehensweisen eines Täters nicht von den restlichen Tätermerkmalen zu trennen. Wenn der mögliche Täterweg bekannt ist, lassen sich zur untersuchten Bedrohungen passende Schwachstellen leichter finden. Insbesondere kann der Weg des Täters aber auch Schwachstellen aufzeigen, die er höchstwahrscheinlich nicht ausnutzen wird.

- Welche Motive könnte ein Täter haben?

Diese Frage ist wichtig zur späteren Ermittlung der Wahrscheinlichkeitsverteilung. Nach [Krallmann] sind mögliche Motive beispielsweise Habgier, finanzielle Probleme, Rache oder der Reiz der Tat selber.

Ein weiteres wichtiges Hilfsmittel zur Bedrohungsanalyse ist nach [Krallmann] die so genannte Fehlerbaummethode. Dabei handelt es sich um ein Top-Down Analyseverfahren, mit dem große Bedrohungen in kleinere Bedrohungen aufgeteilt werden können. Dazu werden für jede Bedrohung mögliche Ursachen ihres Eintritts ermittelt. Diese Ursachen sind ihrerseits wieder Bedrohungen, die weiter zergliedert werden können.
Mit der Fehlerbaummethode werden nicht nur die Bedrohungen zergliedert, es ergibt sich auch ein Bild der kausalen Zusammenhänge im System.

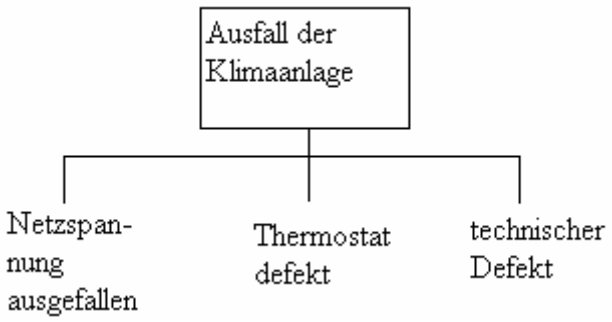


Abbildung 2: Beispiel eines Fehlerbaums aus [Krallmann]

Ermittlung von Schwachstellen

Nach der Bedrohungsanalyse erfolgt die Schwachstellenanalyse. Erste Hinweise auf mögliche Schwachstellen hat die Ermittlung des Täterwegs bereits ergeben. Aus dem

Bedrohungskatalog lassen sich oft mögliche Schwachstellen ableiten, die für diese Bedrohungen relevant sein können. Die meisten Schwachstellen zu bekannten Bedrohungen sind ebenfalls bekannt, da sie für eine Vielzahl von Systemen typisch sind (so sind beispielsweise ungesicherte Türen eine übliche Schwachstelle für Diebstahl). Natürlich muss das System dennoch nach weiteren unentdeckten oder sogar vorher unbekannten Schwachstellen abgeklopft werden. Wie bereits erwähnt, lassen sich Schwachstellen schwieriger katalogisieren als Bedrohungen, weshalb die gefundenen Schwachstellen selten alle tatsächlich vorhandenen Schwachstellen abdecken. Somit ist dieser Punkt der Analyse vermutlich der schwierigste und zugleich der wichtigste, da möglichst viele Schwachstellen gefunden werden müssen.

Im Folgenden werden nun nach [Stelzer] zwei Methoden dargestellt, wie die Risikoanalyse in konkrete Verfahren umgesetzt wird. Diese Methoden sind exemplarisch und werden selten in Reinform angewandt. Vielmehr ist ein Zusammenspiel beider Methoden in der Praxis üblich.

Die erste der beiden Methoden ist die so genannte Szenariomethode. Szenarien sind „Hypothetische Aufeinanderfolge[n] von Ereignissen, welche [...] zur Analyse kausaler Zusammenhänge konstruiert [werden]“ [Stelzer]. Da die Erstellung von Szenarien für eine Risikoanalyse sehr aufwendig sein kann, können nach der Szenariomethode oft nur einzelne besonders wichtige Fallbeispiele untersucht werden. Vor der eigentlichen Szenarioanalyse werden in der Organisation Informationen gesammelt, welche Szenarien sinnvoll und realistisch sind. Daraus werden die Szenarien in Form von Geschichten oder Grafiken ermittelt. Natürlich müssen in den Szenarien die entsprechenden Bedrohungen, Schwachstellen und verletzten Werte dargestellt werden. Das Szenario schildert dabei nicht nur das ermittelte Risiko, sondern einen hypothetischen Vorfall, bei dem sich das Risiko manifestiert. Szenarien liefern gute Hinweise auf mögliche Gegenmaßnahmen und sind daher für Notfallkonzepte von Bedeutung, zumal sie den Vorfall wirklich durchspielen.
Die Szenariomethode bietet vor allem den Vorteil, dass die Mitarbeiter ihr Wissen über Bedrohungen und Schwachstellen effektiv einbringen können. Zudem stärkt sie das Sicherheitsbewusstsein und das Wissen über interne Abläufe im System, da die Szenarien für die Mitarbeiter nachvollziehbar mögliche Abläufe darstellen, was auch ihre große Überzeugungskraft begründet. Allerdings haben Szenarioanalysen den Nachteil, dass sie nur bestimmte, eng begrenzte Bereiche des Systems untersuchen können. Eine umfassende Risikoanalyse eines großen Systems ist mit einer reinen Szenarioanalyse nicht durchführbar.

Bei der zweiten Methode handelt es sich um die Simulationsmethode. Die Simulation besteht dabei nach [Stelzer] in der Nachahmung technischer Vorgänge. Zunächst muss der Analysebereich modelliert werden. Dies ist sehr aufwendig und arbeitsintensiv, da das Modell eventuell die gesamte Organisation mit allen Prozessabläufen umfassen muss. Aufbauend auf dem Modell können dann Gefahrenquellen und ihre Auswirkungen simuliert werden. Der

Hauptunterschied zur Szenariomethode besteht darin, dass die Simulation eine umfassende Analyse im gesamten modellierten System ermöglicht, während die Szenarien nur einzelne Vorgänge in begrenzten Umgebungen untersucht. Zudem kann die Simulation eine Vielzahl bis alle möglichen Auswirkungen einer einzelnen Gefahrenquelle erfassen, wohingegen sich in einem Szenario nur einzelne ausgewählte Auswirkungen durchspielen lassen.
Die Simulationsmethode ermöglicht detailliertere Analysen als die Szenariomethode. Zudem können die Modelle des Systems, wenn sie einmal erstellt wurden, für weitere Analysen genutzt werden.

1.3.4. Risikobewertung

Wurde die Risikoerkennung durchgeführt, müssen für die Risiken die Wahrscheinlichkeiten sowie das Schadenspotential ermittelt werden. Dies geschieht im Rahmen der Risikobewertung. Aus dem Verhältnis von Wahrscheinlichkeit und Schaden ergibt sich dann die Information darüber, wie kritisch oder unkritisch ein Risiko einzustufen ist, und ob für den Fall seines Eintritts ein Notfallkonzept erstellt werden muss.

Die Wahrscheinlichkeitsabschätzung basiert vor allem auf zwei Dingen: Den Ergebnissen aus der Risikoerkennung sowie statistischen Daten über die Manifestation ähnlicher Risiken. Dabei sind die statistischen Daten in der Regel verlässlicher, da sie von tatsächlich eingetretenen Vorfällen berichten und nicht auf Hypothesen beruhen. Sie können allerdings nur herangezogen werden, wenn das untersuchte Risiko ausreichend dem Vorfall aus der Statistik gleicht. Andernfalls müssen die Analytiker sich auf ihre eigene Abschätzung aus den Ergebnissen der vorigen Schritte verlassen.

Die Ermittlung des Schadenspotentials erfolgt ähnlich wie die Bedrohungsanalyse nach der Orientierung an einem Katalog. Die Schäden werden nach [Krallmann] in zwei Hauptgruppen unterteilt:

- Primäre Schäden

Primäre Schäden entstehen unmittelbar durch die Manifestation des Risikos. Sie umfassen beispielsweise Kosten für Ersatzbeschaffung, bauliche Maßnahmen, erhöhten Arbeitsaufwand und externe Hilfe.

- Sekundäre Schäden

Sekundäre Schäden folgen zwar auch aus der Manifestation des Risikos, treten aber erst später als Folgeerscheinung auf. Sie sind schwieriger in Geld zu bemessen als primäre Schäden. Beispiele für sekundäre Schäden nach [Krallmann] sind:

- Cash-Flow Verzögerungen
- Produktionsverzögerungen wegen Rohstoff- oder Geldknappheit
- Zu geringe oder zu hohe Lagerbestände durch Einschränkung der Lagerkontrolle
- Falsche Geschäftsentscheidungen, weil Planungsinstrumente nicht mehr zu Verfügung stehen oder Informationen verfälscht sind
- Lieferverzögerungen
- Irreparabler Geschäftsverlust durch Vereitelung etwa eines Saisongeschäfts
- Verlust von Neugeschäft durch Unterbrechung oder Vernichtung der Forschung
- Verlust von Kunden

Um das Schadenspotential von Risiken vergleichbar zu machen, bietet es sich an, die möglichen Schäden in Geldsummen umzurechnen (Quantifizierung von Werten). Dies ist bei sekundären Schäden im Gegensatz zu primären Schäden nicht immer einfach. Wie bei der Wahrscheinlichkeitsermittlung sind auch hier statistische Daten hilfreich, wenn auch selten verfügbar.
Da der Schwerpunkt dieser Arbeit auf Notfallkonzepten für IT Systeme liegt, sollen hier exemplarisch einige Anhaltspunkte gegeben werden, um den Wert von Daten bzw. den durch ihren Verlust oder ihre Vernichtung entstehenden Schaden zu bestimmen. Nach [Krallmann] stellen sich folgende Fragen:

- Was muss ein Unbefugter aufwenden, um Zugriff auf nicht für ihn bestimmte Daten zu erlangen? Ein hoher Aufwand erhöht dabei den Wert der Daten. Bei wertvollen Daten sollte im Gegenzug der Aufwand sehr hoch sein, etwa durch entsprechende Schutzmaßnahmen.
- Welche Aufwendungen hätte die Konkurrenz, um die gleichen Daten legal zu erwerben? Wäre es beispielsweise ein leichtes für die Konkurrenz, einen geringen Forschungsvorsprung aufzuholen, haben die Forschungsergebnisse nur geringen Wert.
- Was wäre die Konkurrenz bereit aufzuwenden, um an die Informationen zu gelangen? Wenn die Konkurrenz kein Interesse an den Daten hat, ist ihr Wert eher gering.
- Wie hoch könnten die Folgekosten eines Schadens sein? Mit der Höhe der sekundären Schäden steigt auch der Wert der Daten.
- Ist es möglich, den Schaden ungeschehen zu machen? Hier ist beispielsweise an Datenwiederherstellung zu denken. Ist dies schwierig oder unmöglich, haben die Daten einen höheren Wert.
- Was kosten Schutzmaßnahmen? Teure Schutzmaßnahmen erhöhen zwar nicht den Wert der Daten an sich, stellen aber selbst wiederum einen Wert dar.

Ähnliche Überlegungen lassen sich auch für die Quantifizierung anderer Werte anstellen. Ihre Darstellung würde hier aber zu weit führen.

Wie zur Risikoerkennung existieren auch für die Risikobewertung mehrere Konzepte, von denen zwei hier ausgeführt werden, das kardinale und das ordinale Bewertungsprinzip. Dabei orientiert sich die Arbeit erneut an [Stelzer].

Das kardinale Bewertungsprinzip ist eine einfache mathematische Methode, die allerdings nur die primären Schäden berücksichtigt. Die primären Schäden eines Risikos werden in Geld bestimmt und mit der Schadenshäufigkeit pro Zeiteinheit multipliziert, wobei sich die Schadenshäufigkeit aus der Wahrscheinlichkeit ergibt. Das Ergebnis ist ein Geldwert, den das Risiko die Organisation pro Zeiteinheit kostet. Hat also beispielsweise ein Risiko ein primäres Schadenspotential von 5000 Euro und tritt im Mittel dreimal pro Jahr auf, so kostet das Risiko die Organisation pro Jahr 15000 Euro. Mit statistischen Methoden kann das Berechnungsmodell verfeinert werden, um die Realität angemessener abzubilden.
Der Hauptvorteil dieser Methode liegt darin, dass ein Risiko letztlich als Geldwert ausgedrückt wird und mehrere Risiken somit ökonomisch vergleichbar werden. Dies kann aber auch zu einem Nachteil führen, wenn die Schäden sich nicht ohne weiteres in Geld berechnen lassen. Dann ist das Modell schlichtweg nicht anwendbar. Gleiches gilt, wenn die Häufigkeit pro Zeiteinheit nicht oder nur ungenau ermittelt werden kann. Oft muss sich die Berechnung daher auf Vermutungen stützen, täuscht dann aber im Ergebnis eine nicht vorhandene Exaktheit vor.

Das ordinale Bewertungsprinzip setzt schon in der Risikoerkennung an und ordnet Klassen von Bedrohungen, Schwachstellen und Werten Kennwerte zu. Nach einer Berechnungsvorschrift, die in einzelnen Modellen unterschiedlich sein kann, wird dann aus den Kennwerten ermittelt, ob das Risiko tragbar oder untragbar ist. Es wird also kein konkreter Wert für den Schaden errechnet, sondern nur eine Abschätzung darüber, ob die Organisation mit dem Risiko leben kann oder Gegenmaßnahmen ergreifen muss. Das ordinale Modell täuscht also keine falsche Exaktheit vor und ist deshalb verlässlicher als das kardinale. Allerdings hat es auch eine Reihe von Nachteilen. Es ist sehr arbeitsintensiv. Zudem werden die einzelnen Bedrohungen, Schwachstellen und Werte ohne Zusammenhang bewertet, was den Gesamtüberblick erschwert.
Mit der Risikobewertung endet die Risikoanalyse. Danach kann der Hauptteil des Risikomanagements beginnen, in dem geeignete Schutz- und Gegenmaßnahmen ermittelt werden.

1.4. Risikomanagement

Risikomanagement dient der „Bestimmung möglicher Gegenmaßnahmen (eng. c*ountermeasures*) zum Zwecke der Risikominderung“ [Brunnstein 02]. Was genau eine Gegenmaßnahme ist, wird nach [RFC 2828] definiert:

Countermeasure: An action, device, procedure, or technique that reduces a threat, a vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken.

Diese Definition nennt bereits einige Klassen von Gegenmaßnahmen, die im Fortgang dieses Unterabschnitts näher dargestellt werden. Um das Ziel des Risikomanagements zu erreichen, muss zunächst die Risikoanalyse abgeschlossen sein, damit Klarheit darüber besteht, für welche Risiken Gegenmaßnahmen ermittelt werden müssen. Anschließend werden geeignete Gegenmaßnahmen anhand von Katalogen ermittelt und schließlich um- und durchgesetzt. Ob eine Gegenmaßnahme geeignet ist, richtet sich hauptsächlich nach dem Verhältnis von Kosten und Nutzen. Der im Mittel angerichtete Schaden durch ein Risiko (bzw. dessen Manifestation) muss „groß genug“ sein, damit sich die Gegenmaßnahme rechnet. Wenn die Gegenmaßnahme teurer ist als der Schaden, ist sie ungeeignet. Besondere Beachtung verdienen hierbei Immaterialschäden wie Imageverlust, denn diese können schwerlich in Geld umgerechnet werden. Zudem können die Kosten für eine Gegenmaßnahme nicht nur einmalig, sondern auch laufend auftreten, denn viele Gegenmaßnahmen erfordern eine Wartung.
Die Formen von Gegenmaßnahmen können sehr unterschiedlich sein, ebenso wie die Risiken, gegen die sie eingesetzt werden sollen. Dieser Unterabschnitt bietet zunächst einen Überblick über die verschiedenen Formen der Gegenmaßnahmen. Anschließend werden die einzelnen Phasen des Risikomanagements dargestellt und erörtert.

1.4.1. Formen von Gegenmaßnahmen

Gegenmaßnahmen können nach Typen und Aspekten klassifiziert werden. Der Typ einer Gegenmaßnahme richtet sich danach, an welcher Stelle des Risikos die Gegenmaßnahme wirkt. Der Aspekt bestimmt, an welchem Teil des Systems die Gegenmaßnahme angesetzt wird. Beide Klassifikationskriterien können kombiniert werden, so dass letztlich eine Matrix entsteht, die zur Klassifikation verwendet werden kann. Abbildung 3 zeigt einen Ausschnitt dieser Matrix und liefert einige Beispiele für konkrete Gegenmaßnahmen. Allerdings stellt Abbildung 3 nur je zwei Typen und Aspekte dar, es existieren jeweils noch einige mehr.

	Typ: Vermeidend	**Typ: Transfer**	**Typ: ...**
Aspekt: Physikalisch	z.B. Verzicht auf leichtentzündliche Baustoffe bei der Gebäudeplanung	z.B. Lagerung von Bargeld in einem Tresor anstatt wie bisher in einer Schublade des Schreibtischs	...
Aspekt: Personell	...	z.B. Einstellung eines qualifizierteren Administrators	...
Aspekt: ...	...	...	...

Abbildung 3: Typen und Aspekte von Gegenmaßnahmen

Jedes Feld dieser Matrix kann natürlich eine Vielzahl von Gegenmaßnahmen zu den unterschiedlichsten Risiken enthalten. Ähnlich wie der Bedrohungskatalog für die Ermittlung der prinzipiell möglichen Bedrohungen liefert sie einen Anhaltspunkt dafür, welche Arten von Gegenmaßnahmen allgemein zur Verfügung stehen.

Bei der Darstellung der Typen und Aspekte richtet sich diese Diplomarbeit nach [Moses], wobei die konkret genannten Gegenmaßnahmen beispielhaften Charakter haben, ohne jeglichen Anspruch auf Vollständigkeit. Es folgen zunächst die Typen:

- Vermeidung

Durch eine vermeidende Maßnahme soll das Risiko umgangen werden, indem die Arbeitsprozesse an Bedrohung und/oder Schwachstelle vorbeigeleitet werden, bzw. der bedrohte Wert aus dem System entfernt wird. So könnte das Unternehmen zum Beispiel auf die Verarbeitung sensibler Daten verzichten oder sie reduzieren. Ähnliches gilt für materielle Werte. Die Vermeidung ist von der Reduktion der Schwachstelle oder der Bedrohung abzugrenzen, da bei der Vermeidung die Bedrohung oder die Schwachstelle nicht bekämpft, sondern nur umgangen wird. Vermeidung ist im Normalfall nur in begrenztem Umfang möglich, da eine Organisation nicht auf alle Risiko behafteten Prozesse verzichten kann.

- Transfer

Beim Transfer wird der zu schützende Wert aus dem Wirkungsbereich des Risikos heraus getragen. So könnten die sensiblen Daten von einem vernetzen Computer auf einen Einzelrechner verschoben werden, um das Risiko der Netz basierten Datenspionage senken.

- Reduktion der Bedrohung

Diese Maßnahme versucht eine Ursache des Risikos zu bekämpfen, also die Bedrohung zu senken oder zu beseitigen. Beispielsweise könnte das Lagern von brennbaren Materialien im Rechenzentrum verboten werden, um die Bedrohung durch Feuer zu senken. Ein anderes Beispiel wäre eine Gehaltserhöhung für die Mitarbeiter, die mit sensiblen Daten arbeiten, um sie davon abzuhalten, Schaden zu verursachen. Dies ist eine wirksame Maßnahme, denn kaum ein Mitarbeiter wird einen gut zahlenden Arbeitgeber schädigen wollen.

- Reduktion der Schwachstelle

Eine Gegenmaßnahme kann auch an der Schwachstelle ansetzen. Beispielsweise könnten wichtige Daten verteilt gelagert werden, um die Schwachstelle, wie die Konzentration vieler wertvoller Daten auf einem einzelnen angreifbaren Rechner, auszuschalten.

- Reduktion des Schadens beim Vorfall

Dieser Typ von Gegenmaßnahmen richtet sich auf den Zeitpunkt nach der Manifestation des Risikos. Wenn sich beispielsweise das Risiko eines Feuers manifestiert, kann der Schaden durch eine Gegenmaßnahme in Form eines Feuerlöschsystems reduziert werden.

- Entdeckung

Durch die Entdeckung soll die Manifestation eines bestimmten Risikos im Vorfeld verhindert werden. Dabei wird nicht das Risiko an sich bekämpft, sondern die Prozesse im System werden laufend überwacht, um eine sich anbahnende Manifestation des Risikos zu entdecken. Zu den entdeckenden Maßnahmen gehören Errorlogs, Audit Trails, Beobachtung des Netzverkehrs und ähnliches.

- Wiederherstellung

Wiederherstellung dient der möglichst schnellen Bereinigung des Schadens nach der Manifestation eines Risikos. Das klassische Beispiel ist das Anlegen und Einspielen von Backups für wichtige Daten. Aber auch das Wiedererrichten von zerstörten Gebäuden gehört zu den wiederherstellenden Gegenmaßnahmen.

Nach der Darstellung der Typen folgen nun die Aspekte, ebenfalls analog zu [Moses]:

- Physikalisch

Physikalische Maßnahmen setzen an der festen Struktur des Systems an, also an Gebäuden, Türen, dem Belüftungssystem, den IT Systemen usw. Wichtige Beispiele sind etwa Alarmanlagen, Sicherheitsschlösser, eventuell unter Verwendung biometrischer Systeme, oder Feuermelder. Physikalische Maßnahmen richten sich hauptsächlich gegen physikalische Risiken, wie beispielsweise Naturkatastrophen oder Diebstahl im klassischen Sinne. Im

begrenzten Umfang können auch Schäden wie Datenspionage verhindert werden, sofern der Dieb die Daten am Rechner selbst zu stehlen versucht oder es auf tragbare Datenträger abgesehen hat.

- Personell

In den personellen Bereich fallen alle Gegenmaßnahmen, die bei den Mitarbeitern ansetzen. Dazu zählen unter anderem gut formulierte Arbeitsverträge, Sicherheitsvorschriften, bei deren Nichteinhaltung der Arbeitnehmer sich rechtlich verantworten muss, sicherheitsbezogene Fortbildungen und natürlich die Auswahl qualifizierter Mitarbeiter.

- Strahlung

Dieser Aspekt der Gegenmaßnahmen befasst sich mit der Vermeidung elektromagnetischer oder radioaktiver Strahlung. Diese kann einerseits gesundheitliche Folgen für die Mitarbeiter haben, andererseits können über solche Strahlungen Daten abgehört oder drahtlose Übertragungen gestört werden. Gegenmaßnahmen zielen meist auf die Verwendung strahlungshemmender Baustoffe oder auf die Überwachung der vorhandenen Strahlung ab.

- Infrastrukturell und Prozedural

Gegenmaßnahmen aus diesem Bereich betreffen die Prozesse innerhalb der Organisation und sollen diese verbessern. Hauptsächlich fällt hierunter der Erlass von Sicherheitsrichtlinien, wie etwa das Erarbeiten einer Sicherheitspolitik oder eines Codex für das Verhalten bei der Arbeit. Der Bereich umfasst aber auch die weitreichende Dokumentation aller wesentlichen Abläufe und das Errichten einer Sicherheitsinfrastruktur, wie das Bilden eines Sicherheitskomitees.

- Kommunikativ

Der kommunikative Bereich betrifft alle Formen des Datenaustauschs. Für IT Systeme sind hier etwa Verschlüsselung, Zugangskontrollen zu Netzwerken, physikalischer Schutz der Leitung usw. zu nennen.

- Dokumentenbezogen

Gegenmaßnahmen, die sich auf Dokumente beziehen, dienen dazu, die Dokumente zu verwalten. So werden im Rahmen solcher Maßnahmen Schemata erarbeitet, die Dokumente nach ihrer Sicherheitsrelevanz zu markieren und zu registrieren.

- Hardware-Software bezogen

Maßnahmen im Bereich von Hard- und Software spielen naturgemäß für IT Systeme eine wichtige Rolle. Hierunter fallen etwa Passwortschutz, Zugriffsrechteverwaltung, endgültige Löschung unbenötigter Daten, Dokumentation, insbesondere Fehlerdokumentation und ihre

Auswertung, Verschlüsselung von gespeicherten Daten, Einsatz vertrauenswürdiger Programme (soweit möglich), die Verwendung von in der Organisation selbst entstandener Software und vieles mehr.

1.4.2. Die Phasen des Risikomanagements

Das Risikomanagement ist in Phasen unterteilt, von denen die erste die bereits diskutierte Risikoanalyse bildet. Die Phasen haben folgenden Ablauf:

- Risikoanalyse
- Planung und Auswahl von Gegenmaßnahmen
- Implementierung der Gegenmaßnahmen
- Wartung und Kontrolle

Wie der letzte Punkt bereits zeigt, ist das Risikomanagement niemals wirklich abgeschlossen, da die Wartung und Kontrolle einer einmal getroffenen Gegenmaßnahme ein laufender Prozess ist.

Wie bei der Risikoanalyse stellt sich auch bei den anderen Phasen des Risikomanagements die Frage, welche Personen im Unternehmen für die einzelnen Phasen zuständig sind. Einen Überblick über den Regelfall liefert die folgende, aus [Brunnstein 02] entnommene Matrix:

	Risikoerkennungsphase	Risikobewertungsphase	Planungs- und Entscheidungsphase	Realisationsphase	Permanente Kontrolle
Datenschutzbeauftragter	ja	nein	nein	ja	ja
Sicherheitsgruppe	ja	ja	ja	ja	ja
Revision	ja	ja	nein	ja	ja
Externe Berater	teilweise	teilweise	teilweise	ja	Nein
Geschäftsleitung	nein	ja	ja	nein	Ja
Organisation	teilweise	nein	ja	ja	Nein
Andere Fachabteilungen	teilweise	nein	ja	ja	Nein

Abbildung 4: Aufteilung der Zuständigkeiten in den Phasen des Risikomanagements

Die Phasen der Matrix stimmen im Allgemeinen mit den oben genannten Phasen des Risikomanagements überein: Die Risikoerkennungsphase und die Risikobewertungsphase umschreiben die Risikoanalyse. Planungs- und Entscheidungsphase sowie Realisationsphase bilden Planung, Auswahl und Implementierung der Gegenmaßnahmen. Die permanente Kontrolle beschreibt die Wartung und Kontrolle.
Im Anschluss an die Risikoanalyse erfolgt die Planung und Auswahl von Gegenmaßnahmen. Dazu liefert die dargestellte Matrix von Typen und Aspekten (Abbildung 3) das Inventar, das prinzipiell zur Verfügung steht. Üblicherweise wird für jedes Risiko die Gegenmaßnahme ausgewählt, die in der Kostenrechnung am günstigsten ausfällt. Eventuell kann dies auch eine Kombination aus mehreren Gegenmaßnahmen sein. Es existieren zahlreiche, häufig Software gestützte Methoden, um geeignete Gegenmaßnahmen zu finden. Hier soll nur das grobe Vorgehen geschildert werden, da die einzelnen Methoden teilweise stark voneinander abweichen. Wie geeignet eine Gegenmaßnahme ist, lässt sich nach folgender Formel abschätzen:

Vermiedener Schaden = Risikoschaden – (Kosten der Gegenmaßnahme + Restrisikoschaden)

Die einzelnen Werte sind als Kosten pro Zeiteinheit zu sehen. Der Risikoschaden wurde in der Risikoanalyse ermittelt. Bei der Planung der Gegenmaßnahmen müssen nun die anderen Größen errechnet werden. Für die Ermittlung der Kosten einer Gegenmaßnahme werden alle Einzelkosten der Maßnahme aufsummiert. Diese wiederum können nach Kostenfaktoren, Kostenarten und der Phase, während der sie anfallen, aufgeschlüsselt werden.

Zur Errechnung von Einzelkosten nach Kostenarten (linke Spalte) und Phasen (obere Zeile) wird eine Tabelle verwendet, die nach [Brunnstein 02], wie folgt, aussieht:

Maßnahme	Planung	Implementierung	Betrieb	Wartung
Personalkosten				
Sachkosten				
Dienstleistungskosten				
Kapitalkosten				
Summe				

Abbildung 5: Kostenfaktoren von Gegenmaßnahmen

Die in die einzelnen Felder einzutragenden Kostenfaktoren berechnen sich nach [Krallmann] aus den Kosten für Man-Power (Arbeit), für das allgemeine Datenverarbeitungssystem (ADV-System), für Geräte und Vorrichtungen sowie für Material. Unter Man-Power fallen vor allem Kosten für Organisatoren, Programmierer, Handwerker und Wartung. Kosten beim ADV-System sind Benutzungskosten von Systemressourcen wie etwa Datentransfereinheiten oder

Terminals. Unter Geräte und Vorrichtungen fallen alle Kosten für komplexe Apparaturen wie beispielsweise Alarmanlagen. Der Einbau und die Wartung derselben allerdings sind unter Man-Power abzurechnen. Materialkosten fallen schließlich für die Beschaffung von einfachen Materialien wie Kabel, Formulare usw. an.
Mit Hilfe dieses Schemas lassen sich die Kosten einer Maßnahme relativ gut planen. Um das Restrisiko abzuschätzen, ist nun eine Risikoanalyse im Kleinen erforderlich, bei der der Systemausschnitt mit der implementierten Gegenmaßnahme erneut modelliert wird. Diese Risikoanalyse ist bedeutend einfacher als die Gesamtrisikoanalyse in der Anfangsphase, da hier jeweils nur ein Risiko untersucht werden muss und die Ergebnisse der ersten Analyse als Grundlage verwendet werden können.
Die hier dargestellten Verfahren zeigen nur das grobe Vorgehen zur Bestimmung geeigneter Gegenmaßnahmen. Eine Detailbeschreibung von zahlreichen konkreten Berechnungsmethoden ist in [Moses] zu finden.

Wurde die Gegenmaßnahme ausgewählt und implementiert, muss sie für die Dauer ihres Einsatzes kontinuierlich überprüft und gewartet werden. Diese Aufgaben fallen dem Datenschutzbeauftragten, dem Werkschutz sowie der Revision zu. Wichtig ist, alle Tätigkeiten während der Kontrolle und Wartung zu protokollieren, um sie später nachvollziehen zu können.
In regelmäßigen Abständen muss das System daraufhin überprüft werden, ob entweder Unregelmäßigkeiten auftreten oder ob es neue Bedrohungen gibt. Ersteres weist daraufhin, dass die getroffenen Gegenmaßnahmen nicht oder nicht mehr ausreichen. In diesem Fall muss die entsprechende Schwachstelle gefunden werden, was zur Ermittlung von neuen Gegenmaßnahmen bzw. zur Verbesserung der alten führt. Das Auftreten neuer Bedrohungen bedeutet, dass die Gegenmaßnahmen veraltet sind und nicht mehr ausreichend schützen. Die Konsequenzen sind letztlich dieselben wie im Falle der Unregelmäßigkeiten.

Die Revision von Gegenmaßnahmen kann nach [Krallmann] anhand von sachlogischer Programmrevision mit Hilfe von Diagrammen und Programmlisten, dem Durchspielen von Testfällen, der Stichprobenprüfung und des Einsatzes von Revisionsprogrammen erfolgen.
Nachdem die Vorgehensweise beim Risikomanagement nun dargestellt wurde, kommt die Arbeit nun zu den Notfallkonzepten, den Richtlinien für ihren Inhalt und ihrer Erstellung.

1.5. Inhalte eines Notfallkonzeptes

In diesem Abschnitt werden die Inhalte eines Notfallkonzeptes dargestellt. Diese können zwischen einzelnen Notfallkonzepten variieren, da sich mögliche Notfälle stark unterscheiden können. Es existieren jedoch Richtlinien, welche Maßnahmen in einem Notfallkonzept auf jeden Fall enthalten sein müssen. Dazu kommen Detailbeschreibungen, die auf den jeweiligen

Notfall abgestimmt sind. In diesem Abschnitt richtet sich die Arbeit hauptsächlich nach den Angaben aus [Boran], [Wilbert], [BSI] und [Nedon].

Gemäß [BSI] richten sich die Inhalte (und Ziele) eines Notfallkonzeptes nach folgender Inhaltsdefinition:

Notfall-Pläne beinhalten Handlungsanweisungen und Verhaltensregeln für bestimmte Schadensereignisse. Hierbei handelt es sich um Ereignisse, die diejenigen Teile des IT Systems gefährden, die von existentieller Bedeutung sind. Ein Notfall-Plan ist auf die möglichst schnelle Wiederherstellung der Verfügbarkeit gerichtet.

Nach [Mampu] enthält ein Notfallkonzept insbesondere Richtlinien für Backup und Wiederherstellung nach dem Notfall und allgemein der Notfallbearbeitung mit dem Ziel, die Verfügbarkeit kritischer Ressourcen zu gewährleisten, damit im Notfall und nach dem Notfall der Betrieb fortgesetzt werden kann. Um diese Ziele zu erreichen, muss das Notfallkonzept vor allem zwei Eigenschaften besitzen: Es muss sich bei Eintritt des Notfalls schnell umsetzen lassen und es muss die Verfügbarkeit der Ressourcen gewährleisten bzw. wiederherstellen. Ob noch weitere Maßnahmen erforderlich sind und um welche es sich handelt, hängt vom jeweiligen Notfall ab. Falls es sich um Manipulation oder Ausspähung von Daten handelt, sind sicherlich auch Maßnahmen zur Wahrung von Vertraulichkeit und Integrität angezeigt. Im Falle eines Brandnotfalls sind zunächst Feuerlöschmaßnahmen bzw. Brandeindämmungsmaßnahmen durchzuführen, bevor das Wiederanfahren der Prozesse beginnen kann. Ähnliche Beispiele lassen sich für eine Vielzahl anderer möglicher Notfälle finden.
Ein Notfallkonzept hat nicht die Aufgabe, den Normalzustand wiederherzustellen, sondern soll lediglich die Fortsetzbarkeit der Prozesse im System auf einem ausreichenden Sicherheitsniveau gewährleisten. Dieses Sicherheitsniveau kann geringer sein als im Normalzustand, solange es gemäß der Sicherheitspolitik noch ausreicht. Für den langfristigen Wiederaufbau sind nach Ablauf des Notfallkonzepts Pläne aufzustellen bzw. abzuwickeln, die letztlich wieder zum Normalzustand führen, aber nichts mehr mit der akuten Notfallsituation zu tun haben.

Es folgt nun die Aufstellung der wichtigsten Maßnahmen, die ein Notfallkonzept beinhalten muss. Dabei liegt der Schwerpunkt auf IT bezogenen Notfällen, obwohl der Katalog in Teilen auch für andere Notfallklassen gilt. Zusätzlich enthält die Aufstellung auch Maßnahmen, die begleitend zum Notfallkonzept ergriffen bzw. vor seinem Anlauf abgeschlossen sein müssen.

- Backups

Im Regelfall sind bei IT Notfällen die Daten von ihrer Vernichtung bedroht. Wenn sie auch nicht immer völlig zerstört werden, so wird dennoch oft ihre Zugänglichkeit eingeschränkt.

Aus diesem Grund ist es wichtig, vor Eintritt eines Notfalls regelmäßig Datensicherung in Form von Backups zu betreiben. Diese Prozedur ist zwar nicht direkt Teil des Notfallkonzeptes, aber die wichtigste Voraussetzung für die spätere Datenwiederherstellung, weshalb sie hier erwähnt wird. Nach [Boran] ist es zunächst wichtig festzulegen, in welchen Abständen Backups angelegt werden und wer dies zu tun hat. In diesem Rahmen muss ebenso geklärt werden, welche Daten gesichert werden sollen (im unglücklichsten Fall alle Daten). Das [BSI] nennt in diesem Zusammenhang den Begriff des Datensicherungsplans, der zu erstellen ist. Er umfasst unter anderem die Datensicherung nach Eintritt des Notfalls, um die unmittelbar bedrohten Daten zu retten.
Es bleibt noch die Frage zu klären, wie die Backups gelagert werden müssen, damit sie im Notfall nicht mit zerstört oder beeinträchtigt werden. [Wilbert] empfiehlt, die Backups an einem feuersicheren Ort zu lagern. Hier ist zu ergänzen, dass der Ort nicht nur feuersicher, sondern allgemein möglichst gegen Naturereignisse oder physische Zerstörung oder Einflussnahme schützen sollte. Zumindest darf ein Eingriff in das IT System, wie etwa ein Angriff, die gesicherten Daten nicht beeinflussen können. Zudem sollten Backups unvernetzt gelagert werden, und ihre Funktionalität sollte regelmäßig überprüft werden. Dies ist allein schon deshalb nötig, weil Datenträger altern und die Daten durch den Alterungsprozess Schaden nehmen können.

- Wiederherstellung (recovery)

Die (möglichst schnelle) Wiederherstellung der Daten nach einem Notfall ist eine wichtige Komponente des Notfallkonzepts. Nach [Boran] muss die Wiederherstellungsmethodik sorgfältig geplant werden, da bei ihrer Durchführung der Geschwindigkeitsaspekt zum Tragen kommt. Allerdings muss dabei gewährleistet sein, dass das Backup selber unbeschädigt und möglichst unangreifbar bleibt. Wird beispielsweise der Inhalt einer Festplatte auf einer anderen Festplatte als Backup gesichert, so darf zur Wiederherstellung nicht einfach die Backup Platte anstatt der normalen in das System eingebaut werden. Wie auch bei den Backups ist im Vorfeld zu klären, wer für das Wiederherstellen der Daten zuständig ist. Die Wiederherstellungsmethode ist eventuell durch gelegentlich stattfindende Notfallübungen zu trainieren.

- Unmittelbare Notfallbekämpfung

Die meisten Notfälle dauern eine Weile an, wenn sie nicht bekämpft werden. So erlischt ein Feuer selten von alleine, und ein Angreifer über das Netz wird seine Angriffe nicht von alleine stoppen. Die notwendigen Notfallbekämpfungsmaßnahmen lassen sich in zwei Gruppen einordnen: Eindämmungsmaßnahmen und Abstellungsmaßnahmen. Eindämmungsmaßnahmen verhindern, dass der Notfall weiteren Schaden anrichten kann, obwohl er weiterhin besteht. Beispiele hierzu sind das Schließen von Brandschutztüren bei einem Feuer oder das Trennen sauberer Rechner vom Netz beim Befall des Netzes durch

Malware. Abstellungsmaßnahmen haben zum Ziel, die Ursache des Notfalls für den Moment zu beseitigen. Hierzu zählen das Löschen des Feuers oder das Entfernen der Malware von den Rechnern. Normalerweise werden beide Gruppen kombiniert, und die Eindämmungsmaßnahmen finden vor den Abstellungsmaßnahmen statt.

- Verantwortlichkeiten im Notfall

Im Notfall muss jeder Beteiligte wissen, was er zu tun hat. Aus diesem Grund müssen für jede Tätigkeit die Verantwortlichkeiten geklärt werden. Nach [Boran] kann die Einführung einer „Befehlskette“ für den Notfall wichtig sein, bei der eine verantwortliche Person die nötigen Schritte an die anderen Beteiligten delegiert.

- Kommunikation und Infrastruktur

Ein Notfall wird normalerweise nicht von der Person entdeckt, die für seine Bekämpfung ausgebildet ist und den nötigen Überblick hat. Deshalb ist es wichtig, Kommunikationsstrukturen für den Notfall festzulegen, damit der Notfall möglichst schnell den Verantwortlichen gemeldet werden kann. [Boran] nennt dies das Konzept des „Firecalls“, also eine Art Feuermeldung. Wer auch immer den Notfall bemerkt, meldet ihn zu einer Sammelstelle für Notfälle, von der aus der Notfall an den Verantwortlichen weitergegeben wird. Dieses System ist deshalb nützlich, weil für verschiedene Notfälle unterschiedliche Verantwortliche zuständig sein können, dem normalen Benutzer aber nur die Notfallzentrale bekannt sein muss.
Ist die Hierarchie im System komplex, ist ein Alarmierungsplan [BSI] vonnöten. Dieser legt fest, in welcher Reihenfolge welche Personen im Notfall alarmiert werden müssen. Der Alarmierungsplan kann von der Notfallzentrale abgearbeitet werden.
Wurde ein Notfallkonzept aufgestellt, müssen die Mitarbeiter der Organisation darüber informiert werden [Willbert]. Jeder Beteiligte muss wissen, was er im Notfall zu tun hat und an wen er sich wenden muss. Für kleinere Vorfälle schlägt [Boran] die Einrichtung einer Security Hotline und eines Helpdesks vor, bei denen ein Benutzer des Systems Beratung in Sicherheitsfragen (Hotline) und konkrete Hilfe bei Problemen (Helpdesk) erhalten kann. Diese Strukturen können auch bei der Kommunikation des Notfallkonzeptes mitwirken.

Damit die Kommunikationsstruktur im Notfall funktionieren kann, müssen weitere Maßnahmen ergriffen werden. Oft sind gerade die Kommunikationsverbindungen selber vom Notfall betroffen. Das [BSI] schlägt deshalb vor, redundante Kommunikationsverbindungen einzurichten, die im Notfall aktiviert werden können. Wichtige Ansprechadressen und Telefonnummern müssen zudem offline zugreifbar sein [Boran], damit sie immer verfügbar sind.

- Weitere Inhalte

Nach [BSI] ist einer der wichtigsten Bestandteile des Notfallkonzeptes eine Aufstellung der Ziele, die das Konzept haben soll. Auch [Wilbert] spricht von der Notwendigkeit, eine Prioritätenliste zu erstellen. Darin ist aufgestellt, welche Prozesse am dringlichsten verfügbar sein bzw. wiederhergestellt werden müssen und in welcher Reihenfolge dies im Notfall zu realisieren ist.
Das [BSI] verordnet einen detaillierten Wiederanlaufplan. Dieser orientiert sich an der Prioritätenliste und legt fest, wie die einzelnen Wiederherstellungsmaßnahmen durchzuführen sind. Analog dazu sollte es einen Wiederbeschaffungsplan geben, der die Möglichkeiten und Durchführungsarten zur Wiederbeschaffung zerstörter Werte festlegt. Hierzu gehören beispielsweise Ersatzrechner.
Da ein Notfall normalerweise sehr kostspielig ist, rät [Wilbert] zur Abschließung von Versicherungen, die den Schaden durch den Notfall abfangen. Diese sind regelmäßig auf ausreichenden Schutz hin zu überprüfen und gegebenenfalls zu erweitern.
Mitunter reichen die Ressourcen des Systems nicht aus, um ein angemessenes Notfallkonzept durchzuführen. Manchmal tun sie dies von vorn herein nicht, oder der Notfall ist so schwerwiegend, dass das Konzept nicht mehr umgesetzt werden kann. In einem solchen Fall kann ein im Vorfeld mit einer Fremdfirma abgeschlossener Notfallhilfevertrag helfen („Emergency standby contract“, [Boran]).
Schließlich sind gelegentliche Notfallübungen von Vorteil. Diese verbessern die Kenntnis der Mitarbeiter über das Notfallkonzept und das Sicherheitsbewusstsein. Hauptsächlich dienen sie aber der Geschwindigkeitserhöhung bei der Abarbeitung des Notfallkonzeptes in einem echten Notfall.

Nachdem die Inhalte eines Notfallkonzeptes geklärt sind, wollen wir uns nun mit der Frage befassen, wie aus den Ergebnissen des Risikomanagements ein Notfallkonzept entsteht.

1.6. Erstellung eines Notfallkonzeptes

Notfallkonzepte ergeben sich nicht automatisch aus dem Risikomanagement. Denn obwohl das Risikomanagement Gegenmaßnahmen zu den Risiken erarbeitet, haben Risikomanagement und Notfallkonzept unterschiedliche Ziele. Mit dem Risikomanagement sollen Schäden vermieden, verringert oder behoben werden. Hierbei steht der Kostenfaktor im Vordergrund, da der Schaden in Geld gemessen wird. Das Notfallkonzept dient der möglichst schnellen Wiederaufnahme des Betriebes unter akzeptablen Bedingungen, aber nicht der Beseitigung bereits erlittener Schäden. Somit können (und müssen) als Ergebnis des Risikomanagements Teile und Aspekte eines Notfallkonzeptes gewonnen werden. Es müssen für seine Erstellung vor allem infrastrukturelle und organisatorische Gegebenheiten im

System erforscht und im Bedarfsfall angepasst werden, die mit dem eigentlichen Risiko nichts zu tun haben.
Zusätzlich müssen eventuell bauliche, logistische oder wirtschaftliche Maßnahmen durchgeführt werden, damit das Notfallkonzept umsetzbar ist. Dies gehört zwar nicht direkt zur Erstellung des Notfallkonzeptes „auf dem Papier“, ohne sie ist das Konzept aber nutzlos bzw. nicht anwendbar.

Um ein Notfallkonzept zu erstellen, muss zunächst ein Risikomanagement durchgeführt werden. Ohne Risikomanagement sind die möglichen Notfälle nicht einmal bekannt, geschweige denn Maßnahmen, die bei deren Eintritt durchzuführen sind. Das Risikomanagement liefert das nötige Wissen, unter welchen Umständen ein Notfall eintreten kann, welche Auswirkungen er haben könnte und wie dagegen vorgegangen werden kann. Aus diesen Informationen und den oben ausgeführten weiteren Überlegungen ergibt sich die Summe der Maßnahmen, die für die Erstellung des Notfallkonzeptes wichtig sind.
Um die einzelnen Schritte bei der Erstellung darzustellen, nutzt die Arbeit den Inhaltskatalog eines Notfallkonzeptes aus Abschnitt 1.5.. Anhand der Inhaltskategorien werden die Maßnahmen dargestellt, die gewährleisten, dass die entsprechenden Maßnahmen im Notfallkonzept vorhanden sind.

- Ermittlung der Backup Maßnahmen

Bevor ein geeignetes Backup für den Notfall angelegt werden kann, muss geklärt werden, welche Daten in einem Backup enthalten sein sollen. In kleinen Systemen können sämtliche Daten im Backup gesichert werden, in größeren ist dies jedoch aufgrund der Datenmenge nicht immer möglich.
Welche Daten den größten Wert für die Organisation haben bzw. welche Daten wegen eines hohen Schadenspotentials besonders gegen Verlust oder Spionage geschützt werden müssen, folgt aus der Werteermittlung.
Die Form des Backups muss an die Daten angepasst werden. Sind beispielsweise Festplatteninhalte komplett als Backup zu sichern, so bietet sich als Backupform das Plattenimage an, das üblicherweise auf einer CD gespeichert wird.
Außerdem muss für die Lagerung des Backups ein sicherer Ort ermittelt werden. Wo ein solcher Ort liegen könnte, folgt ebenfalls aus dem Risikomanagement.
Fazit: Die Wertebestimmung der Datenwerte und die Risikoanalyse für diese Werte bestimmen sehr direkt die zu sichernden Daten. Organisatorische Mittel sind zu ergreifen, um die Daten sichern zu können.

- Ermittlung der Recovery Maßnahmen

Zur Wiederherstellung beschädigter oder zerstörter Daten im Notfall ist eine Methode auszuarbeiten, wer welche Daten wann von welchem Backup unter welchen Bedingungen

wohin wieder einspielt. Hierzu muss geklärt werden, wer zuverlässig genug ist, um mit der Wiederherstellung betraut zu werden, wer die Rücksicherung freigibt usw. Möglicherweise kann diese Frage bereits aus der Risikoanalyse beantwortet werden. Da Geschwindigkeit gefragt ist, muss die betreffende Person nicht nur Kompetenz und Vertrauenswürdigkeit mitbringen, sondern auch Routine. Welche Daten vorrangig wiederhergestellt werden müssen, lässt sich wiederum aus der Wertebestimmung ableiten.

- Ermittlung der Maßnahmen zur unmittelbaren Notfallbekämpfung

Wie erwähnt, teilen sich die Bekämpfungsmaßnahmen in Eindämmung und Abstellung. Zur Vorbereitung der Eindämmung sind hauptsächlich bauliche und organisatorische Maßnahmen nötig. Zunächst ergibt das Risikomanagement die Informationen, ob und wie der betreffende Notfall sich überhaupt eindämmen lässt. Die ergriffenen Maßnahmen sollen die Eindämmbarkeit des Notfalls gewährleisten. Beispiele, welche Maßnahmen als Vorbereitung für Eindämmung nötig sind, sind der Einbau von Feuerschutztüren oder die Umorganisation des Unternehmensnetzes, damit Malware besser an der weiteren Ausbreitung gehindert werden kann. Ohne solche Maßnahmen kann die Eindämmung zwar geplant, aber nicht realisiert werden.
Ähnliches gilt für die Vorbereitungen zur Abstellbarkeit von Notfällen. Soll das Notfallkonzept eine Feuerlöschung vorsehen, so müssen Feuerlöscher vorhanden und verfügbar sein. Soll ein Wurm aus dem Netz entfernt werden können, so muss entsprechende Software und geschultes Personal vorhanden bzw. ein entsprechender Vertrag mit einer Fremdfirma geschlossen sein.

- Ermittlung geeigneter Verantwortlichkeiten

Die Ermittlung geeigneter Verantwortlichkeiten ist ein analytischer und organisatorischer Vorgang. Wurden im Risikomanagement die Organisations- bzw. Weisungsstrukturen mit untersucht und verbessert, so können Schwachstellen bereits bekannt oder behoben sein. Da es auch bei der Festlegung der Verantwortlichkeiten um Geschwindigkeitsoptimierung geht, stellt sich die Grundfrage, ob die Verantwortlichkeiten und die Befehlskette für den Normalfall auch für den Notfall geeignet sind.
Im Notfall sollte übermäßige Bürokratisierung innerhalb der Organisation vermieden werden. Zugleich sollten die kompetentesten Mitarbeiter für die Umsetzung der sensiblen Punkte des Notfallkonzeptes verantwortlich sein. Um eine geeignete Struktur zu finden, sind vermutlich Notfallübungen die beste Methode. Diese können gegebenenfalls wiederholt werden, um die Geschwindigkeit und den Erfolg zu verbessern.

- Ermittlung geeigneter Kommunikationsmaßnahmen und Infrastruktur

Um Notfälle möglichst schnell an die relevanten Stellen zu melden, sind die entsprechenden Infrastrukturen im Vorfeld zu schaffen. Hierzu muss ermittelt werden, wie diese aussehen

sollen. Anhaltspunkte hierzu kann wieder das Risikomanagement liefern, aber wie bei der Ermittlung der Verantwortlichkeiten können auch zur Evaluation der Kommunikationskanäle Übungen sehr wichtig sein.
Einige Kommunikationskanäle lassen sich automatisieren. So können Feuermelder, im Voraus installiert, ein Feuer sofort an die Notfallzentrale melden. Dieselbe Rolle in IT Systemen besetzen beispielsweise Intrusion Detection Systeme oder On-access-Virenscanner.
Die Festlegung der Kommunikationswege sollte nach der Festlegung der Verantwortlichkeiten erfolgen. Da Kommunikationsleitungen im Notfall oft selber Schaden nehmen, sollten im Notfall nur die Nachrichten eingeplant werden, die zur Alarmierung aller Verantwortlichen auch wirklich nötig sind, um von den schadhaften Leitungen möglichst unabhängig zu sein.

Wurden die Inhalte und die Ausgestaltung eines Notfallkonzeptes festgelegt, kann sich die Organisation noch immer nicht absolut sicher sein, dass das Konzept im realen Notfall den gewünschten Erfolg hat. Deshalb soll in den Szenarien dieser Arbeit die Evolution von Notfallkonzepten untersucht werden. Eingetretene Notfälle und die Arbeit von Incident Response Teams tragen zur Verbesserung noch unvollständiger Notfallkonzepte bei. Doch zunächst wird sich die Arbeit nun mit Incident Response an sich befassen.

2. Incident Response

Incident Response, die Bearbeitung von Vorfällen, wird von vielen Personen und Organisationen vorgenommen. Wird der Begriff der Vorfallsbearbeitung weit gefasst, so zählt nicht nur die Reaktion auf einen konkreten Vorfall dazu, sondern auch das Erarbeiten und Etablieren von Präventivmaßnahmen, das Erstellen von Konzepten zur eigentlichen Vorfallsbehandlung und -vermeidung sowie das Sammeln, Aufbereiten und Verteilen von Informationen über mögliche und tatsächliche Vorfälle.

Auf den IT Sicherheitsbereich bezogen beschreibt Incident Response alle Maßnahmen, die zur Analyse, Vermeidung und Bekämpfung von Sicherheitsvorfällen in IT Systemen ergriffen werden. Auch das Erstellen und der Einsatz von Notfallkonzepten gehören dazu. Im IT Sicherheitsbereich werden die Aufgaben der Vorfallsbearbeitung oft von so genannten Incident Response Teams übernommen. Einige dieser Teams arbeiten unabhängig, andere gehören zu bestimmten Organisationen, oftmals Firmen. Auch einige Universitäten unterhalten Incident Response Teams – sowohl für die eigentlichen Aufgaben als auch zu Ausbildungszwecken.

Kapitel 2 gibt einen Überblick über Incident Response Teams, ihre historische Entwicklung und die momentane Situation. Danach werden in Kapitel 3 die von Incident Response Teams angebotenen Dienstleistungen und die daraus resultierenden Konsequenzen dargestellt.

2.1. Incident Response Teams

Theoretisch können Incident Response Teams für jede Art von Vorfall zuständig sein, denn der Begriff des Vorfalls ist nicht auf eine bestimmte Ursache oder einen bestimmten Wirkungsbereich festgelegt. Im Rahmen dieser Arbeit soll der betrachtete Bereich jedoch auf die IT Systeme und ihre Umgebung beschränkt bleiben. Mit Incident Response Teams seien hier also jene Teams gemeint, die sich ausschließlich mit Computervorfällen befassen. Diese können allerdings jede beliebige Ursache haben. Für die Zuständigkeit eines Incident Response Teams spielt es grundsätzlich keine Rolle, ob ein Computervorfall etwa durch einen Malwareangriff, eine Flutkatastrophe, Stromausfall oder eine andere Ursache hervorgerufen wurde. Manche Incident Response Teams klammern allerdings einzelne Vorfälle aus ihrem Zuständigkeitsbereich aus.

Nach [Kossakowski 00] entstand der Begriff des Incident Response Teams aus dem historischen Computernotfallteam. Zahlreiche Organisationen unterhalten Notfallteams, die beim Eintritt eines Notfalls Maßnahmen ergreifen oder den Verantwortlichen beratend zur Seite stehen. Die Mehrzahl der tatsächlich von den Notfallteams bearbeiteten Vorfälle hat jedoch kein katastrophales Ausmaß. Deshalb und weil das Computer Emergency Response Team Coordination Center® (CERT®/CC) einen markenrechtlichen Schutz für Computer Emergency Response Team® (engl. für Computernotfallteam) hat eintragen lassen entstand

aus dem Begriff des Computernotfallteams mit der Zeit das Incident Response Team. Der moderatere Begriff des Vorfalls (Incident) ersetzte den Begriff des Notfalls im Namen der Teams. Die Aufgabe blieb jedoch dieselbe: Die Bearbeitung von Vorfällen und Notfällen im IT Bereich.
Zahlreiche weitere Namen und Abkürzungen für Incident Response Teams werden heute parallel verwendet. Die wichtigsten sind Computernotfallteam („computer emergency response team“), abgekürzt mit CERT®, incident handling team (IHT) und computer security incident response team (CSIRT). In dieser Arbeit soll der Begriff Incident Response Team verwendet werden, der mit IRT abgekürzt wird.
Nach [Kossakowski 00] wurden die Aufgaben eines IRT in einer Arbeitsgruppe der Internet engineering task force (IETF) in den „Guidelines and Recommendations for Incident Processing” wie folgt festgelegt:

A Security Incident Response Team should be capable off dealing with incidents that occur within its defined constituency. It should provide a means for reporting suspected incidents and offer technical assistance to help sites handle these incidents. Teams should also disseminate important incident-related information to relevant parties.

Der Zuständigkeitsbereich eines IRTs hängt also von seiner Klientel (constituency) ab. Wer zu dieser Klientel gehört, muss jedes IRT für sich selber definieren. Im Falle von firmeninternen IRTs gehört in der Regel nur die eigene Firma zur Klientel, während unabhängige IRTs in der Regel ihre Dienste (zumindest teilweise) für beliebige Kunden anbieten. Außerdem muss nicht jedes IRT zwangsläufig jede Art von Vorfall behandeln oder jede Art von Dienstleistung zu seiner Bekämpfung anbieten (vgl. Kapitel 3 für die möglichen Dienstleistungen). Die meisten IRTs beschäftigen sich beispielsweise nicht mit Vorfällen, die durch natürliche Einflüsse wie etwa Feuer eingetreten sind. Stattdessen beschränken sie sich auf Vorfälle, deren Ursache mit dem IT System verflochten ist, wie etwa Benutzungsfehler, rechner- oder netzbasierte Angriffe oder Missbrauch der Rechneranlagen.
Ebenso wie die Klientel muss auch der Umfang der bearbeiteten Vorfälle sowie die Art der angebotenen Bearbeitung vom IRT definiert werden. Ein universelles IRT, das für jedermann und jeden beliebigen Computervorfall jede mögliche Art der Behandlung anbietet, gibt es nicht. Dafür wäre der personelle und finanzielle Aufwand viel zu hoch. Stattdessen spezialisieren sich IRTs auf bestimmte Gebiete.

2.2. Historie von Incident Response Teams

Bei der Schilderung der Historie der IRT hält sich die Arbeit hauptsächlich an Angaben aus [Kossakowski 00]. Ebenso herangezogen wurden [Menne], [CERT/CC] sowie [FIRST].
In der Frühzeit des Internet gab es kaum nennenswerte Angriffe, obwohl zahlreiche der heute relevanten Sicherheitsprobleme bereits damals bekannt waren. [Kossakowski 00] nennt

Passworte, offene Adressen und den Anreiz am Einbruch in Systeme. Diese Probleme waren bereits 1973 bekannt. Dennoch war das damals aus 31 Rechnern bestehende ARPA Netz eine Zone gegenseitigen Vertrauens. Sicherheitsmechanismen gab es nicht, und ihre Erarbeitung und Implementation wurde auch nicht für notwendig gehalten.
Mit der Zeit stieg die Anzahl der Rechner im ARPA Netz. Zudem schlossen sich Teilnetze dem weltweiten Netz an, wodurch das Internet seinen Namen und die heutige Architektur als Zusammenschluss organisatorisch unabhängiger Teilnetze erhielt. Anfang 1987 gab der drastische Zuwachs von Rechnern Anlass, organisatorische Ansätze zur Bekämpfung von Angriffen zu erarbeiten. Die ersten Ansätze zur Bildung von IRTs gab es bei staatlichen Einrichtungen, wie etwa beim amerikanischen Department of Energy (US DoE). Ursprünglich sollte ein einzelnes Team für alle Einrichtungen zuständig sein, dieser Gedanke wurde aber wieder verworfen, um Interessenskonflikten vorzubeugen. Das IRT des US DoE mit dem Namen „Computer Incident Advisory Capability“ (CIAC) wurde tatsächlich erst 1989 gegründet, ein Jahr später als das erste CERT®.
Im November 1988 startete Robert T. Morris Jr., ein Student der Cornell University, den so genannten Internetwurm. Dabei handelte es sich um ein selbstreplizierendes Programm, das sich im damaligen Internet rasant ausbreitete und nach [Kossakowski 00] die gesamte Internetkommunikation für drei Tage zum Erliegen brachte. Bei der Vorfallsbearbeitung wurde deutlich, dass der Ausfall des wichtigsten Kommunikationsmediums das Hauptproblem war. Die Kompetenzzentren waren nicht mehr erreichbar und konnten ihre Lösungen deshalb nicht weitergeben.
Nach dem Vorfall wurde deutlich, dass eine Einrichtung geschaffen werden musste, die als „Feuerwehr für das Internet“ [Menne] dienen konnte. Am Software Engineering Institute der Carnegie Mellon University in Pittsburgh wurde das CERT® Coordination Center (CERT®/CC) gegründet. Nach [Kossakowski 00] beschreibt das CERT®/CC seine Aufgaben, wie folgt, in einer Charter:

The CERT Charter is to work with the Internet community to facilitate its response to computer security events involving Internet hosts, to take proactive steps to raise the community’s awareness of computer security issues, and to conduct research targeted at improving the security of existing systems.

Im Laufe der Zeit entstanden weitere IRTs, denn der Vorfall mit dem Internetwurm hatte deutlich gemacht, dass alle am Internet beteiligten Parteien durch Sicherheitsprobleme bedroht waren und sind. Im Jahr 1990 wurde schließlich das CERT-System gegründet. Es war ein Zusammenschluss von elf IRTs, davon zehn aus den USA und eines aus Europa. Da der Name CERT-System aber laut [Kossakowski] eine zu starke Bindung an das CERT®/CC suggerierte, wurde die Organisation zwei Jahre später in „Forum of Incident Response and Security Teams“ (FIRST) umbenannt. Noch heute ist FIRST der einzige weltweite Dachverband von IRTs.

Die Anzahl an IRTs wuchs weltweit weiter, zunächst hauptsächlich in den USA, später auch in Europa und anderen Kontinenten. Nicht alle neuen IRTs waren nach dem Beispiel des CERT®/CC aufgebaut und boten ihre Dienstleistungen der gesamten Internetgemeinde an. [Kossakowski 00] nennt folgende Kategorien von IRTs, die alle in FIRST vertreten sind:

- Traditionelle CERT®s nach dem Vorbild von CERT®/CC und CIAC, die für eine breite Klientel zuständig sind. Zu diesen IRTs zählt auch das am Fachbereich Informatik der Universität Hamburg gegründete CERT® des Deutschen Forschungsnetzes.
- Hersteller von Produkten unterhalten IRTs, deren Arbeitsbereich sich auf die Kunden ihrer Unternehmen sowie auf Vorfälle beschränkt, die mit diesen Produkten zu tun haben.
- Kleinere Sicherheitsteams, die in einem abgesteckten Bereich für die Sicherheit zuständig sind.
- Beratungsunternehmen und Dienstleister, die Beratung und teilweise auch andere Dienstleistungen eines IRT gegen Bezahlung anbieten.

Nach [Menne] regeln heutzutage häufig innerbetriebliche CERT®s die Aufgabe der Umsetzung von Notfallplänen. Sie reagieren bei Computervorfällen innerhalb ihrer Firma, teilweise erarbeiten sie auch Sicherheitspolitiken und wirken an deren Umsetzung mit. Firmeneigene IRTs existieren neben den traditionellen IRTs und nehmen häufig ähnliche Aufgaben war. Dabei entsteht ein Konkurrenzdruck, denn laut [Kossakowski 00] werden in den traditionellen IRTs die Interessen der Unternehmen nur rudimentär vertreten. Stattdessen werden allgemeine Sicherheitsprobleme kommuniziert und bearbeitet, die die gesamte Internetgemeinde interessieren. Im Gegenzug hat ein Unternehmen in der Regel kein Interesse daran, Details über seine Infrastruktur und Daten bei einem Vorfall an eine unabhängige Instanz weiterzugeben. Da die meisten relevanten Sicherheitsvorfälle sich in Unternehmen ereignen, führte dies zu der Situation, dass die meisten tatsächlichen Vorfälle heute in firmeneigenen IRTs bearbeitet werden, während die öffentlichen IRTs Informationen über drohende Vorfälle sammeln und verteilen und allgemeine Hinweise zur Vorfallsbehandlung zur Verfügung stellen. Tatsächliche Bearbeitung eines konkreten Vorfalls findet hier allerdings nur noch selten statt.

2.3. Existierende Incident Response Teams

Wie bereits in Abschnitt 2.2. angedeutet, gibt es heute verschiedene Typen von IRTs. Zum einen existieren die traditionellen IRTs im Stil des CERT®/CC, die oftmals von staatlicher Seite aus gegründet wurden und ihre Dienste einer breiten Öffentlichkeit anbieten, wenn auch stattliche Organisationen bevorzugt bedient werden. Die Dienstleistungen dieser klassischen

IRTs variieren sehr stark. Die meisten leisten hauptsächlich Aufklärungsarbeit, indem sie Informationen über Sicherheitslücken, Bedrohungen und Vorfälle sammeln, auswerten und verteilen. Dabei erhalten die IRTs selber die Informationen hauptsächlich von Firmen (hauptsächlich Hersteller von Anti-Malware Produkten oder anderer Sicherheitssoftware), von anderen IRTs oder auch aus anderen Quellen. Mit Sicherheitsfirmen herrscht zudem ein reger Informationsaustausch. Eigene Analysen werden vergleichsweise selten durchgeführt. Bei konkreten Vorfällen geben die traditionellen IRTs auf Anfrage Hilfestellung, in der Regel per eMail. Dabei wird der Vorfall oft nicht näher analysiert, sondern nur anhand der geschilderten Symptome in eine Vorfallsklasse eingeordnet (etwa den Befall des Systems mit der bekannten Malware XYZ). Danach werden die üblicherweise wirksamen Gegenmaßnahmen empfohlen (z.B. Installation des Reinigungstools ABC, das die Malware XYZ vom System wirksam entfernen kann). Die Analyse des Vorfalls wird dabei oft dem Betroffenen selbst überlassen. Er muss die eingetretenen Änderungen am System selbst feststellen, aufgrund derer das IRT dann Maßnahmen vorschlägt. Eventuell kann das IRT aber auch hierbei Ratschläge geben, etwa einen Malwarescanner vorschlagen oder Stellen im System benennen, an deren sich üblicherweise Änderungen zeigen.

Um einer breiten Klientel umfangreichere Hilfe bei konkreten Vorfällen anzubieten, wie etwa eine detaillierte Vorfallsanalyse, fehlen den klassischen IRTs oftmals die Ressourcen. Zudem bietet die heutige Zeit eine derart breite Auswahl an möglichen Vorfällen, dass das Angebot einer umfangreichen Vorfallsbearbeitung für jedermann beinahe unmöglich zu realisieren ist.

Während die klassischen IRTs hauptsächlich die Aufgabe der Aufklärung übernehmen, haben besonders Unternehmen und Behörden oftmals einen Bedarf an konkreterer Hilfe, wenn ein Vorfall oder Notfall eingetreten ist. Deshalb haben viele Organisationen ihre eigenen IRTs gegründet. Im Bereich der Unternehmen werden sie gelegentlich als Corporate CERT bezeichnet. Diese IRTs haben zum einen die Aufgabe, das Sicherheitsbewusstsein innerhalb ihrer Organisation zu stärken. Oft helfen sie auch bei der Erstellung einer Sicherheitspolitik und ihrer Umsetzung mit. Auch beim Risikomanagement innerhalb der Organisation können sie mitwirken. Zusätzlich haben organisationsinterne IRTs die Aufgabe, auf konkrete Vorfälle zu reagieren. Da der Zuständigkeitsbereich des IRTs auf die eigene Organisation und ihre IT Systeme beschränkt bleibt, ist das Feld der möglichen Vorfälle kleiner, was eine detaillierte Vorfallsbearbeitung möglich macht. Das organisationsinterne IRT erarbeitet in der Regel eine Reihe von Präventivmaßnahmen gegen bestimmte Vorfälle. Falls der Vorfall dennoch eintritt, hilft das IRT bei der Umsetzung des Notfallkonzepts, analysiert den Vorfall detailliert und entwickelt weitere Gegenmaßnahmen.

Anders als die klassischen IRTs betreiben die organisationsbezogenen IRTs nur selten breite Aufklärungsarbeit. Zwar sammeln auch sie Informationen über Bedrohungen, Schwachstellen und Vorfälle, doch werden diese Informationen nur innerhalb der Organisation verwendet. Dabei verwenden organisationsbezogene IRTs oftmals die Informationen, die von den klassischen IRTs zur Verfügung gestellt werden. Eine weitere wichtige Aufgabe

organisationsbezogener IRTs besteht darin, mögliche Vorfälle auf ihr Schadenspotential für die Organisation zu untersuchen.
Eine dritte Gruppe bilden jene IRTs, die sich hauptsächlich mit der Forschung befassen. Diese IRTs werden von Forschungseinrichtungen wie Universitäten unterhalten. Ihre Hauptaufgabe besteht in der Analyse, mit dem Ziel, bekannte Vorfälle besser zu verstehen und auf unbekannte Vorfälle besser vorbereitet zu sein. Dazu werden in einem Labor Vorfälle nachgestellt oder simuliert, analysiert und ausgewertet. Neben den Erkenntnissen über die Vorfälle selber ergeben sich dabei auch Ansätze für bessere Incident Response Verfahren (etwa Schemata für eine umfassende Systemanalyse). Außerdem werden von diesen IRTs Tools zur Vorfallsanalyse oder –Bearbeitung entwickelt.
Die forschenden IRTs befassen sich nur sehr selten mit konkreten Vorfällen, obwohl ein konkreter Vorfall Anlass für eine Untersuchungsreihe sein kann. Da es bei der Bearbeitung von konkreten Vorfällen aber in der Regel auf Geschwindigkeit ankommt, können ForschungsIRTs hier nur selten helfen, da ihre Labore für schnelle Hilfe nicht ausgestattet sind.
Dieser Abschnitt hat gezeigt, dass es eine gewisse Arbeitsteilung zwischen den einzelnen Gruppen von IRTs gibt, und dass kaum ein IRT den gesamten Katalog an Dienstleistungen für eine breite Klientel anbietet. Um dies tun zu können, ist der IT Bereich mittlerweile zu komplex geworden, und zu viele innere und äußere Einflüsse wirken auf ihn ein. Für eine ausreichend schnelle und dennoch umfassende Behandlung von beliebigen Vorfällen in beliebigen IT Systemen wäre ein immenser Aufwand an Kosten und Personal nötig, den heute niemand aufzubringen bereit oder imstande ist. Dies gilt vor allem dann, wenn ein solches IRT mehrere Vorfälle parallel bearbeiten können soll.
Aus diesen Überlegungen folgt der Schluss, dass ein IRT sich entweder in seinem Leistungsangebot oder seiner Klientel einschränken muss, damit es effektiv und effizient arbeiten kann.

2.4. Incident Response am Fachbereich Informatik

Diese Arbeit entstand im Rahmen des IRTs am Fachbereich Informatik der Universität Hamburg. Deshalb soll hier ein kurzer Überblick über die Incident Response Arbeit am Fachbereich Informatik gegeben werden.
Im Jahr 1993 entstand an der Universität Hamburg im Fachbereich Informatik das CERT des Deutschen Forschungsnetzes, das DFN CERT, unter Mitwirkung von Klaus Brunnstein, Hans Joachim Mück und Klaus Peter Kossakowski [DFN CERT], [Kossakowski 03]. Ausgelegt war es als Forschungsprojekt, das über Drittmittel finanziert wurde. Die Ziele, die das DFN CERT verfolgte, entsprechen denen, die sich auch andere klassische IRTs wie das CERT®/CC gesetzt hatten. Eine Abgrenzung der Aufgaben des DFN CERT von denen anderer IRTs, entnommen aus [Kossakowski 03]:

„Während das DFN CERT als unabhängige Stelle Vorfälle zwischen unterschiedlichen Organisationen und Unternehmen koordinieren sowie Unterstützung bei der Bewältigung dieser Vorfälle leisten kann, müssen innerhalb geschlossener Benutzergruppen wie Organisationen und Unternehmen die einzelnen Aufgaben von den Verantwortlichen "vor Ort" wahrgenommen werden. Dies zeigt Stärken unabhängiger Notfallteams - und die Schwächen, die durch eine Anpassung des Konzepts beseitigt werden müssen.“

In [DFN CERT] werden als Aufgaben des DFN CERT das Versenden von Warnungen über Mailinglisten, das Veranstalten von Seminaren und Workshops, sowie das Sammeln und Bereitstellen von themenrelevanten Dokumenten und der Unterhalt eines Archivs mit Schutzprogrammen angegeben. Dieser Aufgabenkatalog entspricht im Allgemeinen den Tätigkeiten, die die meisten öffentlichen IRTs wahrnehmen. Zusätzlich bietet das DFN CERT Hilfe bei konkreten Vorfällen an, sofern diese im Umfeld einer deutschen Hochschule oder Universität stattfinden.
Anfang 1997 wurde das DFN CERT nach [Mück, RRZ] mit dem Projekt DFN PCA zusammengeschlossen. Dieses im Januar 1996 gegründete Projekt widmete sich dem Aufbau einer Public-Key Infrastruktur für die Mitglieder des Deutschen Forschungsnetzes. Das Ziel lag nach [Mück, RRZ] darin, eine authentisierte elektronische Kommunikation der DFN Mitglieder zu ermöglichen. Durch den Zusammenschluss der Projekte konnten nun neben den oben genannten Dienstleistungen auch Unterstützung bei kryptographischen Anwendungen, sowie der Aufbau einer Zertifizierungshierarchie für die authentische Kommunikation angeboten werden.
Anfang 1999 wurde das DFN CERT in eine gemeinnützige GmbH, das Zentrum für sichere Netzdienste, umgewandelt. Damit war eine Ausgliederung des DFN CERT aus dem universitären Kontext verbunden.
Um die Incident Response Arbeit am Fachbereich Informatik wieder präsent zu machen, wurde im Jahr 2002 das Incident Response Team des Fachbereichs Informatik unter Leitung von Klaus Brunnstein gegründet. Das neue IRT definierte seine Aufgaben anders als es das DFN CERT getan hatte. Während das DFN CERT hauptsächlich die Arbeit eines klassischen IRT machte, verstand sich das neue Incident Response Team eher als Forschungsprojekt. Folgendes Diagramm aus [IRT] illustriert die Zielsetzung:

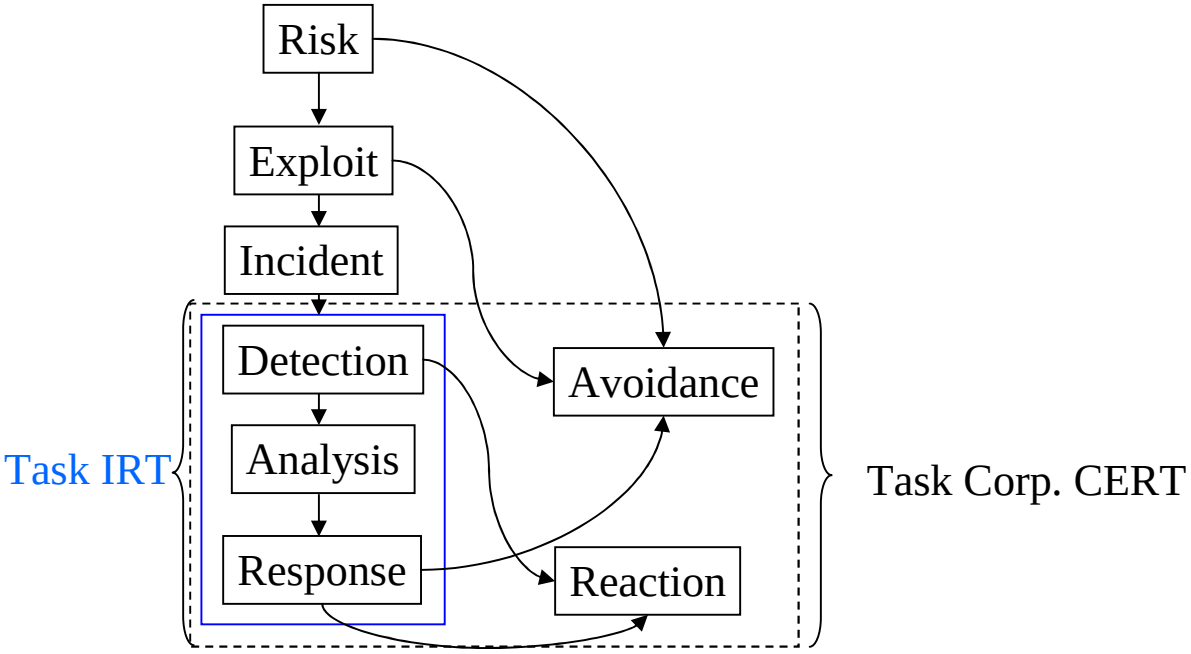


Abbildung 6: Zielsetzung des IRT am Fachbereich Informatik

Nach diesem Diagramm arbeitet das IRT der Universität Hamburg ausschließlich in den Aufgabenfeldern der Vorfallsentdeckung (Detection), Vorfallsanalyse (Analysis) und der Erarbeitung von Gegenmaßnahmen (Response). Die tatsächliche Umsetzung der Gegenmaßnahmen (Reaction) sowie das Erarbeiten und Umsetzen von Präventivmaßnahmen (Avoidance) gehört hingegen nicht zum Aufgabenbereich, sondern wird der Zuständigkeit von organisationszugehörigen IRTs zugeschrieben.

Dass die Gegenmaßnahmen zu konkreten Vorfällen nur ermittelt und nicht umgesetzt werden, deutet den Forschungscharakter dieses IRTs an. Tatsächlich werden in einem Labor des Fachbereichs Vorfälle nachgestellt. Im Rahmen dieser Versuche wird dann zunächst die Vorfallsentdeckung betrachtet. Dabei ist zu beachten, dass die Entdeckung von konkreten Vorfällen im Regelfall nicht Aufgabe eines IRT ist. Im Rahmen von Laborversuchen bietet es sich jedoch an zu untersuchen, wie der nachgestellte Vorfall entdeckt werden könnte.

Anschließend wird im Labor untersucht, welche Auswirkungen der Vorfall auf die Testsysteme hatte. Hierzu werden innerhalb des IRTs auch Analysetools entwickelt, wie etwa das in [Menne] beschriebene Tool „CompareSys“. Als letzter Schritt werden Gegenmaßnahmen gegen die Folgen des Vorfalls erarbeitet.

Bislang behandelt das IRT noch keine konkreten Vorfälle, sondern beschränkt sich zur Grundlagenforschung auf Laborarbeit. Da die Laborversuche jedoch konkreten Vorfällen nachempfunden sind, ist eine Ausweitung des Tätigkeitsfeldes angedacht worden.

3. Ergebnisse der Arbeit von Incident Response Teams

Incident Response Teams bieten eine Vielzahl von Dienstleistungen an. Dieses Kapitel gibt einen Überblick über diese Dienstleitungen und über die Reihenfolge, in der sie normalerweise erbracht werden. Außerdem werden die weiterreichenden Konsequenzen dieser Arbeit dargestellt, die nicht mehr zum Aufgabenbereich des IRTs selber gehören. Die beschriebenen Dienstleistungen umfassen Reinigung, Vermeidung und Gegenmaßnahmen. Danach folgen die langfristigen Konsequenzen: technische Fortschritte, rechtliche Schritte und Reaktionen der Angreifer. Zunächst wird allerdings die dem ganzen vorgeschaltete Vorfallsanalyse dargestellt. Eine grobe Darstellung des zeitlichen Verlaufs bei der Bearbeitung eines Vorfalls bietet Abbildung 7:

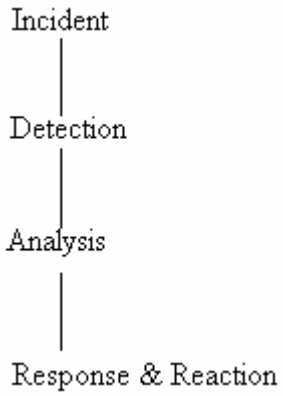


Abbildung 7: zeitlicher Verlauf bei der Bearbeitung eines Vorfalls

Da es in diesem Kapitel um die Arbeit von IRT geht, werden die Vorfälle hier auf IT Vorfälle beschränkt. Auf einen Vorfall (Incident) folgt zunächst die Vorfallserkennung (Detection). In dieser Phase wird registriert, dass es überhaupt einen Vorfall gegeben hat. Dabei sind noch keinerlei Einzelheiten über den Vorfall bekannt. Der Betroffene teilt nur mit, dass „irgend etwas passiert ist“. Die Vorfallserkennung ist in der Regel keine Dienstleistung eines Incident Response Teams, sondern wird vom Betroffenen selbst vorgenommen. Dabei kann er sich von spezieller Software unterstützen lassen, beispielsweise von Intrusion Detection Systemen.

Nach der Erkennung beginnt die Arbeit des IRTs mit der Vorfallsanalyse (incident analysis), bei der die Einzelheiten des Vorfalls abgeklärt werden. Wurde der Vorfall untersucht, erfolgen die Bearbeitungsmaßnahmen (Response & Reaction) des Incident Response Teams. Hierunter fallen die restlichen Dienstleistungen der IRT, die nicht mehr zur Vorfallsanalyse gehören, also Reinigung, Vermeidung und Gegenmaßnahmen. Je nach Zielsetzung des IRTs werden die notwendigen Maßnahmen vom IRT entweder nur erarbeitet (Response) oder auch umgesetzt (Reaction). Zusätzlich erarbeiten einige IRT noch Präventivmaßnahmen, die nicht

direkt zu den Gegenmaßnahmen für einen konkreten Vorfall gehören, sondern Vorfälle von vorn herein verhindern sollen.
In den folgenden Unterabschnitten werden nun die einzelnen Dienstleistungen von IRT vorgestellt. Der Rahmen des Beschriebenen ist dabei bewusst sehr weit gefasst, um auch das Umfeld von IRT sowie die Auswirkungen der Dienstleistungen mitbetrachten zu können.

3.1. Vorfallsanalyse (incident analysis)

Nach dem Auftreten eines Vorfalls muss das IRT diesen analysieren. Diese Analyse dient dem Zweck, mehr über den Vorfall zu erfahren und nach Möglichkeit auch Wege der Schadensbeseitigung aufzuzeigen. Nach einem Vorfall stellen sich eine ganze Reihe von Fragen, wie etwa die folgenden:

- Um welche Klasse von Vorfall handelt es sich (Angriff, Benutzerfehler...)?
- Wer hat den Vorfall ausgelöst?
- Im Falle eines Angriffs, ist er abgeschlossen, oder dauert er noch an?
- Wurden Daten verändert, gelöscht oder mitgelesen?
- Ist der Vorfall lokal beschränkt oder nicht?
- Sind ähnliche Vorfälle bekannt und wie wurden diese bekämpft?
- ...

Diese Auswahl von Fragen ließe sich fast beliebig lange fortsetzen, denn die Beantwortung von einer Frage wirft oft gleich die nächsten Fragen auf. Zudem ist die Beantwortung einzelner Fragen oft sehr schwierig, vor allem zu Beginn der Analyse. Das IRT bekommt meist nur das vorfallbehaftete System und eventuell einige Aufzeichnungen von Monitoren über den Vorfallsablauf zu sehen und hat zunächst nur wenige Anhaltspunkte darüber, was genau passiert ist.
Aus diesem Grund greifen viele existierende IRT heute nur noch auf die Angaben der Anti-Malware Industrie zurück und nehmen statt einer ausführlichen Analyse nur noch eine Vorfallsklassifikation bzw. Identifikation vor. Die Anti-Malware Hersteller untersuchen neue bösartige Software auf ihre Eigenschaften, vor allem ihre Verbreitung und ihre Schadfunktionen
Das IT System wird durch ein IRT nur auf die Präsenz von bestimmter Malware untersucht. Anschließend wird nach Schäden am System und den Daten gesucht, und danach erfolgt die Entwicklung von Gegenmaßnahmen. Ähnlich ist die Vorgehensweise bei „Standardvorfällen“, wie etwa typischen Benutzerfehlern.

Bei einer Reihe von Vorfällen ist eine ausführliche Analyse aber unumgänglich. Vor allem auf bislang unbekannte Vorfälle trifft dies zu, wenn beispielsweise eine neue Malware

aufgetreten ist, oder eine neue Schwachstelle in einem Betriebssystem bekannt geworden ist, wodurch neue Vorfälle zu erwarten sind
Die Analyse erfolgt häufig intuitiv. Ein Untersuchungsergebnis liefert Hinweise darauf, welcher Teil des Systems oder der Daten als nächstes untersucht werden sollte.
Einige Konzepte sind dennoch bekannt. Allerdings bleiben sie zu allgemein, um auf eine Vielzahl von Vorfällen anwendbar zu sein. Hauptsächlich werden zwei Arten der Analyse unterschieden:

- Statische Analyse
- Dynamische Analyse

Die statische Analyse untersucht den Systemzustand nach dem Vorfall. Das betroffene System wird oftmals abgeschaltet und führt dann während der Analyse keine eigenen Prozesse mehr durch. Mit Hilfe von Sondierungstools wird der Systemzustand abgefragt. Aus den gewonnenen Daten können Rückschlüsse auf den Vorfall gezogen werden. Eine Sonderform der statischen Analyse ist die statisch-komparative Analyse, bei der der Systemzustand nach dem Vorfall mit dem Systemzustand vor dem Vorfall verglichen wird. Hieraus ergeben sich direkte Informationen, wie der Vorfall auf das System eingewirkt hat.
Der Vorteil der statischen Analyse besteht in der relativ einfachen Durchführbarkeit. Allerdings wird die Untersuchung auf einen bestimmten Zeitpunkt im Betrieb des Systems beschränkt. Daten über den zeitlichen Verlauf des Vorfalls gehen dabei verloren. Bei länger andauernden Angriffen kann die statische Analyse zudem nur einen Teil des Angriffs erfassen. Wenn zum Beispiel eine Malware Systemressourcen wie Prozessorleistung verbraucht, erfasst die statische Analyse diese Eigenschaft nicht, außer sie wird im Code der Malware entdeckt.

Die dynamische Analyse erfolgt hingegen während des laufenden Vorfalls. Dabei kann ein realer Vorfall zwar analysiert werden, dies ist jedoch in der Praxis fast immer unmöglich, da das vorrangige Interesse darin besteht, den Vorfall zu beenden und nicht zu Analysezwecken gewähren zu lassen. Oft wird die dynamische Analyse im Rahmen eines Laborversuchs durchgeführt. Hierzu bedient sich das IRT eines Testnetzes, in dem der Vorfall simuliert wird. Dabei können Daten über den zeitlichen Verlauf des Vorfalls gewonnen werden. Das Hauptproblem bei der dynamischen Analyse im Labor besteht darin, den realen Vorfall exakt nachzubilden. Das Testnetz muss dem real betroffenen Netz oder Netzabschnitt möglichst ähneln. Zudem muss der „richtige“ Vorfall simuliert werden. Im Falle bislang unbekannter Malware etwa muss diese Malware zunächst korrekt identifiziert werden und schließlich auch zum Testen zur Verfügung stehen.
Es folgen nun beispielhaft zwei Formen der Vorfallsanalyse nach [Kossakowski 00].

- Schwachstellenanalyse

Mit dem Begriff Schwachstellenanalyse ist hier die Analyse neuer oder neu bekannt gewordener Schwachstellen gemeint. Anders als in der Risikoanalyse werden nicht die Schwachstellen eines bestimmten Systems analysiert, sondern Schwachstellen, die eine Vielzahl von ähnlichen Systemen in unterschiedlichen Umgebungen haben.
Neben der eigentlichen Analyse hat das IRT die Aufgabe, Informationen über neue Schwachstellen zu verifizieren. Insbesondere muss die Korrektheit von Gerüchten überprüft werden. Liegt tatsächlich eine Schwachstelle vor, so müssen in Tests die technischen Details geklärt und dargestellt werden. Ebenso müssen mögliche Korrekturen untersucht werden.
Es stellt sich die Frage, ob die Ergebnisse der Schwachstellenanalyse der Öffentlichkeit zugänglich gemacht werden sollten oder nicht. Einerseits kann ein hoher Bekanntheitsgrad einer Schwachstelle ihre Schließung in den meisten Systemen vorantreiben. Andererseits bieten sie auch möglichen Angreifern detaillierte Informationen darüber, wie die Schwachstelle ausgenutzt werden kann.
Die Schwachstellanalyse kann entweder im Rahmen der Analyse eines Vorfalls oder davon losgelöst erfolgen. Im zweiten Fall hat sie dann eine präventive Funktion.

- Malwareanalyse

Dieser Teil der Analyse greift immer dann ein, wenn eine neue Malware entdeckt wird. Es gibt Überschneidungen zur Schwachstellenanalyse, wenn die neue Malware eine ebenfalls neue Sicherheitslücke ausnutzt.
Wie bei jeder Analyse muss die Malware systematisch untersucht werden, und die Ergebnisse müssen dokumentiert werden. Diese Arbeit wird heute vor allem von der Anti-Malware Industrie geleistet. Zunächst muss die Wirkung der Malware ermittelt werden. Bei replikaktiver Malware zählt hierzu auch der Verbreitungsmechanismus. In jedem Fall sind die Schadfunktionen zu untersuchen sowie alle weiteren Effekte, die die Malware sonst noch haben könnte.
Dies wird entweder durch Untersuchung des Quellcodes geleistet, oder durch Reverse Engineering des Maschinencodes, falls der Quellcode nicht verfügbar ist. Aus der Analyse der Malware werden wiederum Gegenmaßnahmen abgeleitet, mit denen der Schaden durch diese Malware verhindert, reduziert oder rückgängig gemacht werden kann.

Nach der Analyse eines Vorfalls erfolgt die eigentliche Vorfallbehandlung. Die einzelnen Konzepte der Vorfallsbehandlung folgen nun in den weiteren Unterabschnitten.

3.2. Reinigung (cleaning)

Unter Reinigung wird die Säuberung eines Systems von allen unerwünschetn Hinterlassenschaften eines Vorfalls verstanden. Korrektes Reinigen setzt eine gute

Vorfallsanalyse voraus, denn ohne genaue Kenntnis darüber, was durch den Vorfall verändert wurde, könnten die Reinigungsmaßnahmen den Systemzustand noch verschlimmern.
Auch müssen nach der Analyse die geeigneten Reinigungsmaßnahmen erst einmal erarbeitet werden. Denn selbst wenn feststeht, was und wie gereinigt werden muss, so müssen diese Konzepte noch korrekt in den Reinigungsprozess übersetzt werden.
Bevor wir die Einzelheiten des Reinigens erläutern, soll zunächst das saubere System nach [RFC 2828] definiert werden:

Clean system:
A computer system in which the operating system and application system software and files have just been freshly installed from trusted software distribution media.

Wie an der Definition zu sehen ist, können Reinigungsmaßnahmen also niemals wirklich ein sauberes System erzeugen, es sei denn, die Maßnahmen bestehen in einer Neuinstallation des Systems. Ziel der Reinigung ist also, einen Systemzustand herzustellen, der dem des sauberen Systems möglichst nahe kommt.
Geeignete Reinigungsmaßnahmen müssen zu jedem Vorfall oder zumindest zu jeder Vorfallsklasse getrennt erarbeitet werden. Die einzige pauschal wirksame Maßnahme ist die Neuinstallation, die jedoch in hochverfügbaren Systemen oft nicht ohne weiteres möglich ist, da während der Neuinstallation die Hochverfügbarkeit nicht gewährleistet ist. Um eine geeignete Maßnahmen zu finden, muss bekannt sein, was durch den Vorfall am System verändert wurde. Dazu werden zunächst Zeitpunkte für den Beginn und das Ende des Vorfalls als Messzeiten festgelegt. Wie diese Zeitpunkte zu wählen sind, geht im Idealfall aus Erfahrungen mit ähnlichen Vorfällen hervor. Zum ersten Zeitpunkt gilt das System noch als unverändert, zum zweiten als durch den (abgeschlossenen) Vorfall verändert. Die Unterschiede am Systemzustand, gemessen an beiden Zeitpunkten bilden dann die Veränderungen, die der Vorfall verursacht hat.
Während der Vorfallsanalyse können Informationen über Veränderungen gesammelt werden, aber diese sind oft unvollständig. Dies gilt vor allem dann, wenn der Systemzustand des Zeitpunkts vor dem Vorfall nicht bekannt ist. Deshalb bietet sich hier eine Simulation des Vorfalls im Labor an, wo der Zustand des verwendeten Testsystems vor dem Versuch problemlos aufgezeichnet werden kann. Ein solcher Versuch hat die im Abschnitt 3.1. angedeuteten Nachteile. Der Vorfall muss möglichst genau auf den Laborversuch abgebildet werden, wodurch sich zwangläufig Unschärfen ergeben. Bei der Analyse einer Malware sind die Ergebnisse eines Tests aber dennoch meistens zufrieden stellend.
Wird die Veränderung am Systemzustand untersucht, den eine Malware hervorgerufen hat, gestaltet sich der Labortest vergleichsweise einfach, wenn diese Malware im Quellcode vorliegt. Entweder lassen sich die Veränderungen direkt aus dem Code ablesen, oder die Malware wird im Debuggingmodus gestartet und untersucht. Dabei hält das Programm nach jedem Befehl oder bei gesetzten Wartepositionen an und gibt dem Betrachter die Möglichkeit,

die Wirkung jedes Befehls nachzuvollziehen. Derartige Versuche werden heutzutage nur noch selten von den IRT selber durchgeführt. Stattdessen übernehmen die Anti-Malware Hersteller diesen Teil der Analyse, da ihre Labore speziell für diese Arbeiten ausgestattet sind.
Aus der Analyse ergibt sich ein Katalog, welche Auswirkungen der Vorfall auf das System hat. Diese Veränderungen fallen in folgende grobe Klassen:

- Löschen von Dateien
- Hinzufügen von Dateien
- Ändern von Dateien

Diese Punkte umfassen nur die am System statisch komparativ messbaren Effekte. Effekte, die auf den Festplatten des IT Systems keine Spuren hinterlassen, wie etwa Datenspionage oder das Verbrauchen von Rechenzeit, können mit Reinigungsmaßnahmen nicht ungeschehen gemacht werden. Die Reinigungsmaßnahmen müssen statisch komparativ messbare Veränderungen am System wieder umkehren. Dies bedeutet im Einzelnen:

- Gelöschte Dateien müssen identifiziert und wiederhergestellt werden. Dazu muss bekannt sein, welche Dateien durch den Vorfall gelöscht wurden. Wiederherstellungsmaßnahmen sind nur dann erfolgreich, wenn der Speicher auf dem Datenträger noch nicht anderweitig beschrieben wurde. Deshalb müssen sie möglichst schnell nach dem Vorfall erfolgen.
- Hinzugefügte Dateien müssen ebenfalls identifiziert und anschließend gelöscht werden. Um zusätzliche Sicherheit zu erzielen, sollten diese Dateien so gelöscht werden, dass sie nicht ohne weiteres wieder hergestellt werden können.
- Geänderte Dateien, außer es handelt sich um Protokolldateien, müssen in ihren alten Zustand versetzt werden. Dazu muss entweder die alte Datei verfügbar sein, oder es muss exakt bekannt sein, welche Veränderungen der Datei widerfahren sind.

Um diese Ziele zu erreichen, müssen die Veränderungen durch den Vorfall am System katalogisiert werden. Für die Reinigung wird jeder Punkt dieses Katalogs abgearbeitet und der umgekehrte Effekt auf das System bzw. die betroffene Datei angewandt. Einige Veränderungen lassen sich aber nicht ohne weiteres beheben, weil beispielsweise das Löschen eines Abschnitts aus einer Datei in der Regel nur dann behebbar ist, wenn die Originaldatei noch existiert.
Falls der Vorfall in eine Vorfallsklasse gehört, in der die einzelnen Vorfälle immer nach dem gleichen Schema ablaufen, bietet sich das Entwickeln eines Reinigungstools an. Dies ist bei der meisten Malware der Fall, denn oft werden Systeme einer Klasse, z.B. eines bestimmten Betriebssystems, durch eine Malware immer auf dieselbe Weise verändert, egal auf welchem konkreten System sich die Malware befindet. Solche Tools werden von der Anti-Malware

Industrie für viele Malwareprogramme zur Verfügung gestellt oder sind in die Malwarescanner bereits integriert. Der Scanner verfügt in diesem Fall über eine spezielle Reinigungsoption. Die Aufgabe eines IRT besteht häufig nur noch in der Identifikation des Vorfalls als Auftreten einer bestimmten Malware und dem Weiterleiten des entsprechenden Reinigungstools.
Solche Tools bringen allerdings auch Nachteile mit sich. Da niemals alle möglichen Systemkonfigurationen bekannt sein können, das Tool aber nur schablonenhaft vorgeht, gibt es immer Systeme, auf denen das Cleaning fehlschlägt. Entweder werden betroffene Dateien übersehen oder es werden die falschen Dateien „gesäubert“ oder gar gelöscht. Aus diesem Grund stellt sich immer die Frage, ob nicht eine Neuinstallation des Systems einer Reinigungsmaßnahme vorzuziehen ist. Wie die Antwort ausfällt, hängt vom System und vom Grad der Verseuchung ab. Auf einem Privatsystem ohne wichtige bzw. wertvolle Daten ist eine Neuinstallation leicht durchführbar und stellt die anschließende Sauberkeit des Systems sicher (siehe Definition des sauberen Systems). Reinigungsmaßnahmen sind hier nur angebracht, wenn lediglich wenige Dateien betroffen sind und sich diese auch leicht bereinigen lassen. Ist dagegen ein sensibles System in einem Unternehmen oder gar ein ganzes Netz betroffen, so können Reinigungsmechanismen überlebenswichtig sein. Vor allem, wenn wichtige Daten auf dem System vorhanden sind, werden diese durch eine Neuinstallation vernichtet. Dies lässt sich nur durch regelmäßige Back-Ups verhindern, die eventuell nicht vorhanden sind. Außerdem benötigt die Neuinstallation eines komplexen Systems in der Regel mehr Zeit als eine Säuberung. Da während dieser Zeit das System nicht benutzt werden kann, ist es bei einer Säuberung eventuell wieder schneller verfügbar (abhängig von dem Grad der Auswirkungen des Vorfalls auf das IT System). Allerdings steigen mit der Komplexität des Systems auch die Risiken des Cleanings, weshalb die Entscheidung zwischen Reinigung und einer Neuinstallation immer im Einzelfall abzuwägen ist.

3.3. Vermeidung (avoidance)

Unter Vermeidung werden alle präventiven Maßnahmen verstanden, um das Eintreten eines Vorfalls zu verhindern. Abzugrenzen ist dieser Begriff von der Risikovermeidung aus dem ersten Kapitel, bei der es darum ging, den Geschäftsprozess am Risiko vorbeizuleiten. Bei Vermeidung geht es zwar auch darum, die Prozesse am Vorfall vorbeizuleiten (also den Vorfall zu verhindern). Auf welche Weise dies geschieht, kann sehr vielfältig sein. Die ergriffenen Maßnahmen können Risikovermeidung beinhalten, aber auch andere Dinge.
Nach [Kossakowski 00] zeichnen sich Vermeidungsmaßnahmen dadurch aus, „dass ein konkreter technischer Zusammenhang mit konkreten oder potentiellen Vorfällen besteht“. Jede Maßnahme ist also auf einen bestimmten Vorfall oder eine Vorfallsklasse zugeschnitten. Dabei können die Maßnahmen viele unterschiedliche Formen annehmen. Beispielweise könnte das Sammeln und Weitergeben von wichtigen Informationen über mögliche Vorfälle

zahlreiche tatsächliche Vorfälle verhindern. Eine andere Maßnahme wäre die Änderung des Systems durch Einbau einer Präventivsoftware, wie etwa einer Firewall. Es gibt noch weitere Maßnahmen, von denen sich nach [Kossakowski 00] die meisten im Risikomanagement wieder finden.
[Kossakowski 00] nennt eine Reihe von Dienstleistungen, die ein IRT zum Zwecke der Vermeidung anbietet. Dabei handelt es sich genau genommen nicht um Incident Response Maßnahmen, denn es handelt sich nicht um die Bearbeitung bereits eingetretener Vorfälle, sondern um das Verhindern derselben. Die angebotenen Dienstleistungen sind die folgenden:

- Announcements
- Technology watch
- Security audit
- Neighborhood watch
- Security tools
- Tool development
- Intrusion detection

Im weiteren Verlauf werden die einzelnen Punkte nun näher betrachtet, vgl. [Kossakowski 00].

Announcements
Unter Announcements wird die Verteilung von Warnungen und Hinweisen verstanden. Wie und an wen diese Informationen verteilt werden, kann sehr unterschiedlich sein. Neben der Erhöhung des Informationsstands und der Wachsamkeit dienen die Announcements indirekt auch zur Vorfallsentdeckung. Announcements gehören laut [Kossakowski 00] bereits seit 1988, also seit Gründung der ersten IRTs, zu den Standarddienstleistungen.
Meist erfolgen Announcements über Mailinglisten, in die sich die Interessierten eintragen. Es gibt von vielen IRTs aber auch Informationsserver mit Suchfunktionen. Ähnliche Server stellen auch die Anti-Malware Hersteller bereit.
Nach [West-Brown et al.] gibt es folgende Arten von Announcements:

- Heads up

Hierbei handelt es sich um eine kurze Nachricht an die wartende Gemeinde der Interessenten, also etwa die Mitglieder einer Mailingliste. Sie kann dazu dienen, eine Vorwarnung zu geben, um Geduld zu bitten, oder auch nur dazu, die Flut eingehender Anfragen einzudämmen, während das IRT daran arbeitet, nähere Informationen zu erhalten, die dann anschließend publiziert werden können.

- Alert

Ein Alarm oder Alert ist eine kurzfristige Nachricht über einen drohenden Angriff oder ein Problem. Er kann die Verantwortlichen in bedrohten Organisationen warnen und zur Wachsamkeit aufrufen, ohne bereits Details über den Angriff zu beinhalten.

- Advisory

Diese Art der Information ist eine Sammlung von Hinweisen und Ratschlägen zu einem Problem, die auf mittel- bis langfristigen Informationen beruhen. Advisories basieren auf gesicherten, vollständigen Informationen über ein Problem und seiner Lösung.

- For your information

Nachrichten vom Typ for your information, kurz FYI, dienen ebenso wie Advisories der mittel- bis langfristigen Information über ein Problem. FYI richten sich aber weniger an die direkt betroffenen in einer Organisation, sondern an die breite Masse der Interessierten. Deshalb enthalten FYI oft weniger technische Details als Advisories.

- Guideline

Richtlinien oder Guidelines beschreiben langfristig gültige Schritte zur Lösung eines Problems. Sie richten sich an eine ganze Personengruppe, die innerhalb der Organisation mit der Lösung des Problems betraut ist.

- Technical procedure

Dies sind ebenfalls Richtlinien, die jedoch eher auf die technischen Details eingehen als auf die organisatorische Problemlösung.

Technology watch

Diese Dienstleistung lässt sich grob als Überwachung, Katalogisierung und Diskussion der Technologien beschreiben. Im Internet werden über Newsgroups, Archive, Foren und Chat Kanäle zahlreiche Diskussionen über Protokolle, Anwendungen und andere computerrelevante Dinge geführt. Oft dreht es sich dabei um Fragen der Handhabung eines bestimmten Programms, um Verbesserungsmöglichkeiten der Effizienz, um neue Einsatzmöglichkeiten von Tools und natürlich auch um Sicherheitsfragen. Dabei handelt es sich um eine unsortierte Menge von (nur teilweise) sicherheitsrelevanter Informationen, die von ihren Eigentümern nicht näher katalogisiert oder aufbereitet wird.

Diese Aufbereitung solcher Informationen wird Technology watch genannt und ist Aufgabe der IRT. Aus der Aufbereitung werden dann eigene Announcements abgeleitet, die wiederum an die eigene Klientel weitergegeben werden. Das Auswerten selber ist dabei allerdings kein nach außen angebotener Dienst. Kein IRT möchte mit Anfragen, wie etwa „Werte mir Archiv XYZ auf sicherheitsrelevante Informationen aus“ überschüttet werden. Da die Technology

watch sehr zeitaufwendig ist, werden oft nur ausgewählte Quellen untersucht, diese dafür jedoch regelmäßig. Außerdem erfordert die Arbeit einen sehr hohen Sachverstand, da die Informationen in den Quellen nicht zwangsläufig korrekt und vollständig sein müssen.

- Security audit

Secutity audit ist eine Dienstleistung, die sich mit der Überprüfung des bestehenden Sicherheitsniveaus in einem System befasst. Das Ziel besteht darin, möglichst gesicherte Erkenntnisse über das System zu erlangen und bestehende Sicherheitslücken zu identifizieren. Nach [Kossakowski 00] gibt es folgende Möglichkeiten eines Sicherheitsaudits:

- Zero-knowledge penetration

Bei dieser Methode werden ohne jegliche Vorbereitung und ohne Vorwissen sämtliche Informationen gesammelt, die über das System bekannt sind, insbesondere über die Infrastruktur und die Prozessabläufe. Danach werden diese Informationen, meist mit Hilfe von Tools, ausgewertet, um nach Sicherheitslücken zu suchen. Dabei werden die Systembereiche nicht nach ihrem Sicherheitsbedarf gewertet: Alle Systemteile gelten in Bezug auf den Sicherheitsbedarf als gleichrangig.

- In-Depth analysis

Hierbei wird ein bestimmter, besonders kritischer Systemteil von außen getestet. Die Analyse ist dabei so intensiv wie möglich, deshalb werden alle zur Verfügung stehenden Mittel eingesetzt. Eine Beschränkung des Testumfangs unter den Radius des Möglichen ist nur dann angezeigt, wenn der Systemteil nur für kurze Zeit zu Testzwecken aus dem Betrieb herausgenommen werden kann, wie etwa bei Systemteilen, die hochverfügbar sein müssen.

- Review

Bei einem Review wird ein Systemteil passiv auf Sicherheitslücken analysiert. Er wird also keinem simulierten Angriff ausgesetzt, sondern mit Hilfe von Vulnerability Scannern oder manuell auf Sicherheitslücken überprüft. Nicht nur die Programme selbst, sondern auch ihre Konfigurationen werden dabei untersucht.

- Observed attacks

Eine beobachtete Attacke wird durchgeführt, um zu untersuchen, wie sich ein Systemteil verhält, bzw. ob er anfällig für diese Attacke ist. Observed attacks sind auch nützlich, um die Warnmeldungen und Gegenmaßnahmen bestimmter Sicherheitsprogramme wie Firewalls und Intrusion Detection Systemen auf ihre Korrektheit und Verständlichkeit zu untersuchen.

- Zertifizierung

Eine Zertifizierung unterzieht den zu untersuchenden Systemteil einem formalisierten und standardisierten Analyseprozess. Der Prozess ist deshalb formalisiert, damit er wiederholt und auf viele verschiedene Systeme angewandt werden kann. Besteht der Systemteil den Test, so erhält er ein Sicherheitszertifikat für das definierte Sicherheitsniveau. Das Zertifikat dient nicht nur dem Unternehmen selbst als Bestätigung ihrer Sicherheit, sondern soll auch potentiellen Kunden die Sicherheit des Systems garantieren.

Soll ein System oder ein Systemteil auf Verwundbarkeiten hin getestet werden, kommen oft so genannte Tiger Teams zum Einsatz. Dabei handelt es sich um externe Gruppen von Angreifern, die das System von außen penetrieren sollen. Dabei gelten die betriebsinternen Regeln für Tiger Teams nicht, damit Angriffe unter realen Bedingungen stattfinden können. Natürlich sollen die Tiger Teams keinen wirklichen Schaden anrichten, sondern nur Schwachstellen aufzeigen. Tiger Teams müssen nach [Kossakowski 00] deshalb von außen arbeiten, weil Betriebsangehörige zu sehr durch die Betriebsregeln vorbelastet sind, und deshalb leicht mögliche Angriffsformen übersehen.
Es gibt einige Gründe, die für und gegen den Einsatz von Tiger Teams sprechen. Dafür spricht, dass Mitglieder eines Tiger Teams „Experten“ auf ihrem Gebiet sind, und dass dieses Fachwissen innerhalb der Organisation oft nicht verfügbar ist und auch nicht verfügbar sein soll. Zudem nutzen Externe alle Unsicherheiten aus, die sie aufspüren können, während interne Mitarbeiter eventuell ein Interesse daran haben könnten, Unsicherheiten im System zu verschleiern. Gegen den Einsatz von Tiger Teams spricht, dass Externe möglichst nichts über Unsicherheiten des Systems wissen sollten, es aber durch ihre Aktivitäten im Tiger Team zwangsläufig erfahren. Falls die Mitglieder des Tiger Teams zweifelhafte Charaktere sind, ist die Gefahr des Informationsmissbrauchs besonders groß. Zudem ist immer unklar, wie die gewonnenen Informationen behandelt werden sollen. Nach dem Angriff eines Tiger Teams ist das Wissen über die Schwachstellen nur dem Tiger Team bekannt, benötigt wird dieses Wissen aber intern. Es muss gewährleistet werden, dass das Wissen vollständig weitergegeben wird.

Neighborhood watch

Der Hauptnachteil beim Security audit besteht darin, dass die Ergebnisse der Analyse veralten. Eventuell geschieht das sehr schnell, denn im unglücklichsten Fall kann sofort nach Abschluss der aufwendigen Analyse eine neue Sicherheitslücke bekannt werden.
Um diese Schwäche zu kompensieren, wird das so genannte Neighborhood watch durchgeführt. Dabei werden die Systemteile in meist regelmäßigen Abständen daraufhin überprüft, ob sie auch den neuen Sicherheitsgefahren gewachsen sind. Diese Untersuchungen können nach [Kossakowski 00] mit zwei unterschiedlichen Zielrichtungen angesetzt werden. Bei der ersten Methode werden einzelne Systemteile detailliert auf Anfälligkeiten gegen neue Bedrohungen überprüft. Diese Methode ist sehr aufwendig, wenn sie regelmäßig für alle

Systemteile angewendet werden soll. Sie liefert dafür aber auch sehr verlässliche Ergebnisse. Die zweite Methode untersucht flächendeckend das ganze System. Dabei werden eventuell nicht alle Sicherheitslücken gefunden. Deshalb ist die Herangehensweise ein wenig anders als bei der Detailanalyse. Statt nach einzelnen Sicherheitslücken zu suchen, wird geprüft, welche Funktionen auf dem System oder Systemteil erlaubt sind, und ob damit nach der Sicherheitspolitik unerlaubte Kommunikationen möglich sind.
In den meisten Fällen ist die zweite Methode vorzuziehen. Die Analyse braucht sehr viel weniger Zeit als die Untersuchung in der Tiefe. Somit können größere Teile des Systems untersucht werden, und die Abstände zwischen den einzelnen Tests sind kleiner wählbar. Da die Methode aber weniger vollständig ist, sollte in größeren Abständen zusätzlich eine Detailanalyse angesetzt werden.

Security Tools

Die Industrie für IT Sicherheit bietet eine Vielzahl von Tools an, um das Sicherheitsniveau auf Systemen zu erhöhen oder um Systeme zu reinigen. Die Vorteile, die solche Tools bieten, liegen auf der Hand. Allerdings müssen die meisten dieser Tools korrekt installiert werden und benötigen zudem eine fachmännische Konfiguration. Ein Beispiel hierfür ist etwa eine Firewall. Sie muss an der passenden Stelle eines Rechnernetzes eingesetzt werden, je nachdem, welche Ziele durch ihren Einsatz verfolgt werden sollen. Außerdem müssen die Sicherheitsvorgaben korrekt in die Filterregeln der Firewall umgesetzt werden. Häufig sind auch mehrere gekoppelte Firewalls nötig.
Diese Aufgaben sind sehr umfangreich, und durch die Verfügbarkeit einer Vielzahl verschiedener Tools für dieselbe Aufgabe werden Installation und Konfiguration noch komplexer, da Vorwissen über die Handhabung eines Tools nicht ohne weiteres auf andere Tools übertragen werden kann.
Oft ist das nötige Know How zur Auswahl eines passenden Tools, seiner Installation, Konfiguration und Pflege in einer Organisation nicht verfügbar. Manchmal sind sich die Mitglieder einer Organisation nicht einmal bewusst, dass passende Tools existieren. An dieser Stelle können IRTs helfen. Sie können nach Belieben eine, mehrere oder alle Aufgaben beim Einsatz von Sicherheitstools übernehmen. So könnte ein IRT eine Organisation bei der Auswahl einer geeigneten Firewall beraten, diese auf dem passenden Rechner im Netz installieren und anschließend gemeinsam mit der Organisation eine Konfiguration erarbeiten. Fraglich ist allerdings, ob die permanente Wartung eines Tools in den Aufgabenbereich eines IRTs fällt. Nach hier vertretener Ansicht ist dies nicht der Fall, stattdessen hat das IRT eher die Aufgabe, im Falle von akuten Problemen, also „bei Bedarf“ zu helfen.
Nach [Kossakowski 00] ist vom Bereich Secutity Tools als Teil der Dienstleistung Avoidance der Einsatz von Labortools abzugrenzen, die das IRT selber einsetzt, um Vorfälle zu analysieren. Solche Tools, wie etwa Line Tracer, werden selten in Organisationen eingesetzt. Stattdessen werden sie vom IRT mitgebracht bzw. im Labor benutzt und nur im konkreten Vorfall zur Analyse benutzt. Sie unterscheiden sich also von den hier diskutierten Security

Tools einerseits dadurch, dass sie sich nicht im Dauereinsatz befinden, sondern immer nur kurzfristig und nicht in der Organisation selber zum Einsatz kommen. Andererseits besteht der Unterschied darin, dass die Analysetools des IRTs nicht das Sicherheitsniveau anheben oder garantieren sollen, wie dies bei Security Tools der Fall ist.

Tool development

Die Unterstützung bei der Installation, Konfiguration und Pflege von Sicherheitstools reicht oft nicht aus, um ein gewünschtes Sicherheitsniveau zu erreichen. Dies liegt daran, dass die Einsatzfelder von Tools in den verschiedenen Organisationen stark variieren können. Zudem hat jede Organisation eine eigene Sicherheitspolitik, die sehr spezielle Aspekte enthalten kann, die für eben diese Organisation sehr wichtig sind, aber in keiner anderen Sicherheitspolitik erwartet würden. Tools können oftmals nur so konfiguriert werden, dass sie die „Standardpunkte“ einer Sicherheitspolitik abdecken. Für spezielle Sicherheitsanforderungen bleibt kein Raum, wenn das Tool vom Hersteller für eine breite Masse von Kunden konzipiert wurde.

Aus diesem Grund ist das Entwickeln von neuen Sicherheitstools ein eigenständiger und wichtiger Punkt im Rahmen der Avoidance. Der Unterschied zu gewöhnlichen Sicherheitstools besteht darin, dass das IRT im Auftrag einer Organisation für diese ein Tool für eine besondere Einsatzumgebung produziert und dieses dann auch installiert, konfiguriert und im Gegensatz zum Punkt Security tools auch wartet. Die Wartung ist in diesem Fall in der Dienstleistung enthalten, da die Wartung normalerweise vom Hersteller oder einer vom Hersteller lizenzierten Wartungsfirma vorgenommen wird, und in diesem Fall IRT und Hersteller zusammenfallen.

Ebenfalls ein wichtiger Teil der Dienstleistung ist die Verteilung von Warnungen, falls am Tool sicherheitskritische Fehler entdeckt wurden.

Tool development ist zu einem erheblichen Teil eine softwaretechnische Aufgabe. Deshalb müssen neben den Sicherheitsanforderungen auch insbesondere softwaretechnische Aspekte berücksichtigt werden. Das Tool development verläuft in folgenden Phasen:

- Bestimmung der Zielsysteme und des Ziels der Programmentwicklung

Zu Beginn des Prozesses wird eine Zielsetzung erarbeitet. Dazu gehört das Abstecken der Aufgaben des Tools anhand der Sicherheitspolitik ebenso wie die Festlegung der Ziele des Programms. Dies sind zwei unterschiedliche Punkte, denn viele Sicherheitsziele lassen sich auf unterschiedlichen Wegen mit unterschiedlichen Implementationen erreichen. Ebenfalls in die erste Phase gehört die Festlegung eines Zeitplans zur Fertigstellung und Inbetriebnahme des Tools.

- Zuweisung der notwendigen Ressourcen

Hierbei handelt es sich um eine rein organisatorische Phase. Es wird festgelegt, welches Personal für welche Aufgaben zuständig ist und wie die Ressourcen und die Zeit aufgeteilt werden.

- Aufstellung der Spezifikation

Diese Phase umfasst die meisten softwaretechnischen Aspekte der Toolentwicklung. Die Spezifikation muss so gestaltet werden, dass mit dem späteren Programm alle gewollten Sicherheitsziele erreicht werden. Aber auch die Frage der Verständlichkeit und der Benutzbarkeit des Tools durch die Anwender bzw. die Administratoren ist hier zu beantworten. Deshalb müssen neben der Sicherheitsanalyse auch Prozessanalysen und Interviews mit den Personen vorgenommen werden, die später mit dem Tool arbeiten sollen. Die softwaretechnischen Aspekte sollen hier nicht weiter vertieft werden. Es soll nur deutlich gemacht werden, dass auch das sicherste Tool immer nur so gut sein kann wie seine Beherrschbarkeit durch seine späteren Nutzer.

- Durchführung der Programmierung

Zur Programmierung sei hier so soviel angemerkt, dass die Spezifikation möglichst genau in das Programm umgesetzt werden muss. Der Idealfall bestünde darin, dass das Tool formal nachweisbar alle Aspekte der Spezifikation umfasst, wenn dieser Fall auch in der Praxis kaum zu erreichen ist.

- Abnahme und Übergang zum Dauerbetrieb

Vor dem Dauereinsatz muss das Tool auf seine Wirksamkeit getestet oder verifiziert werden. Es ist also möglichst genau zu prüfen, ob das Tool das gewünschte Sicherheitsniveau durchsetzt. Zu diesem Punkt gehören auch die ausführliche Dokumentation des Programms, eine abschließende Bewertung der gewonnenen Sicherheit und eine Schulung der Mitarbeiter im Umgang mit dem Tool. Wie bereits gesagt, fällt hier auch die Wartung in den Aufgabenbereich des IRTs.

Intrusion detection

Um Vorfälle frühzeitig zu erkennen, bedarf es der ständigen Beobachtung des Netzverkehrs, der Zugänge zum Netz und der einzelnen Transaktionen oder auch der Akltivitäten auf einzelnen Rechnern. Solche Maßnahmen, die Angriffe oder Ressourcenmissbrauch von innen entdecken sollen, werden unter dem Begriff Intrusion detection zusammengefasst. [RFC 2828] definiert Intrusion detection wie folgt:

Intrusion detection: A security service that monitors and analyzes system events for the purpose of finding, and providing real-time or near real-time warning of, attempts to access system resources in an unauthorized manner.

In dieser Definition muss der Begriff des Systems so verstanden werden, dass er auch ein Netzwerk von einzelnen Rechnern umfasst. Dennoch bieten die meisten existierenden Tools für Intrusion detection nur die Überwachung einzelner Rechner an.
Nach [Kossakowski 00] gehören auch Malwarescanner in den Bereich der Intrusion detection, da sie Viren, Trojaner und andere Malware entdecken und so den durch sie angerichteten Schaden verhindern sollen. Manche Intrusion Detection Systeme leiten automatisierte Gegenmaßnahmen ein, etwa die Benachrichtigung des Administrators oder das Aussondern einer eMail mit verseuchtem Inhalt. Diese Systeme werden auch als Intrusion Response Systeme bezeichnet.
Die Aufgabe eines IRT in diesem Bereich besteht anders als bei Security Tools und Tool development nicht in der Beratung beim Einsatz des Tools in einer Organisation oder dem Entwurf und der Entwicklung des Tools. Vielmehr übernimmt das IRT den Betrieb des Intrusion Detection Systems und seine Feinabstimmung für die Organisation. [Kossakowski 00] stellt eine Sonderform des Outsourcings fest, da zum Betrieb des Intrusion detection Systems eine kontinuierliche Überwachung des Netzverkehrs ebenso notwendig ist wie eine uneingeschränkte Anbindung an die Informations- und Kontrollflüsse der Organisation.

Wie gezeigt wurde, ist Avoidance eines der komplexesten Aufgabenfelder eines IRT, wobei die Anti-Malware Industrie diese Arbeit stark unterstützt. Allerdings werden die umfangreichsten Dienstleistungen wie Tool development heutzutage von den meisten existierenden IRT nicht angeboten. Stattdessen beschränken sich viele IRT im Bereich Avoidance auf das Announcement, da sie hier nicht in die Struktur von einzelnen Organisationen eintauchen müssen. Oft werden neben der breiten Benachrichtigung der Interessenten auch Nachfragen beantwortet. Die meisten IRT bieten keine „Hausbesuche“ oder Analyse zugesandter Daten mehr an, bei denen direkt mit der Organisation zur Problemlösung zusammengearbeitet wird. Um diese Lücke zu füllen, haben viele Unternehmen ihr eigenes IRT gegründet, das sich ausschließlich mit den Sicherheitsfragen des eigenen Unternehmens befasst.

3.4. Gegenmaßnahmen

Viele Vorfälle basieren auf Angriffen von außen oder Ressourcenmissbrauch von innen. Einige von ihnen dauern längere Zeit an oder treten wiederholt auf. Denial of service Attacken beispielsweise blockieren einen im Netz verfügbaren Dienst auf längere Zeit, Missbrauch von Netzkapazität durch privates Surfen tritt üblicherweise wiederholt auf, usw. Oft haben Organisationen großes Interesse daran, nicht nur spontan auf den Notfall zu

reagieren und die Schäden zu beheben, sondern auch daran, den Vorfall erst einmal zu beenden und den Angreifer daran zu hindern, den Angriff fortzusetzen oder zu wiederholen. Solche Gegenmaßnahmen sollen in diesem Unterabschnitt besprochen werden.

Dem Umfang von Gegenmaßnahmen sind ethische Grenzen gesetzt. Viele Privatnutzer mit ausreichender Fachkenntnis versuchen, wenn sie einen Angriff auf ihren Rechner entdecken, nun ihrerseits den Angreifer zu schädigen bzw. lahm zu legen. Dieses im Szenejargon als „Backfire“ bekannte Vorgehen ist unethisch, da es seinerseits wieder einen Angriff darstellt. Ethisch einwandfreie Gegenmaßnahmen haben passiven Charakter. Sie betreffen ausschließlich das eigene System und seine Umgebung und versuchen, weiteren Schaden vom System abzuhalten.

Gegenmaßnahmen stehen teilweise in Konkurrenz zu den Maßnahmen der Avoidance. Der Grund ist darin zu sehen, dass Avoidance auf eine Bedrohung bzw. die Ausnutzung einer Schwachstelle reagiert, eine Gegenmaßnahme aber auf einen konkreten Vorfall. Dennoch können die ergriffenen Maßnahmen gelegentlich zusammenfallen. Nehmen wir als Beispiel ein trojanisches Pferd, welches Passwörter vom System ausliest und an den Angreifer sendet. Dann könnte der Einsatz eines Trojanerscanners einerseits verhindernden Charakter haben, um etwa zu verhindern, dass der Trojaner das System infiziert. Andererseits kann er auch den Charakter einer Gegenmaßnahme haben, um den Trojaner im System aufzuspüren und wieder zu entfernen, um so das Auslesen weiterer Passwörter zu verhindern, und damit den Angriff zu beenden. Zeitlich stehen damit Gegenmaßnahmen nach der Avoidance, aber vor dem Cleaning. Denn bevor das System gesäubert werden kann, muss der Angriff beendet worden sein.

Welche Gegenmaßnahmen geeignet sind, hängt vom konkreten Vorfall ab. Sie sind oft Teil eines Notfallkonzeptes, da zur Wiederherstellung der Betriebsfähigkeit eine Beendigung des Vorfalls Voraussetzung ist. In diesem Fall steht auch hier der Geschwindigkeitsaspekt im Vordergrund, wie auch beim gesamten Notfallkonzept. Beispiele für solche Gegenmaßnahmen wurden im Abschnitt 1.5. unter „unmittelbare Notfallbekämpfung“ bereits gegeben, sie werden wie dort beschrieben in Eindämmungsmaßnahmen und Abstellungsmaßnahmen unterteilt. Diese Gegenmaßnahmen wirken allerdings nur kurzfristig. Wurde nach einiger Zeit der Normalbetrieb wieder hergestellt, ist das System für den Vorfall noch immer genauso anfällig wie vorher. Deshalb gibt es eine zweite Klasse von Gegenmaßnahmen, die langfristiger wirkt. Sie werden nach dem Notfall angesetzt oder im Bedarfsfall erst einmal erarbeitet, was eine Vorfallsanalyse voraussetzt. Ihr Ziel ist es, den Angriff dauerhaft abzustellen, indem das System gegen ihn immun gemacht wird.

Eine beispielhafte Aufzählung von kurzfristigen und langfristigen Gegenmaßnahmen soll im Folgenden gegeben werden. Diese Liste ist allgemein gehalten und nimmt keine Rücksicht auf spezielle Vorfälle, in denen auch spezielle Gegenmaßnahmen vonnöten sind. Es wird insofern kein Anspruch auf Vollständigkeit erhoben.

Kurzfristige Gegenmaßnahmen

- Vom Netz Nehmen

Die einfachste Form, einen Angriff von außen abzustellen besteht darin, den Kommunikationsweg vom Angreifer zum System zu kappen. Dies geschieht üblicherweise dadurch, dass der Eingang ins Netz blockiert wird. Mit dieser Maßnahme können allerdings nur Angriffe von außen, nicht aber Missbrauch von innen unterbunden werden. Zudem muss sichergestellt sein, dass es außer dem Angriffsweg keine alternativen Wege ins Netz gibt, auf die der Angreifer wechseln könnte. Dabei muss es sich nicht um physikalische Leitungen halten. Der Angreifer könnte auch einen ähnlichen Angriff auf derselben Leitung starten, beispielsweise über ein anderes Protokoll.
Aus nahe liegenden Gründen ist das System vom Netz zu nehmen niemals eine langfristige Lösung. Schließlich müssen die Informationen und Dienste der Organisation dauerhaft im Netz verfügbar sein, um kommunizieren zu können.

- Aufzeichnen

Dass auch das Aufzeichnen des Angriffs eine Gegenmaßnahme ist, mag auf den ersten Blick unlogisch erscheinen. Tatsächlich wird dadurch der Angriff nicht aufgehalten. Es können sich aber wichtige Hinweise auf die Identität des Täters und die Art des Angriffs ergeben, wodurch wiederum weitere geeignete Gegenmaßnahmen abgeleitet werden können. Zudem sind Aufzeichnungen für die spätere rechtliche Verfolgung des Vorfalls wichtig.

- Rettung bedrohter Werte

Wird ein Wert bedroht, ist es mitunter möglich, ihn kurzfristig aus dem Gefahrenbereich herauszubringen. So könnten wichtige Akten im Brandfall schnell aus dem Gebäude gebracht werden. Im Falle eines IT Vorfalls gehört das Erstellen eines Panik-Backups in diese Kategorie. Nach Entdeckung eines Angriffs werden die aktuellen Daten so schnell wie möglich noch einmal gesichert. Auch die eventuelle Löschung wichtiger Daten vom angegriffenen Systemteil gehört zur Rettung bedrohter Werte, denn dadurch lässt sich eventuell eine Ausspionierung verhindern.

- Vorcleaning

Das Vorcleaning dient der Entfernung von Malware vom System. Dadurch wird verhindert, dass diese weiteren Schaden anrichten kann. Anders als beim echten Cleaning werden beschädigte Dateien aber nicht wiederhergestellt oder repariert, dies geschieht erst später.

Langfristige Gegenmaßnahmen

- Verbesserungen im Notfallkonzept

Die Analyse eines Vorfalls, vor allem auf Basis der vorgenommenen Aufzeichnungen, kann dazu beitragen, das Notfallkonzept zu verbessern. Dadurch können bei einem erneuten Vorfall der gleichen Klasse Schäden effizienter verhindert und beseitigt werden.

- Verbesserung des Schutzes

Dies ist der Punkt, an dem die Gegenmaßnahmen mit den Maßnahmen zur Avoidance zusammenfallen. Einer Organisation wird oft erst nach einem Vorfall verstärkt die Notwendigkeit von schützender Hard- und Software bewusst. So kann die Integration einer Firewall, eines Intrusion Detection Systems oder anderer Schutzmaßnahmen eine wirksame langfristige Gegenmaßnahme sein.

- Umstellung der Infrastruktur

Als Antwort auf einen Vorfall können die Infrastruktur und der Prozessablauf in einem Unternehmen geändert werden (siehe hierzu auch die Gegenmaßnahmen im Risikomanagement, Abschnitt 1.4.). Durch eine geeignete Anpassung kann die Organisation gegen einen weiteren Vorfall immun werden. Auch hierzu sind wieder eine detaillierte Aufzeichnung des Vorfalls und eine Vorfallsanalyse erforderlich. Außerdem muss geprüft werden, inwieweit die erforderlichen Strukturanpassungen in der Organisation umgesetzt werden können.

- Rechtliche Schritte

Ist ein Angreifer identifiziert worden, können gegen ihn rechtliche Schritte eingeleitet werden. Dies führt dazu, dass dieser Angreifer für sein Tun im Rahmen des geltenden Rechts bestraft wird. Außerdem kann es eventuell andere potentielle Angreifer davon abhalten, einen ähnlichen Angriff zu versuchen. In Abschnitt 3.6. werden rechtliche Schritte noch näher betrachtet.
Geht der Vorfall auf Ressourcenmissbrauch von innen oder auf die Nachlässigkeit eines Mitarbeiters zurück, so kann der Betroffene entlassen werden. Hierdurch wird die Ursache des Vorfalls bekämpft.

- Anpassung der Sicherheitspolitik

Mitunter geschehen Vorfälle aufgrund von Aktivitäten, die durch die Sicherheitspolitik nicht untersagt wurden. In einem solchen Fall muss eine Anpassung der Sicherheitspolitik in Betracht gezogen werden. Zwar lassen sich Vorfälle nicht einfach „verbieten“, aber wenn die Sicherheitspolitik in der Organisation konsequent durchgesetzt wird, pflanzt sich ein Verbot der entsprechenden Aktivitäten konsequent bis in die Implementation der Sicherheit fort.

3.5. Technische Fortschritte

Die Analyse von Vorfällen und die Reaktionen auf selbige können im IT Bereich die technische Entwicklung vorantreiben. Ansatzweise wurde dies im Zusammenhang mit Tool development schon deutlich: Wenn ein IRT für ein bestimmtes Sicherheitsproblem ein neues Tool entwickelt, stellt dieses Tool ein neues Stück Technologie dar.
Der Fortschrittsaspekt im Bereich Tool development ist allerdings relativ gering. Meist werden nur alte und bewährte Sicherheitskonzepte in einem neuen Kontext zusammengefügt, um sie auf das Sicherheitsproblem anzupassen. IRTs könnten die technische Entwicklung noch auf breiterem Feld vorantreiben. Die Fortschritte liegen dabei hauptsächlich in der Weiter- und Neuentwicklung von Software, mit der ein Sicherheitsniveau erreicht bzw. durchgesetzt werden kann. Allerdings können auch völlig neue Sicherheitsmodelle aus der Arbeit von IRT hervorgehen. Diese sind dann vorerst rein theoretische Modelle, die erst später in konkrete Produkte umgesetzt werden.
In der Praxis ist der Aspekt, dass speziell IRTs die technische Entwicklung vorantreiben, noch nicht allzu sehr zum Tragen gekommen. Deshalb sind die folgenden Beispiele eher als Ansatzpunkte zu sehen, wo die Arbeit von IRTs die technische Entwicklung in Zukunft unterstützen könnte.

- Patches

Patches, zu Deutsch „Flicken“, sind zusätzliche Programmstücke, die nachträglich in ein existierendes Programm integriert werden können. Sie sollen Programmfehler, die erst nach der Markteinführung der Software entdeckt wurden, nachträglich korrigieren. Sie werden auch Updates oder Bugfixes genannt.
Mit Patches lassen sich alle möglichen Fehler in einem Programm korrigieren, hier sind jedoch nur diejenigen Patches relevant, durch die Sicherheitslücken in Programmen geschlossen werden. Oft wird nach Bekannt werden einer Sicherheitslücke vom Hersteller nach kurzer Zeit ein Patch für diese Lücke zur Verfügung gestellt. Obwohl das Erstellen von Patches prinzipiell eine Arbeit des Herstellers ist, können IRT mit ihrem Wissen über die Sicherheitslücke den Hersteller beim Entwurf des Patches unterstützen. Zudem wird die Notwendigkeit eines neuen Patches oft überhaupt erst durch ihre Analyse erkannt.

- Neue Modelle

Damit eine Software ein gewünschtes Sicherheitsniveau garantieren kann, bedarf es zunächst fundierter theoretischer Sicherheitsmodelle, auf denen die Software fußt. Ein passendes formales Modell kann beweisbar eine bestimmte Sicherheitsanforderung umsetzen. Wurde dieser Beweis geführt, kann das Modell in ein Programm umgesetzt werden. Im Idealfall ist die Umsetzung eines Modells in ein Programm wiederum beweisbar korrekt. Genau genommen müsste bei jedem Schritt der Programmentwicklung ein Beweis darüber geführt werden, dass das Sicherheitsniveau der früheren Entwicklungsschritte auch beim nächsten

Schritt erhalten bleibt, also beim Modell selber, der Programmspezifikation, der Programmierung, der Kompilation, der Assemblierung usw.
Dieser Idealfall tritt in der Praxis höchstens für sehr einfache oder lebenskritische Programme ein. Ein beweisbar sicheres Modell ist zum Beispiel das Bell La-Padula Modell zur Durchsetzung der Vertraulichkeit. In ihm wird die mandatorische Zugriffskontrolle auf Systemressourcen modelliert. Solche Modelle wurden schon für die Entwicklung von Programmen, vor allem von Betriebssystemen, verwendet, wenn auch nicht beweisbar korrekt.
Es ist möglich, dass in Zukunft die Arbeit von IRTs neue Möglichkeiten zur Erstellung von Sicherheitsmodellen aufzeigt. Dazu müssten allerdings die vielen einzelnen Analysen zusammengefasst werden, um einen Weg aufzuzeigen, wie eine Software prinzipiell sicherer gemacht werden kann, zumindest für einige ausgewählte Sicherheitsaspekte. Die momentane Arbeit von IRTs besteht dafür noch zu sehr aus Flickwerk, da sie sich nur um einzelne Vorfälle kümmert.

- Hardware

Systemsicherheit kann auch durch Hardware durchgesetzt werden, oft sogar besser als durch Software. Ein gutes Beispiel hierzu liefert die Verschlüsselungstechnik. Wird eine Verschlüsselung in einem zusätzlich beispielsweise passwortgeschützten Hardwarebaustein ausgeführt, besteht beispielsweise für den Diebstahl des privaten Schlüssels kaum eine Chance. Wird dagegen nur auf der Ebene der Software verschlüsselt, kann ein Schlüssel eventuell von einem Angreifer ausgelesen werden.
Zudem gilt auch für die Hardware das altbekannte Prinzip, dass ein System nur die Teile enthalten sollte, die es wirklich braucht. Ein Standalone System benötigt beispielsweise keine Netzwerkkarte, also sollte es auch keine enthalten. Ansonsten würde der Betreiber sich vollkommen unnötig dem Risiko netzbasierter Angriffe aussetzen, sofern die Netzwerkkarte mit einem Netz verbunden wird. Dieses Prinzip wurde auch schon in der Firewalltechnik umgesetzt. So gibt es beispielsweise inzwischen Firewalls, die auf einem fertigen Rechner geliefert werden und deren komplette Konfiguration auf einer schreibgeschützten Bootdiskette gespeichert ist. Somit benötigt der Firewallrechner keine Festplatte mehr, auf der sich Malware einnisten könnte.
Bei der Entwicklung von Hardwarelösungen wie etwa solchen Firewalls können IRTs durch die Ergebnisse ihrer Arbeit Hilfestellung leisten. Die Analyse von Vorfällen zeigt unter anderem, welche Teile eines Systems durch einen Vorfall besonders gefährdet sind. Daraus können Konzepte erwachsen, auf welche Komponenten bei sicherheitskritischen Systemen verzichtet werden sollte, bzw. ob diese in einen festen, schwer angreifbaren Hardwarebaustein ausgelagert werden können.

- Neue Tools

Dieser Aspekt wurde bereits beim Tool development angesprochen: IRTs können für spezielle Kontexte neue Tools entwickeln und erstellen. Zusätzlich zum Tool development von Sicherheitstools für eine Organisation können IRT allerdings auch Tools entwickeln, die sie bei ihrer eigenen Arbeit besser unterstützen. Solche neuen Tools verbessern dann die Analysemöglichkeiten des IRTs.
Vermutlich ist der Aspekt der Tools derjenige, bei dem die IRT am stärksten Einfluss auf die technische Entwicklung nehmen können. Tools sind oft für einen begrenzten Kontext gedacht und lassen sich daher besonders leicht aus der Analyse einiger weniger Vorfälle gewinnen.

- Protokolle

Viele Sicherheitsprobleme liegen in den Kommunikationsprotokollen selber verborgen. So haben weit verbreitete Protokolle wie das Internetprotokoll (IP) zahlreiche Schwächen.
Diese Schwächen sind darin begründet, dass diese Protokolle mehr ermöglichen, als eigentlich ihrer Aufgabe entspricht. Hinzu kommt, dass viele Internetprogramme diese „Zusatzfunktionen“ benutzen, ohne auf die Sicherheitsrisiken Rücksicht zu nehmen.
Der Grund für diese Schwächen ist in der Geschichte des Internets zu finden. Die ersten Computernetzwerke hatten ihren Einsatzkontext in wissenschaftlichen Einrichtungen mit nur einer stark begrenzten Zahl von Nutzern. Da damals davon ausgegangen wurde, dass diese wenigen Nutzer verantwortungsvoll mit den Netzressourcen umgehen und diese nicht missbrauchen, wurden keinerlei Sicherheitsaspekte in die Protokolle eingefügt. So werden Datenpakete (sofern nicht entsprechende Zusatzfunktionen oder –Protokolle verwendet werden), unverschlüsselt im Klartext übertragen. Adressen können gefälscht, Pakete umgeleitet werden usw.
In letzter Zeit hat die Entwicklung verbesserter Internetprotokolle begonnen, die über entsprechende Sicherheitsfunktionen verfügen. Allerdings basiert ein Grossteil der Internetkommunikation noch immer auf den alten unsicheren Protokollen.

- Anti-Malware

Anti-Malware ist genau genommen ein Teil des Tool-developments. Allerdings ist sie so bedeutend, dass sie hier gesondert aufgeführt werden soll. Die Analyse von Malware, speziell von Viren, Würmern und Trojanern wird hauptsächlich von der Anti-Malware Industrie durchgeführt. Daher ist es nicht verwunderlich, wenn auch die entsprechende Anti-Malware von ihr bereitgestellt wird. Prinzipiell gibt es allerdings keinen Grund, warum IRTs nicht bei dieser Arbeit mithelfen sollten, da die Vorfallsanalyse auch die Analyse von Malware beinhaltet. Wie bereits erwähnt, wird diese Arbeit aber von den heutigen IRTs selten wahrgenommen bzw. nur von spezialisierten wie dem AntiVirus Emergency Responce Team (AVERT) von McAfee.

- Neue Innovationen

Die Arbeit von IRTs kann und wird eines Tages zu völlig neuen technischen Entwicklungen führen. Da auch die Arten möglicher Angriffe sich weiter entwickeln, werden auch die Gegenmaßnahmen und die dafür nötigen Techniken immer fortschrittlicher. Neue Ansätze und Konzepte erwachsen aus der Analyse von Angriffen und Vorfällen. Auch wenn die Entwicklung passender Gegenmaßnahmen nicht in den IRT selber vollzogen wird, können sie dennoch den Grundstein dafür legen.

3.6. Rechtliche Schritte

Oftmals ist eine Organisation nicht nur an der Beseitigung der Folgen eines Vorfalls interessiert, sondern auch an einer Rechtsverfolgung gegenüber demjenigen, der den Vorfall verursacht hat. Dies hat mehrere Gründe. Zum einen ist eine strafrechtliche Verfolgung interessant, um den Täter durch eine Bestrafung davon abzuhalten, weitere Angriffe zu verüben. Zum anderen kann der Täter zivilrechtlich auf Ersatz des verursachten Schadens verklagt werden. Die Ermittlung des Täters und schließlich seine Überführung anhand von Beweisen ist Aufgabe der so genannten forensischen Informatik.
Dieser Aufgabenbereich beschränkt sich im Wesentlichen auf die Vorfallsanalyse, allerdings in einem weiter gesteckten Rahmen. Es geht bei der forensischen Analyse schließlich nicht nur darum, den Angriff an sich zu analysieren, sondern den Täter zu finden. Deshalb scheidet eine Analyse des Vorfalls durch Nachstellung im Labor schon von vorn herein aus, denn es müssen die tatsächlichen Spuren des Angreifers gesucht und ausgewertet werden. Die forensische Analyse eines Vorfalls bis zur Erhebung einer Anklage lässt sich grob in folgende Schritte gliedern:

- Analyse des Vorfalls im klassischen Sinne
- Weg des Angreifers
- Identität des Angreifers
- Spurensicherung beim Angreifer
- Schadensermittlung
- Bestimmung einschlägiger Gesetze
- Erhebung der Anklage

Analyse des Vorfalls im klassischen Sinne

Dieser Schritt beschreibt zunächst eine „gewöhnliche“ Vorfallsanalyse. Ziel ist herauszufinden, um welchen Vorfall es sich handelt und wie in den weiteren Schritten vorgegangen werden muss. Wichtig sind Informationen über mögliche Täterwege, die sich aus der Art des Angriffs folgern lassen. Aus den gewonnenen Indizien und Beweisen werden die Ansatzpunkte für die nächsten Schritte abgeleitet.

Weg des Angreifers

Handelt es sich bei dem zu untersuchenden Vorfall um einen Angriff von außen, muss die Analyse sehr weite Wege gehen. Denn um den Täter zu überführen, muss der vollständige Weg vom Angreifer zum Opfersystem bekannt sein und nachgewiesen werden können. Deshalb müssen die Untersuchungen auch auf das öffentliche Internet ausgedehnt werden. Viele Informationen von Servern, Providern oder anderen Dienstanbietern stehen nicht öffentlich zur Verfügung und müssen erst angefragt werden. Für die Wegeermittlung sollte so viel wie möglich über die Eigenschaften des Angriffs bekannt sein. Wurde Adressfälschung verwendet? Handelt es sich um eine verteilte Attacke? War es eine automatisierte Attacke? Die Beantwortung solcher und ähnlicher Fragen helfen bei der Wegfindung.

Ein Hauptproblem bei der Ermittlung des Täterwegs ist die rasche Veralterung von Informationen. Die Netzarchitektur im Internet unterliegt ständigen Veränderungen, sodass aufgezeichnete Wege eventuell zum Zeitpunkt der Untersuchung nicht mehr existieren. Besonders schwerwiegend ist dieser Punkt bei drahtlosen Netzen.

Das Nachvollziehen des Angriffswegs ist aus zwei Gründen bedeutsam. Einerseits führt das Nachvollziehen des Wegs zum Ursprung des Angriffs und damit zum Angreifer. Andererseits ist der Weg des Angreifers juristisch bedeutsam, weil die Eigentümer und Betreiber der auf dem Weg benutzten Rechner zur Aufklärung des Falls beitragen können.

Identität des Angreifers

War die Ermittlung des Täterwegs erfolgreich, so ist im Idealfall der Rechner oder das Rechnernetz bekannt, von dem aus der Angriff gestartet wurde. Im Anschluss muss untersucht werden, wer als Täter in Frage kommt. Hierzu muss geklärt werden, wer wann Zugriff auf den Rechner oder das Rechnernetz hatte. Eventuell ist bekannt, zu welcher Zeit der Angriff gestartet wurde, was die Suche nach einem passenden Personenkreis einfacher werden lässt. Falls mehrere Personen Zugang zum Rechner oder Rechnernetz hatten, können Profile möglicher Täter ebenfalls weiterhelfen, da sie Auskunft darüber geben, wer ein Motiv für den Angriff gehabt haben könnte. Allerdings ist dies aus Datenschutzgründen problematisch, da Profile von Personen auch leicht missbraucht werden können. Alle Untersuchungen im Umfeld des Startrechners sollten letztlich dazu führen, dass eine Person oder ein kleiner Kreis von Personen als Tatverdächtige feststeht.

Spurensicherung beim Angreifer

Die Spurensicherung beim Angreifer hat zwei wichtige Aspekte. Zum einen dient er der Beweissicherung. Wenn beim Verdächtigen eindeutige Spuren des Angriffs zu finden sind, kann der Verdacht erhärtet werden. Zum anderen können solche Spuren, wie etwa Quellcode von Malware oder frühere Versionen von ihr dabei helfen, ähnliche Angriffe in Zukunft effizienter aufzuklären. Das gleiche gilt für die Informationen, die eine eventuelle Befragung des Verdächtigen hervorbringt.

Zur Spurensicherung beim Angreifer sind viel Know How und die passenden Tools nötig. Oftmals werden Verdächtige ihre Daten löschen, die dann von den Analysatoren wiederhergestellt werden müssen, bevor sie ausgewertet werden können. Da sich für gewöhnlich nicht alle Daten wiederherstellen bzw. auffinden lassen, müssen die gefundenen Teile korrekt zueinander in Beziehung gebracht werden.
Als endgültiges Ziel der Spurensicherung soll eine lückenlose Beweiskette erstellt werden, dass dieser Angreifer von dem ermittelten Startsystem über die ermittelten Wege genau den festgestellten Angriff bei der betroffenen Organisation zu der festgestellten Zeit verübt hat.

Schadensermittlung
Wurde der Angreifer eindeutig und beweisbar ermittelt, folgt die Festlegung der durch den Angriff angerichteten Schäden. Dieser Punkt ist wichtig, um später die korrekte Anklage zu erheben. Es macht keinen Sinn, einen Angreifer, der Forschungsergebnisse ausgespäht hat, dafür verantwortlich machen zu wollen, dass am nächsten Tag die Konkurrenz eben diese Daten selber erforscht hat und auf ihrer Grundlage ein besseres Produkt entwickelt.
Die hier behandelte Schadensermittlung im juristischen Sinne ist keine Aufgabe der forensischen Informatik mehr, denn die geforderte Beweiskette wurde bereits erbracht. Für die Gesamtanalyse des juristischen Falls allerdings ist die Schadensermittlung von Bedeutung.
Zu beantworten ist die Frage, für welche Schäden der Angreifer verantwortlich ist, welche Schäden also aus dem Angriff folgen und somit dem Angreifer zurechenbar sind. Zur Beantwortung dieser Fragen existieren diverse juristische Theorien der Zurechenbarkeit, deren Darstellung hier jedoch über den Rahmen dieser Diplomarbeit hinausgehen würde.

Bestimmung einschlägiger Gesetze
Nach der Schadensermittlung müssen die Gesetze bestimmt werden, auf deren Grundlage später Anklage erhoben werden soll. Für einige Tatbestände existieren solche Gesetze erst seit kurzer Zeit. Zudem können Probleme mit dem Geltungsbereich der Gesetze auftreten, da die Internetkommunikation sich nicht an nationale Grenzen hält. Dies gilt auch für Angriffe. Aber auch außerhalb des Sicherheitsbereichs kann die Bestimmung einschlägiger Gesetze schwierig sein, etwa bei im Internet geschlossenen Geschäftsverträgen über nationale Grenzen hinweg.
In letzter Zeit hat diese Problematik allerdings einen Teil ihrer Bedeutung verloren, da internationale Gesetze geschaffen wurden. Ein Beispiel hierfür ist etwa die internationale Zivilprozessordnung.

Erhebung der Anklage
Als letzter Schritt wird schließlich die Anklage erhoben. Wie bei der Bestimmung einschlägiger Gesetze kann es auch hier dann Probleme geben, wenn der Angriffsweg über Landesgrenzen hinwegführt.

Der hier dargestellte Weg einer forensischen Analyse ist oft nur schwer gangbar. Die forensische Analyse von IT Vorfällen stößt auf zahlreiche Schwierigkeiten. Mittlerweile hat vor allem in der Gesetzgebung ein Prozess eingesetzt, der diese Schwierigkeiten zu beheben versucht, allerdings ist auf diesem Gebiet noch viel Arbeit nötig. Die Probleme bei einer forensischen Analyse lassen sich in vier Klassen einteilen:

- Fehlende Gesetze
- Internationalität des Netzes
- Automation von Angriffen oder Beteiligung mehrerer Personen
- Probleme bei der Beweisführung

Fehlende Gesetze

Noch bis in die späten achtziger und die frühen neunziger Jahre waren zumindest in Deutschland viele wichtige Tatbestände von IT Vorfällen nicht gesetzlich geregelt. Selbst wenn einem Angreifer eine Tat nachgewiesen werden konnte, fehlte es an der gesetzlichen Grundlage für Sanktionen. Beispielsweise wurde der Tatbestand des Computerbetrugs erst 1986 gesetzlich geregelt [Ulrich].

In den letzten Jahren hat sich der Gesetzgeber bemüht, diese Lücken zu füllen. So wurden im Strafgesetzbuch wichtige neue Paragraphen eingefügt. In [StGB] sind jetzt insbesondere enthalten: §202a Ausspähen von Daten, §263a Computerbetrug, §268 Fälschung technischer Aufzeichnungen, §269 Fälschung beweiserheblicher Daten, §303a Datenveränderung und §303b Computersabotage. Nicht alle diese Paragraphen sind neu, bei einigen wurden lediglich bisherige Tatbestände auf den IT Bereich übertragen. Dennoch sind diese Gesetze wichtig, da Angreifer jetzt anhand einer legalen Grundlage zur Rechenschaft gezogen werden können.

Weitere wichtige Gesetze sind das Urheberrechtsgesetz und das Bundesdatenschutzgesetz [BDSG]. In beiden wurden ebenfalls Tatbestände und Rechtslagen für den IT Bereich nachträglich eingeführt. So sind beispielsweise das Urheberrecht an einer Software und Regelungen, wie mit personenbezogenen, elektronisch gespeicherten Daten umzugehen ist, in die Gesetze integriert worden.

Zudem wurden zivilrechtliche Bestimmungen im elektronischen Geschäftsverkehr ins Bürgerliche Gesetzbuch eingefügt. Diese sind jedoch für Vorfälle und ihre Aufklärung von geringerer Bedeutung.

Internationalität des Netzes

Das Internet erstreckt sich weltweit und überbrückt somit zahlreiche Grenzen von Ländern. Diese oft gefeierte Eigenschaft, aufgrund dessen Menschen aus der ganzen Welt miteinander kommunizieren und Geschäfte abschließen können, bringt aber auch einen bedeutenden Nachteil mit sich. Das Netz überbrückt auch die Geltungsbereiche zahlreicher Gesetze. Wenn also ein Vorgang im Netz über große Distanzen stattfindet, stellt sich immer die Frage,

welche Gesetze für welchen Beteiligten überhaupt anwendbar sind. Hierbei spielt es keine Rolle, ob es um einen im Netz geschlossenen Kaufvertrag und dessen Abwicklung oder um die Aufklärung und Verfolgung eines Vorfalls geht.
Auch auf diesem Gebiet haben die Staaten und auch die Bundesländer inzwischen begonnen, die rechtlichen Probleme zu beseitigen. So schlossen zahlreiche deutsche Bundesländer den Mediendienstestaatsvertrag. Nach [MDSTV] hat er folgende Aufgabe:

§1: Zweck des Staatsvertrages ist, in allen Ländern einheitliche Rahmenbedingungen für die verschiedenen Nutzungsmöglichkeiten der im Folgenden geregelten elektronischen Informations- und Kommunikationsdienste zu schaffen.

Der Staatsvertrag legte somit zunächst einmal den Grundstein dafür, dass zumindest deutschlandweit einheitliche Regelungen für den Verkehr im Internet (oder allgemein in der elektronischen Geschäftswelt) gelten. Zumindest in Deutschland ansässige Internetbenutzer können sich nun auf diese Regelungen berufen.
Mittlerweile entstanden auch Ansätze, die Zuständigkeit von Gesetzen international zu regeln. Vor allem innerhalb der europäischen Union gibt es entsprechende Regelungen.

Automation von Angriffen oder Beteiligung mehrerer Personen
Zahlreiche Angriffe im Netz werden nicht von einem Angreifer persönlich verübt und gesteuert, sondern laufen automatisch ab. So breiten sich Viren und Würmer ohne weiteres Zutun des Angreifers (bzw. in diesem Fall des Autors) aus und richten Schaden an. Verteilte Denial of service Attacken benutzen Rechner anderer Personen, von denen aus das Zielsystem lahm gelegt wird. Auch hat ein Autor eines Trojanischen Pferdes keinen Einfluss darauf, wer seine Malware zu welchem Zweck einsetzt. Oft kann er nicht einmal mit Sicherheit sagen, ob sein Programm überhaupt jemals verwendet werden wird.
Hier stellt sich vor allem das Problem, welcher Beteiligte sich vor dem Gesetz zu verantworten hat. Es ergeben sich eine Reihe von Fragen, die größtenteils nicht oder nicht einheitlich in der Rechtsprechung beantwortet werden. Eine Auswahl:

- Ist der Autor einer Malware alleine für den angerichteten Schaden verantwortlich, oder trifft die Schuld auch diejenigen, welche die Malware verbreitet haben?
- Ist alleine das Schreiben von Malware schon zu bestrafen, auch wenn diese nicht eingesetzt wird? Muss die bösartige Software auch implementiert sein, um den eigentlichen Autoren zur Rechenschaft ziehen zu können?
- Wird Malware nicht vom Autor, sondern von einem anderen schadbringend eingesetzt, wer wird bestraft? Der Autor, der andere oder beide? Wie sind die Anteile an der Schuld?
- Ist jemand für Schäden verantwortlich, die durch sein fahrlässig nicht gepatchtes System bei einer verteilten Attacke entstanden sind?

- Entfallen Ansprüche auf Schadensersatz o.ä., wenn die betroffenen Systeme nicht gegen bekannte Sicherheitslücken geschützt werden?
- Kann ein Autor von Malware sich darauf berufen, sein Programm wäre nicht mit maliziöser Intention geschrieben worden (beispielsweise bei den sog. „Remote Administration Tools“)?
- …

Offensichtlich besteht auf diesem Gebiet noch eine Menge Klärungsbedarf. Oft sind an einem Angriff oder Vorfall so viele Personen beteiligt (freiwillig oder unfreiwillig), dass die Klärung der Verantwortlichkeit in Gesetzen sehr schwer fallen dürfte, vor allem wegen der vielen möglichen Fälle

Probleme in der Beweisführung

Dieser Bereich wurde in der Schilderung der forensischen Analyse schon angesprochen. Die Beweisführung wird durch die Schnelllebigkeit der Daten und Wege im Netz und durch die teilweise Nicht-Verfügbarkeit von Logfiles erschwert. Zudem können geschickte Angreifer ihre Spuren zusätzlich verwischen. Vor allem bei verteilten Angriffen oder großflächigen Vorfällen wie dem Auftreten von Würmern kann die Ermittlung eines Täters große Probleme bereiten.

3.7. Reaktionen der Angreifer

Dieser Abschnitt beschäftigt sich mit den Reaktionen der Verursacher von Vorfällen auf die Arbeit der IRTs und andere Maßnahmen gegen Vorfälle. Dieser Aspekt gehört zwar nicht zum Aufgabenbereich von IRTs, ist mit diesem aber eng verflochten, weshalb er hier erwähnt werden soll.

Oft wird das Wechselspiel von Angreifern und denen, die Gegenmaßnahmen entwickeln, mit einem Schachspiel verglichen. Die Angreifer entdecken eine neue Schwachstelle und nutzen diese aus. Dies verschafft ihnen einen „Vorsprung“ gegenüber den Reaktionskräften, die nun ihrerseits eine Lösung gegen den neuen Exploit entwickeln müssen. Auf der anderen Seite entwerfen die Reaktionskräfte mitunter Entdeckungsmaßnahmen, auf die die Angreifer dann ihrerseits reagieren. Als Beispiel hierzu sei das in [Freitag] entworfene und beschriebene Programm zum Aufspüren bösartiger Software genannt.

Die Angreifer, die dieses Wettrüsten betreiben, machen allerdings nur einen Teil der Angreifer aus. Im Allgemeinen lassen sich vier Typen von Angreifern unterscheiden:

- Unfreiwillige Angreifer

Viele Personen, die mit IT Systemen zu tun haben, besitzen nur einen geringen Kenntnisstand im Umgang mit solchen Systemen. In IT Sicherheit wurden sie nicht ausgebildet, oft fehlen

ihnen sogar wichtige Kenntnisse bei der normalen Bedienung ihres Systems. Aufgrund dieser fehlenden Kenntnisse kommt es immer wieder vor, dass Benutzer eines Systems unfreiwillig zu Angreifern werden. Beispielsweise löschen sie aus Versehen wichtige Daten, zerstören ihr System durch Fehlkonfiguration oder laden aus dem Internet unbewusst Malware herunter und führen sie aus. Diese Unwissenheit der Benutzer wird von den „echten“ Angreifern gerne ausgenutzt. Als Beispiel seien Würmer genannt, die sich durch das bloße Ausführen eines eMail Anlages auf dem System ausbreiten und Schaden verursachen können. Hier ist ein aktives, wenn auch unbewusstes, Mitwirken des Benutzers erforderlich.

- Angreifer mit geringer Kompetenz

Die meisten Angreifer, die ihre Angriffe absichtlich durchführen, fallen in diese Kategorie. Es handelt sich hierbei um Personen, die Spaß beim Durchführen von Angriffen und dem Schädigen anderer Leute empfinden. Deshalb versorgen sie sich, meist aus dem Internet, mit Angriffssoftware und wenden diese auf ihre Opfer an. Allerdings fehlt ihnen die Kompetenz, neue Angriffsformen zu entwickeln oder auf Incident Response Maßnahmen zu reagieren.
Angriffe durch Angreifer mit geringer Kompetenz lassen sich häufig vergleichsweise einfach aufklären, weil solche Angreifer zahlreiche Spuren hinterlassen. Außerdem verwenden diese Angreifer nur bereits verfügbare Malware, weshalb ein Großteil der Systeme vor diesen Angriffen geschützt werden könnte, wenn die Betreiber ihre Sicherheitsvorkehrungen aktuell hielten.

- Kriminelle

Diese Kategorie beschreibt die Angreifer, die sich aus ihrem Angriff einen persönlichen Vorteil erhoffen. Sie stehlen beispielsweise geheime Daten, um sie später zu verkaufen. Oder sie greifen ihren früheren Arbeitgeber an, um sich für eine Kündigung zu rächen.
Wie kompetent diese Angreifer sind, kann sehr unterschiedlich sein. Deshalb überschneidet die Kategorie der Kriminellen sich sowohl mit den Angreifern niedriger als auch hoher Kompetenz.

- Angreifer mit hoher Kompetenz

Dies sind die Angreifer, die eine wirkliche Herausforderung für IRTs und andere Sicherheitseinrichtungen darstellen. Sie suchen nach neuen Schwachstellen oder neuen Wegen, Schwachstellen auszunutzen. Dabei produzieren sie neue Malware und andere Angriffsformen. Zudem entwickeln sie Möglichkeiten, Abwehrmaßnahmen zu überwinden.
Die Motivation dieser Angreifer liegt häufig in der Herausforderung. Viele wollen mit ihrer Tätigkeit zeigen, dass eine bislang nur theoretisch angedachte Angriffsform tatsächlich durchführbar ist („prove of concept“).

Im Folgenden sollen einige Formen des Wechselspiels zwischen Angreifern und Sicherheitseinrichtungen aufgezeigt werden. Dabei sind es lediglich die Angreifer mit hoher Kompetenz, die eine Gegenwehr gegen Sicherheitsmaßnahmen entwickeln. Wenn diese aber erst einmal bekannt ist, wird sie oft auch von anderen Angreifern übernommen, weshalb die Sicherheitseinrichtungen auf jeden Fall jede Art von Gegenwehr ernst nehmen muss.

Der wichtigste Aspekt bei diesem Wechselspiel ist die Zweiseitigkeit von Announcements (siehe zu Announcements den Unterabschnitt 3.3). Zum einen warnen diese Meldungen die Systembetreiber vor neuen Schwachstellen, Bedrohungen usw., andererseits werden aber auch die Angreifer mit neuen Informationen versorgt, die ihnen Denkanstöße für neue Angriffe geben können.
Ein weiterer Aspekt ist die Eigeninitiative von Angreifern. Diese suchen selbständig nach neuen Angriffstechniken. Diese werden allerdings oft nicht geheim gehalten, sondern im Gegenteil auf Internetseiten präsentiert und angepriesen. Deshalb können mitunter schon Gegenmaßnahmen im Vorfeld ergriffen werden, wenn die neue Angriffstechnik rechtzeitig aufgefunden wird.
Auch der Fortschritt der Technik bietet neue Gelegenheiten für Angriffe. Hier muss die Sicherheitsindustrie mit ihrer Schwachstellenanalyse von neuen Systemen schneller sein als die Angreifer, damit neue Angriffe möglichst keinen Schaden anrichten können.
Natürlich reagieren Angreifer auch direkt auf die Gegenmaßnahmen der Sicherheitsindustrie. So werden Informationen über neue Angriffstechniken im Netz geschützt, damit die Sicherheitsindustrie sie nicht mehr ohne weiteres abfragen kann. Außerdem werden Maßnahmen entwickelt, um Sicherheitsprogramme wie etwas Firewalls und Virenscanner zu umgehen. So gab es bereits Würmer, die nach dem Eindringen in ein System zunächst einige gängige Virenscanner deinstalliert haben.

Wie erwähnt, ist die Anzahl der Angreifer, die aktiv Gegenwehr leisten, sehr gering. Dennoch ist stets Wachsamkeit gefragt, um nicht nur gegen die Angriffe selber sondern auch für die Gegenwehr gewappnet zu sein.

4. Einfluss von Incident Response auf Notfallkonzepte

Notfallkonzepte dienen der Bekämpfung von Notfällen zur schnellen Wiederaufnahme der Arbeitsprozesse in einem vertretbaren Rahmen. Damit haben die in einem Notfallkonzept enthaltenen Maßnahmen oft Parallelen zu den Handlungen, die ein IRT zur Bekämpfung eines Vorfalls oder Notfalls ergreift. Allerdings gibt es auch Differenzen, da Notfallkonzepte eher kurzfristig ausgelegt sind, während die Arbeit eines IRT die Vorfallsbehandlung in ihrem gesamten Rahmen umfasst.
Ein IRT, bzw. seine Arbeitsergebnisse können Notfallkonzepte beeinflussen und verbessern. Dasselbe gilt für Vorfallsbekämpfungsmaßnahmen, die an einer anderen Stelle wirken. Der Einfluss auf Notfallkonzepte ist jedoch am größten. Dieses Kapitel gibt einen kurzen Überblick über die Möglichkeiten, wie ein IRT auf ein Notfallkonzept einwirken kann.

4.1. Der Zyklus von Notfallkonzept, Vorfall und Incident Response

Werden Gegenmaßnahmen, die ein Betroffener bei einem Vorfall ergreift, in ihrer zeitlichen Aufeinanderfolge betrachtet, so können drei Gruppen von Gegenmaßnahmen unterschieden werden. Präventivmaßnahmen werden vor Eintritt eines Vorfalls ergriffen und sollen sein Eintreten verhindern. Unmittelbar nach dem Vorfall greifen die Maßnahmen eines Notfallkonzepts. Sie sollen die Fortsetzbarkeit der Arbeitsprozesse in einem annehmbaren Rahmen wiederherstellen, wozu auch ein ausreichendes Sicherheitsniveau gehört. Schließlich gibt es die langfristigen Maßnahmen nach einem Vorfall, die den Normalzustand wiederherstellen sollen. Einen Überblick gibt Abbildung 8:

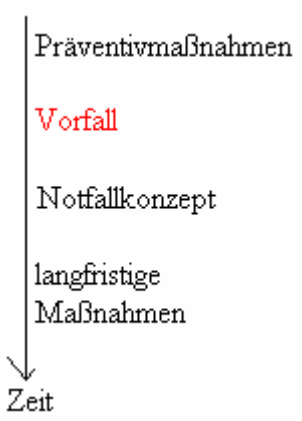


Abbildung 8: zeitliche Einordnung von Gegenmaßnahmen und Vorfall

Obwohl diese Phasen zeitlich nacheinander liegen, können sie überlappen. Beispielsweise kann das Notfallkonzept bereits angelaufen werden, während der Vorfall noch andauert. Während mit langfristigen Maßnahmen die letzten Folgen eines Vorfalls beseitigt werden,

können bereits wieder Präventivmaßnahmen gegen den nächsten derartigen Vorfall ergriffen werden usw.
Die Arbeiten eines IRT können diesen zeitlichen Phasen von Gegenmaßnahmen zugeordnet werden. Dies verschafft einen Überblick darüber, zu welchem Zeitpunkt welche angebotene Arbeit des IRTs die ergriffenen Maßnahmen beeinflusst oder sich mit ihnen deckt. Beispielsweise kann die Reinigung eines Systems im Rahmen eines Notfallkonzepts von einem IRT durchgeführt werden. Hier decken sich die Maßnahmen. Die organisatorischen Maßnahmen eines Notfallkonzepts, etwa die Alarmierung aller Verantwortlichen nach einem Alarmierungsplan, kann von einem IRT zwar empfohlen (etwa durch Beratungen) aber nicht direkt durchgeführt werden. Hier liegt nur eine Beeinflussung vor.
Einen Überblick über die Zuordnung von Incident Response Arbeit und den zeitlichen Phasen gibt Abbildung 9:

Zeitliche Phase		Präventivmaß-nahmen	Vorfall	Notfallkonzept	langfristige Maßnahmen
IRT Maßnahme	Vorfallsanalyse	Nein	Ja	Ja	Ja
	Reinigung	Nein	Nein	Ja	Nein
	Vermeidung	Ja	Nein	Nein	Nein
	Gegenmaßnahmen	Nein	Ja	Ja	Nein

Abbildung 9: Zuordnung von IRT Arbeiten zu den zeitlichen Phasen

Ein Vorfall kann erst nach seinem Eintritt analysiert werden, deshalb wird in der Präventivphase keine Vorfallsanalyse durchgeführt. Danach allerdings können fortlaufende Analysen immer wieder neue Möglichkeiten der Vorfallsbekämpfung aufzeigen, weshalb die Analyse genau genommen erst ganz am Schluss der Vorfallsbekämpfung wirklich abgeschlossen ist. Die Reinigung wird nur im Rahmen der kurzfristigen Maßnahmen des Notfallkonzepts durchgeführt, da die betroffenen Systeme schnell wieder verfügbar sein müssen. Vermeidungsmaßnahmen, die ein IRT anbietet, können ihrer Natur nach nur Präventiv eingreifen. Gegenmaßnahmen, die den Vorfall abstellen oder weiteren Schaden verhindern sollen, können schon während des Vorfalls und im Notfallkonzept eingreifen.

Ob die anstehenden Arbeiten in den einzelnen Phasen tatsächlich von einem IRT übernommen werden, hängt vom konkreten Vorfall und von den gegebenen Umständen ab. Prinzipiell kann ein Betroffener sämtliche Bekämpfungsmaßnahmen natürlich auch ohne ein IRT durchführen. Die Abbildung zeigt lediglich die Möglichkeiten auf, wann und wo ein IRT mit seinen Dienstleistungen Hilfestellung geben kann.
Die Abbildung zeigt ferner, dass die Einflussmöglichkeiten eines IRT in der Phase des Notfallkonzepts am stärksten sind (lediglich die Vermeidungsmaßnahmen spielen in dieser

Phase keine Rolle). Sie zeigt aber auch, dass das IRT während jeder Phase einen Einfluss auf die Vorfallsbekämpfung ausüben und Hilfe geben kann.

Wenn ein eingetretener Vorfall komplett abgehandelt wurde, ist eine Organisation nicht davor sicher, dass ein gleicher oder ähnlicher Vorfall erneut eintritt. Deshalb ist sie immer daran interessiert, die Maßnahmen zur Vorfallsbekämpfung zu optimieren. Die Erfahrungswerte aus einem bereits überstandenen Vorfall sind hierbei eine wertvolle Informationsquelle. Ist ein Vorfall beispielsweise trotz ergriffener Präventivmaßnahmen eingetreten, so kann die Analyse, an welcher Stelle die Prävention versagt hat, Aufschluss darüber geben, wie diese verbessert werden kann. Die verbesserten Präventivmaßnahmen werden für den nächsten Vorfall dann vielleicht ausreichen.
Ähnliches gilt für Notfallkonzepte und langfristige Maßnahmen. Das Notfallkonzept hat sich in der Praxis vielleicht als zu langsam herausgestellt. Oder vielleicht waren die ergriffenen Maßnahmen generell ungeeignet, um den Betrieb schnell wieder aufnehmen zu können. Eventuell wurden die Maßnahmen sogar dermaßen fehlgeplant, dass sie zur Bekämpfung des tatsächlichen Vorfalls gar nicht geeignet waren.
Praxiserfahrungen bieten also große Möglichkeiten für Verbesserungen. Wird ein IRT zur Vorfallsbekämpfung herangezogen und übernimmt dieses einen Teil der Arbeiten, so kann es seine Erfahrungen bei der Bekämpfung des konkreten Vorfalls und in Verbesserungsvorschlägen für die Zukunft umsetzen. Somit kann die Arbeit eines IRT großen Einfluss auf die Planung der Bekämpfung von Folgevorfällen haben. Und da die Einflussmöglichkeiten eines IRT in der Phase des Notfallkonzepts am größten sind, kann Incident Response entscheidend sowohl bei der Umsetzung wie auch der Verbesserung von Notfallkonzepten mitwirken.

4.2. Möglichkeiten und Grenzen der Einflussnahme

Die Möglichkeiten eines IRT auf Notfallkonzepte und andere Gegenmaßnahmen einzuwirken sind weitreichend, aber nicht unbegrenzt. Wie Abbildung 9 bereits gezeigt hat, können in jeder Gruppe von Gegenmaßnahmen immer nur bestimmte Arbeiten von IRT mitwirken. Da wie in Kapitel 2 beschrieben die angebotenen Dienste der IRT so gut wie nie den gesamten Katalog an Incident Response Dienstleistungen umfassen, bietet ein bestimmtes IRT die zur Einflussnahme nötigen Dienste eventuell gar nicht an. Manche IRT betreiben zudem ausschließlich Forschung und bieten nach außen hin gar keine Dienste an. Diese IRT haben nahezu keinen Einfluss auf die Weiterentwicklung von Gegenmaßnahmen.

Die Einflussmöglichkeiten sind in der Regel auf eine bestimmte Organisation beschränkt. Innerhalb einer Organisation tritt ein Vorfall ein, dessen Bearbeitung dann das IRT nach den Vorgaben der Organisation übernimmt. Beispielsweise wird das IRT mit der Umsetzung des zuvor ausgefertigten Notfallkonzepts beauftragt. In einem solchen Fall hat das IRT

weitreichende Möglichkeiten, eben dieses Notfallkonzept zu verbessern. Allerdings ergeben sich daraus keine allgemeingültigen Regeln, da jede Organisation andere Strukturen und Werte aufweist und daher ihr ganz eigenes Notfallkonzept benötigt.

Das IRT kann zudem nur dann auf die Gegenmaßnahmen Einfluss nehmen, wenn es auch zu entsprechenden Aufgaben eingesetzt wird. Wird ein IRT beispielsweise damit beauftragt, nach dem Eindringen eines Wurms ins Netz der Organisation die einzelnen Rechner im Rahmen des Notfallkonzepts zu reinigen, so kann das IRT Einfluss auf das Notfallkonzept nehmen. Es kann beispielsweise die Reihenfolge, in der die Rechner gereinigt werden, optimieren. Oder es kann ein geeignetes Reinigungsverfahren ermitteln und durchführen, denn das Notfallkonzept hat hierzu vielleicht keine konkreten Richtlinien gegeben.
Erleidet die Firma aber beispielsweise aufgrund des Wurmangriffs einen Imageverlust, so muss dieser durch langfristige Maßnahmen wieder ausgeglichen werden, etwa durch Werbekampagnen. Auf diese Maßnahmen hat das IRT überhaupt keinen Einfluss, weil es an ihrer Planung und Umsetzung nicht beteiligt ist.

Die Möglichkeit, Gegenmaßnahmen zu beeinflussen, bietet sich einem IRT zudem nur im Rahmen seiner Zuständigkeit. Das Aufgabenfeld eines IRT ist die Reaktion auf Computervorfälle. Andere Vorfälle, wie etwa ein Feuer in einer Scheune auf einem Bauernhof, die nichts mit IT Systemen zu tun haben, überschreiten den Kompetenzbereich eines IRT. Obwohl für solche Vorfälle durchaus Notfallkonzepte benötigt werden, hat ein IRT auf diese keinerlei Einfluss.
Auf diesem Gebiet ist das Finden einer Grenze schwierig. Viele Vorfälle entstehen nicht im Zusammenhang mit IT Systemen, wirken sich aber dennoch auf die aus. Tritt in einer Firmenfiliale beispielsweise ein Feuer auf, so liegt dies eigentlich nicht im Zuständigkeitsbereich eines IRT. Betrifft der Brand jedoch das Rechenzentrum und beeinträchtigt auf diese Weise die IT Systeme (besonders ihre Sicherheit), so ist der Vorfall plötzlich doch für das IRT von Bedeutung. Ein Beispiel für einen solchen Vorfall gibt das vierte Szenario in dieser Arbeit (siehe Abschnitt 5.4.).

Inwieweit ein IRT bei einem bestimmten Vorfall in einer Organisation Einfluss auf Durchführung und Verbesserung von Notfallkonzept und anderen Gegenmaßnahmen hat, ist im Einzelfall jedoch schwer im voraus abzuschätzen, da hier viele Einzelheiten der Organisationsstruktur und des Vorfallsablaufs eine Rolle spielen. Einige Eindrücke über die Einflussmöglichkeiten geben die Szenarien in Kapitel 5.

5. Szenarien

Dieses Kapitel stellt den Hauptteil dieser Arbeit dar. In ihm werden sechs Szenarien vorgestellt, bei denen es um verschiedenartige Notfälle in einer fiktiven Organisation geht. Bei dieser Organisation handelt es sich um ein wirtschaftliches Unternehmen. Das zugrunde liegende Testnetz ist bei allen Szenarien gleich, um die Vergleichbarkeit zu sichern.
In jedem Szenario wird untersucht, ob das erstellte Notfallkonzept für den Vorfall ausreichend ist, und inwieweit die Arbeit eines IRT das Notfallkonzept verbessern kann. Gegebenenfalls werden alternative Abläufe des jeweiligen Szenarios angedacht, wenn ein anderes Notfallkonzept den Ablauf beeinflusst hätte.
Den Szenarien liegt das in Abbildung 10 dargestellte Organisationsnetz zugrunde:

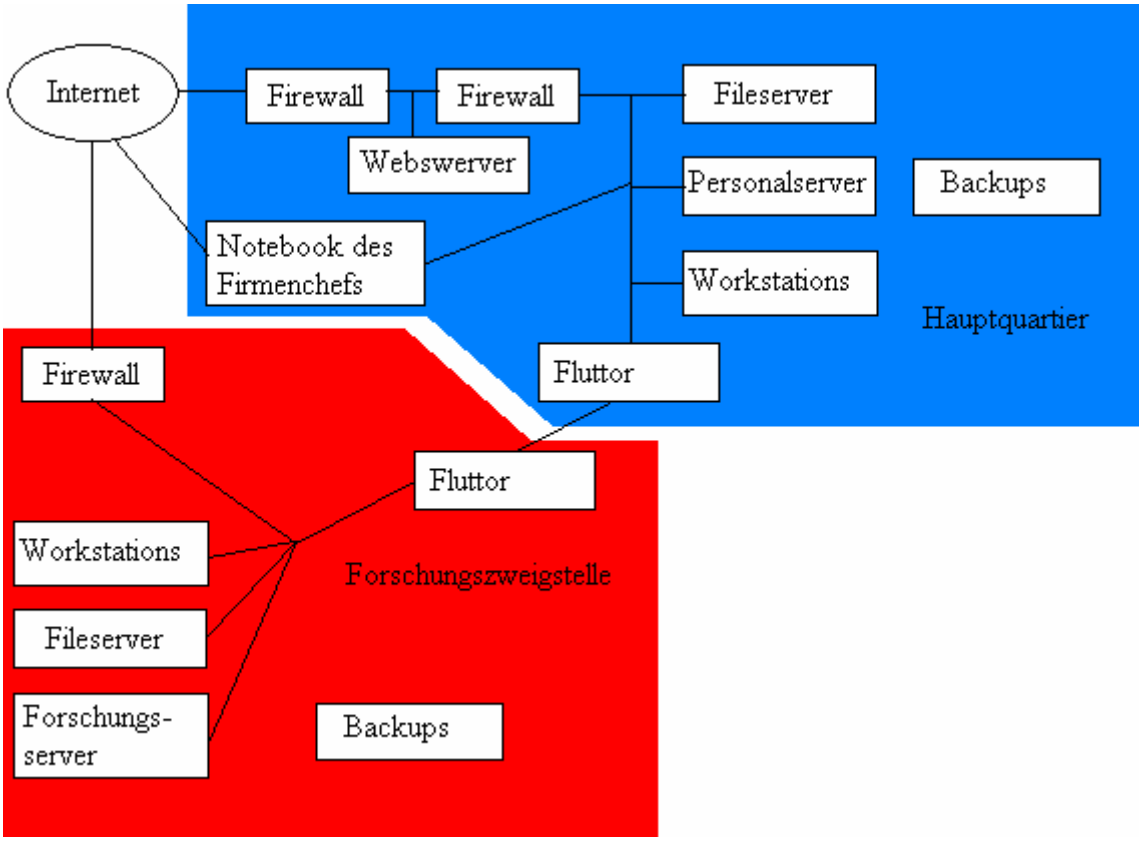


Abbildung 10: Netz der Firma in den Szenarien

Die Organisation verfügt über ein Hauptquartier (HQ) und mehrere Zweigstellen, von denen in den Szenarien nur die Forschungszweigstelle betrachtet wird. Das Hauptquartier ist über zwei Firewalls an das Internet angeschlossen. Zwischen den Firewalls befindet sich eine demilitarisierte Zone, die den Webserver der Organisation enthält. Dieser soll von beiden Seiten aus zugreifbar sein. Das interne Netz des Hauptquartiers beinhaltet einen Fileserver, auf dem die Geschäftsdaten gespeichert sind. Ein weiterer Server des Hauptquartiers ist der Personalserver mit den Mitarbeiterdaten. Zudem befinden sich im Netz die Workstations der

Mitarbeiter. Getrennt vom Netz lagern die Backups. In welchen zeitlichen Abständen sie angelegt werden und welche Daten sie enthalten, soll zwischen den Szenarien variieren. Zudem befindet sich im Hauptquartier der Firmenchef, der in einem der Szenarien mit seinem mobilen Rechner sowohl mit dem internen Netz des HQ als auch mit dem Internet verbunden ist und somit die Firewalls umgeht.
Über ein Fluttor, eine Firewall, mit der das eigene Netz in Unternetze aufgeteilt wird, ist das HQ mit der Zweigstelle verbunden. Auf der Seite der Zweigstelle befindet sich ein weiteres Fluttor, dahinter das Netz der Zweigstelle. Es enthält ebenfalls einen Fileserver und Workstations. Zusätzlich gibt es einen Forschungsserver, auf dem die Forschungsdaten hinterlegt sind. Er wird gesondert modelliert, da für ihn eine andere Sicherheitspolitik gelten kann als für den Fileserver. Über eine einzelne Firewall ist die Zweigstelle mit dem Internet verbunden.

In den sechs Szenarien werden unterschiedliche Vorfälle dargestellt. Dabei handelt es sich bei den ersten drei um Angriffe und bei den letzteren um Unfälle (siehe Kapitel 1).

- Angriff von innen: Datenschmuggel vom Forschungsserver

Bei diesem Szenario spioniert ein korrupter Mitarbeiter den Forschungsserver der Zweigstelle aus, um durch die Daten einen finanziellen Vorteil zu erlangen und die Firma zu schädigen. Da viele Angriffe auf Organisationen aus dem eigenen Netz heraus erfolgen, ist dieses Szenario von großer Bedeutung. Das Szenario gibt zudem ein Beispiel für einen Vorfall, bei dessen Bekämpfung eine Organisation mit einem Notfallkonzept alleine ohne weitere Maßnahmen nicht weit kommt.

- Angriff von außen: unbekannter Wurm

Dieses Szenario modelliert das Eindringen eines hypothetischen Wurms ins Netz der Firma. In der hier verwendeten Modellierung dringt er zunächst durch die Firewall ein und befällt das Netz nach der Behebung des Vorfalls über die unsichere Verbindung des Firmenchefs ein zweites Mal.

- Angriff von außen: Trojaner

Das dritte Szenario, das ebenfalls einen Angriff von außen beschreibt, befasst sich mit einem hypothetischen Trojaner, der ins Netz der Organisation gelangt ist und Daten ausspäht.

- Unfall: Brand im HQ Rechenzentrum

Während sich die ersten drei Szenarien mit vorsätzlichen Angriffen beschäftigt haben, modellieren die restlichen drei Szenarien zufällige Vorfälle. Im vierten Szenario geht es um einen physischen Vorfall, den Brand im Rechenzentrum.

- Unfall: Epidemie unter den Mitarbeitern

Dieses Szenario befasst sich mit einer grassierenden Krankheit unter den Mitarbeitern und untersucht, inwieweit das Sicherheitsniveau und die Produktivität durch den Ausfall des entsprechenden Personals bedroht sind. Besondere Beachtung finden mögliche Folgevorfälle, die die Firma stärker bedrohen könnten als ohne den Ausfall der Mitarbeiter.

- Unfall: Ausfall der HQ Firewalls

Im letzten Szenario soll es um den zufälligen Ausfall der Firewalls gehen und um die damit verbundene Unsicherheit bzw. die Nichtverfügbarkeit des Internetzugangs. Dabei handelt es sich um zwei getrennte Vorfälle, die eine gemeinsame Ursache haben.

Für jedes der sechs Szenarien werden einige Kenngrößen festgelegt, die die Details des modellierten Vorfalls beschreiben. Bei einigen Szenarien werden die Kenngrößen teilweise variabel gehalten, um ihren Einfluss auf den Ausgang des Vorfalls darzulegen. Folgende Kenngrößen werden verwendet:

- Bedrohte Werte

Bei jedem Vorfall werden unterschiedliche Werte bedroht, die in dieser Kenngröße festgestellt werden. Besonderes Augenmerk fällt dabei auch auf die drei Sicherheitsgrößen Vertraulichkeit, Verfügbarkeit und Integrität. Die bedrohten Werte werden im Rahmen der Szenariovorstellung erläutert.

- Systeme

Unter dieser Kenngröße sind alle relevanten Eigenschaften der Computersysteme vereinigt, wie etwa relevante Eigenschaften des Betriebssystems, bekannte und ausgenutzte Schwachstellen, usw.

- Backups

Diese Kenngröße beschreibt die Inhalte der Backups und die Zyklen, in denen sie angelegt werden. Bei Bedarf werden weitere Informationen gegeben, wie etwa Zugriffsrechte auf die Backups, die Art ihrer Lagerung etc.

- Zugriffsrechte

Mit dieser Kenngröße sind die rollenbasierten Zugriffsrechte auf die einzelnen Systeme gemeint, nicht die Abbildung der Rollen auf die Mitarbeiter. So würde dieser Punkt beispielsweise beschreiben, dass nur der Sicherheitsadministrator Zugriff auf die Konfiguration der Fluttore hat, aber nicht, dass Mitarbeiter Moritz Mustermann Sicherheitsadministrator ist.

- Mitarbeiterkompetenzen

Bei Bedarf werden in dieser Kenngröße die einzelnen Mitarbeiter vorgestellt, denen wichtige Aufgaben zugewiesen wurden. Sie umfasst außerdem Eigenschaften wie Zuverlässigkeit und Fähigkeit zur Bewältigung dieser Aufgaben.

- Sicherheitspolitik

Diese Kenngröße beschreibt auszugsweise die geltende Sicherheitspolitik für die Organisation, soweit sie für den Vorfall relevant ist. Die Sicherheitspolitik soll hier nicht vollständig modelliert werden, da die Modellierung der Organisation dafür zu grob ist und dies über den Rahmen dieser Arbeit hinausgehen würde.

- Konfiguration der Firewalls

Soweit erforderlich werden hier Details der aktuellen Filterregeln der Firewalls beschrieben. Für einige Szenarien, wie z.B. Brand, sind die Firewalls nicht relevant, dort entfällt diese Kenngröße.

- Konfiguration der Fluttore

Für diese Kenngröße gilt im Wesentlichen dasselbe wie für die Konfiguration der Firewalls. Da Fluttore und Firewalls aber im Regelfall unterschiedlich konfiguriert werden (obwohl sie auf der gleichen Software beruhen können), ist die Konfiguration der Fluttore ein eigenständiger Punkt.

- Weitere Kenngrößen

Manche Szenarien erfordern eine Modellierung weiterer Details, wie etwa Brandschutzmaßnahmen. Falls solche Details erforderlich sind, werden sie hier beschrieben.

- Bestehendes Notfallkonzept

Da der Schwerpunkt dieser Arbeit auf den Notfallkonzepten liegt, soll diese Kenngröße besonders detailliert betrachtet werden. Eventuell werden Variationen des Notfallkonzepts angegeben, um einen alternativen Szenarioverlauf aufzuzeigen.

Nach der Beschreibung der Vorgehensweise werden nun die Szenarien im Einzelnen dargestellt.

5.1. Angriff von innen: Datenschmuggel vom Forschungsserver

Das erste Szenario beschreibt einen gängigen Angriff von innen: Die Datenspionage. Um die Notwendigkeit von Vorausplanung aufzuzeigen, wurde dieses Szenario bewusst mit einer sehr gutgläubigen und fehlerbehafteten Sicherheitspolitik der Organisation modelliert. Auch der

Angreifer, der in diesem Fall aus dem eigenen Unternehmensreihen stammt, macht bei seinem Vorgehen einige Fehler, die letztlich zur Aufklärung des Vorfalls und zur Überführung des Täters führen.

5.1.1. Vorstellung des Szenarios

Ein unzufriedener Mitarbeiter der Forschungsabteilung möchte sein Gehalt aufbessern. Er hat erfahren, dass ein Konkurrenzunternehmen der Organisation bemüht ist, einen gravierenden Forschungsrückstand aufzuholen. Da die Organisation bereits einen erheblichen Vorsprung in der Erforschung eines neuen Produktes namens Mastergadget 2003 erarbeitet hat, ist der Rückstand durch eigenständige Forschung in absehbarer Zeit für den Konkurrenten nicht aufholbar. Deshalb möchte der Konkurrent gerne in den Besitz der Forschungsdaten gelangen. Der Mitarbeiter bietet dem Konkurrenten an, die Forschungsdaten zu besorgen. Dafür verlangt er eine Geldsumme, die halb so groß ist wie der Preis, zu dem die Firma ihre Forschungsdaten verkaufen würde.
Da dem Mitarbeiter ein Verschicken der Forschungsdaten über das Firmennetz als zu auffällig erscheint und der Zugriff auf den CD Brenner protokolliert wird, möchte er die Daten vom Forschungsserver auf Disketten kopieren und der Kontaktperson des Konkurrenten übergeben. Die Forschungsdaten haben einen Umfang von 12 Megabyte und sind zudem verschlüsselt. Sie lassen sich nur mit einer speziellen Software lesen, die in der Firma selber entwickelt und nicht nach außen weitergegeben wurde. Diese Software hat einen Umfang von weiteren 2 Megabyte. Der Mitarbeiter benötigt insgesamt 14 Disketten, um alle Daten vom Server zu schmuggeln.

Zu den in diesem Szenario bedrohten Werten gehören sowohl die Forschungsdaten selbst, als auch die Software, um sie auslesen zu können. Durch die Spionage des Mitarbeiters wird die Vertraulichkeit dieser Daten beeinträchtigt. Integrität und Verfügbarkeit werden nicht beeinflusst, da die Daten weder verändert noch gelöscht oder anderweitig unzugänglich gemacht werden. Diese Betrachtung der bedrohten Werte ist allerdings auf die primären Schäden begrenzt. Als sekundäre Schäden treten beispielsweise Kosten für die Entwicklung einer neuen sicheren Verschlüsselungssoftware auf, sowie Wegfall der besonderen Einnahmen, die mit der Marktersteinführung des Mastergadget 2003 erzielt worden wären. Zu den sekundären Schäden zählen zudem Imageverlust bei Bekannt werden des Vorfalls, der Verlust von Kunden sowie die damit verbundenen Gewinneinbußen.

5.1.2. Technischer Aufbau und Art des Vorfalls

Zunächst werden die genannten Kenngrößen angegeben, dann wird der genaue Ablauf des Vorfalls geschildert.

- Systeme

Für dieses Szenario ist nur das System des Forschungsservers von Belang, da die anderen Systeme nicht involviert sind. Der korrupte Mitarbeiter kopiert die Daten direkt per Diskette vom Forschungsserver, so dass kein Netzverkehr entsteht, der betrachtet werden könnte.
Zugriffe auf die Daten werden vom System protokolliert und auf einer zweiten Festplatte im System abgespeichert. Auf diese Platte hat nur ein Benutzer Zugriff, der als Chef der Forschungsabteilung angemeldet ist.
Die Daten über den Mastergadget 2003 liegen in verschlüsselter Form vor. Der Verschlüsselungsalgorithmus ist allerdings recht primitiv, da mit einem einzigen festen Schlüssel gearbeitet wird, der in der Software zum Auslesen integriert ist. Ohne den Schlüssel zu kennen bzw. die Software zu besitzen, lässt sich die Verschlüsselung aber nicht mit für die Konkurrenz vertretbarem Aufwand entschlüsseln. Die Software kann auch einen neuen Schlüssel generieren, mit dem dann alle Daten auf dem Server neu verschlüsselt werden.
Der Forschungsserver ist rund um die Uhr verfügbar. Er befindet sich in einem verschlossenen Raum, zu dem eine Person nur dann Zutritt hat, wenn sie den passenden Sicherheitsschlüssel besitzt. Einen solchen Schlüssel haben der Administrator, der Chef der Forschungsabteilung sowie dessen Stellvertreter.

- Backups

Die Backups sind für dieses Szenario nicht von Belang, da mit einem Backup keine Schäden an der Vertraulichkeit behoben werden können. Zwar könnte der Datendieb anstatt den Forschungsserver anzuzapfen auch versuchen, die Backups zu stehlen. Diese befinden sich jedoch auf einer Wechselplatte im Tresor des Forschungsleiters und ließen sich nicht mit für den Mitarbeiter vertretbarem Risiko kopieren.

- Zugriffsrechte

Das Betriebssystem des Forschungsservers ist so konfiguriert, dass es nur Mitarbeiter der Forschungsabteilung als Benutzer zulässt. Wer sich als solcher anmeldet, kann mit den Daten über den Mastergadget 2003 und der Verschlüsselungssoftware arbeiten und diese Daten auch kopieren. Allerdings hat er keinen administrativen Zugriff auf das System und kann die Zugriffsprotokolle nicht auslesen. Als Administrator angemeldete Personen dürfen das System administrieren, haben aber keinen Zugriff auf die Daten. Der Chef der Forschungsabteilung hat Zugriff auf die Daten und auf die Zugriffsprotokolle, kann das System aber nicht administrieren.

- Mitarbeiterkompetenzen

Der korrupte Mitarbeiter hat Benutzerrechte am Forschungsserver, aber keine Administratorrechte. Über die Zugriffsprotokolle wurde er zwar wie alle Mitarbeiter vom

Leiter der Forschungsabteilung informiert und hat ihnen zugestimmt, hat diese aber bei der Planung seiner Tat vergessen.
Der korrupte Mitarbeiter ist nicht im Besitz des Schlüssels für den Serverraum. Allerdings weiß er aus sorgfältigen Beobachtungen, dass der Stellvertreter des Chefs den Schlüssel vor der halbstündigen Mittagspause immer in einem unverschlossenen Fach seines Schreibtischs verwahrt.
Der Chef der Forschungsabteilung ist die einzige Person, die sich auf dem Server sowohl als Administrator als auch als Chef anmelden darf. Sein Stellvertreter kann sich nur als Benutzer anmelden. Der Sicherheitsadministrator kann sich als Administrator anmelden, tut dies für gewöhnlich aber über das Netz und nicht am physikalischen System selber.

- Sicherheitspolitik

Die Sicherheitspolitik des Forschungsservers besagt, dass alle Daten einmal am Tag mit einem neuen Schlüssel gespeichert werden müssen, was automatisch um 19.00 Uhr geschieht. Zudem ist die Tür zum Serverraum immer verschlossen zu halten, wenn sich niemand im Serverraum aufhält.
Die Protokollierung der Zugriffe wurde dem Chef der Forschungsabteilung von der Firmenleitung angeordnet, um den besonderen Wert der Daten über den Mastergadget 2003 zu unterstreichen. Diese Protokolle werden montags und donnerstags vom Chef der Forschungsabteilung durchgesehen. Sie umfassen Daten über die Person des angemeldeten Benutzers, den Zeitraum des Zugriffs und die Art der Handlung (lesen, schreiben, kopieren an ein anderes Laufwerk oder eine andere Datei usw.).
Normalerweise werden die Daten des Servers nur über das Netz abgefragt oder geändert, nur bei besonders wichtigen administrativen Aufgaben oder in Notfällen soll der Serverraum betreten werden. Zudem muss er zum Erstellen von Backups betreten werden, was einmal pro Woche vom Chef der Forschungsabteilung vorgenommen wird.
Alle Mitarbeiter der Forschungsabteilung wurden darüber belehrt, dass die Daten auf dem Server als vertraulich zu behandeln sind, und dass ihre Weitergabe rechtliche und andere Konsequenzen nach sich ziehen wird.

- Konfigurationen der Firewalls und Fluttore

Die Konfigurationen der Firewalls und Fluttore sind für dieses Szenario nicht von Belang, da keine Daten über die Netz versandt werden.

- Weitere Kenngrößen

Das Kopieren der 14 Megabyte Daten auf 14 Disketten dauert 24 Minuten. Zusammen mit dem Diebstahl des Schlüssels und dem anschließenden Zurückbringen an den Arbeitsplatz des Stellvertreters vom Chef dauert der ganze Vorfall 27 Minuten. Zudem gibt es an der Ausgangstür des Forschungsgebäudes eine Kontrollstation, an der Personen, die das Gebäude

Betreten oder Verlassen stichprobenartig daraufhin überprüft werden, ob sie Datenträger bei sich tragen. Diese Kontrolle wird durchgeführt, da das Einbringen von firmenfremden Datenträgern aufgrund der Virengefahr unerwünscht ist. Werden solche Datenträger gefunden, werden sie vor Ort auf Viren und andere Inhalte überprüft. Zudem erhält der betroffene Mitarbeiter eine Verwarnung. Bei wiederholten Verwarnungen werden die Vorfälle dem Chef der Forschungsabteilung gemeldet. Um diese Kontrolle durchführen zu können, sind alle firmeneigenen Datenträger mit einer physikalischen Markierung versehen.

Der Ablauf des Vorfalls

An einem Freitag nach der Arbeit erfolgt beim korrupten Mitarbeiter ein Anruf der Konkurrenz, in dem ihm das beschriebene Geschäft vorgeschlagen wird. Er soll die Daten auf einem Speichermedium seiner Wahl bis Mittwochmorgen beschafft haben. Bis dahin soll er sie entweder einer Kontaktperson übergeben oder sie an eine bestimmte eMail Adresse versendet haben. Am Montag fasst der korrupte Mitarbeiter den Entschluss, die Daten über den Mastergadget 2003 für die Konkurrenz auszuspionieren. Er fasst den Plan, dem Stellvertreter des Chefs den Schlüssel während dessen Mittagspause zu entwenden, dann in den Serverraum einzudringen und dort die Daten auf Disketten zu kopieren. Anschließend hofft er den Schlüssel unbemerkt wieder zurücklegen zu können, bevor der Stellvertreter etwas bemerkt.

Allerdings kennt der korrupte Mitarbeiter den Umfang der Daten nicht. Deshalb loggt er sich noch am Montag auf dem Forschungsserver ein und fragt die Größe der Daten des Mastergadget 2003 sowie der Verschlüsselungssoftware ab. Dieser Zugriff wird als normaler Lesezugriff protokolliert.

Der korrupte Mitarbeiter rechnet sich aus, dass er 14 Disketten für die Daten benötigt. Aus Erfahrung weiß er, dass der Kopiervorgang innerhalb einer halben Stunde abgeschlossen sein müsste. An seinem Arbeitsplatz hat er allerdings keinen Vorrat von 14 leeren Disketten, deshalb beschließt er, die Daten erst am nächsten Tag zu stehlen.

Zur gleichen Zeit wertet der Chef der Forschungsabteilung die protokollierten Zugriffe aus. Der als Lesevorgang vermerkte Zugriff des korrupten Mitarbeiters fällt nicht weiter auf, da pro Tag viele Lesezugriffe dieser Art von den Mitarbeitern durchgeführt werden.

Zu Hause deckt der korrupte Mitarbeiter sich mit Disketten ein. Er nimmt 16 Disketten mit, für den Fall, dass einige seiner Disketten einen Defekt haben oder die Daten wider Erwarten doch nicht auf 14 Disketten passen. Beim Betreten der Firma hat er Glück: Er wird nicht auf firmenfremde Datenträger kontrolliert, da die Kontrolle nur stichprobenartig vorgenommen wird.

In der Firma wartet er die Mittagspause des Stellvertreters ab. Als dieser zum Mittagessen in die Kantine aufbricht, nimmt der korrupte Mitarbeiter den Schlüssel aus dem Schreibtischfach. Meist geht der Stellvertreter zusammen mit den anderen Kollegen zur

Mittagspause. So auch an diesem Tag, weshalb das Entwenden des Schlüssels niemandem auffällt.
Der korrupte Mitarbeiter betritt den Serverraum und verschließt die Tür hinter sich wieder. Er beginnt mit dem Kopiervorgang, der 24 Minuten dauert. Der Kopiervorgang verläuft problemlos, und die Daten finden auf 14 Disketten Platz. Der Kopiervorgang wird in den Logfiles des Servers aufgezeichnet. Die Aufzeichnungen geben an, dass die Daten des Mastergadget 2003 sowie die Verschlüsselungssoftware von 12.03 bis 12.27 Uhr von der Festplatte an das Diskettenlaufwerk gesandt wurden.
Nach dem Kopiervorgang verlässt der korrupte Mitarbeiter umgehend den Serverraum und legt den Schlüssel zurück in den Schreibtisch des Stellvertreters. Da dieser zusammen mit seinen Kollegen die Mittagspause geringfügig überzieht, wird der korrupte Mitarbeiter auch diesmal von niemandem bemerkt.

Zu diesem Zeitpunkt fällt dem korrupten Mitarbeiter erst die Datenträgerkontrolle an der Tür wieder ein. Da er die Disketten bereits am Mittwochmorgen übergeben haben soll, muss er die Disketten unbedingt noch am Dienstag aus dem Firmengebäude herausschmuggeln. Da ihm auf die Schnelle kein anderer Plan einfällt und er langsam in Panik gerät, entschließt er sich, die Disketten in einer Plastiktüte kurz vor dem Verlassen des Gebäudes aus dem Fenster der Toilette zu werfen und sie draußen wieder einzusammeln.
Bis zum Feierabend versteckt er die Disketten in seinem Schreibtisch und führt am Abend seinen Plan durch. Er bleibt an diesem Tag etwas länger in der Firma, damit die Wahrscheinlichkeit, beim Einsammeln der Disketten beobachtet zu werden, möglichst gering ausfällt.
Allerdings vergisst er die beiden Ersatzdisketten, die er für Notfälle dabei hatte. Diese befinden sich noch immer in seiner Aktentasche, als er das Firmengebäude verlässt.
Beim Hinausgehen wird er diesmal kontrolliert. Dabei werden die beiden Disketten gefunden. Die durchgeführte Virenkontrolle ergibt jedoch korrekterweise, dass es sich um formatierte Leerdisketten handelt. Die Tatsache, dass eben dieser Mitarbeiter firmenfremde Datenträger bei sich trug, wird vermerkt. Da die Datenträger jedoch unkritisch sind, bleibt es bei einer mündlichen Verwarnung, und der Vorfall wird nicht an den Leiter der Forschungsabteilung gemeldet. Nach Verlassen des Firmengebäudes begibt er sich zu der Stelle, an der die Disketten liegen und sammelt sie wieder ein. Wie er erhofft hatte, wird er dabei nicht beobachtet.
Am Mittwochmorgen übergibt er die Disketten einer Kontaktperson des Konkurrenzunternehmens. Anschließend geht er ganz normal seiner Arbeit nach.
Am Donnerstag bei der Auswertung der Logfiles fällt dem Chef der Forschungsabteilung auf, dass die Daten auf Disketten kopiert wurden. Er spricht den korrupten Mitarbeiter daraufhin auf den Kopiervorgang an. Da der korrupte Mitarbeiter von den Logfiles nichts wusste, kommt die Frage für ihn sehr überraschend und ihm fällt auf die Schnelle keine Rechtfertigung ein, weshalb er vorerst die Auskunft verweigert. Der Chef der

Forschungsabteilung leitet daraufhin eine Untersuchung ein, in die auch ein IRT einbezogen wird...

5.1.3. Bestehendes Notfallkonzept

Der Knackpunkt bei einem herkömmlichen Notfallkonzept für einen Vorfall der Datenspionage, wie er hier vorliegt besteht darin, dass die Hauptaufgabe eines Notfallkonzepts, die schnelle Wiederherstellung der Verfügbarkeit, gar nicht erfüllt werden muss. Die ausspionierten Daten sind weiterhin verfügbar, nur wurde ihr Wert durch den Vertraulichkeitsverlust reduziert. Es bliebe noch die Aufgabe, den Notfall unmittelbar zu beenden bzw. zu bekämpfen und die Schäden durch Recovery und ähnliche Maßnahmen zu beseitigen (vgl. Kapitel 1). Im vorliegenden Vorfall greifen auch solche Maßnahmen nicht, denn der Vorfall ist zum Zeitpunkt der Entdeckung bereits abgeschlossen, wodurch eine unmittelbare Bekämpfung nicht mehr möglich ist. Den Schaden durch Sofortmaßnahmen zu mindern oder aufzuheben ist ebenfalls unmöglich, da die Daten sich nicht einfach der Konkurrenz wieder wegnehmen lassen.
Aus den klassischen Inhalten eines Notfallkonzeptes bleiben somit nur die infrastrukturellen Maßnahmen, wie etwa die Etablierung einer Kommunikationsstruktur und die Festlegung von Verantwortlichkeiten. Durch eine solche Struktur für den Notfall kann immerhin schnell mit der Spuren- und Beweissicherung begonnen werden, wodurch sich die langfristige Vorfallsbearbeitung einfacher gestaltet.

Aufgrund dieser Überlegungen und den Gegebenheiten im Szenario lässt sich nun ableiten, welche Inhalte das Notfallkonzept zur internen Datenspionage zum Zeitpunkt des Vorfalls hatte. Wie sich zeigen wird, enthält das Notfallkonzept in diesem Fall nur sehr wenige Maßnahmen, wenn das Notfallkonzept im klassischen Sinne verstanden wird.
Da das Szenario so modelliert war, dass die Firma eine relativ löchrige Sicherheitspolitik hatte, wird auch das bestehende Notfallkonzept in dieser Weise modelliert. Das Notfallkonzept der Organisation erwächst aus den Kontrollmaßnahmen, die in der Sicherheitspolitik festgelegt sind. Wurde ein Notfall entdeckt, etwa an der Türkontrolle (wenn sich auf den Datenträgern zwar keine Viren, aber vertrauliche Daten befinden) oder beim Durchsehen der Logfiles, läuft das Konzept an. Es soll vorsehen, dass der Notfall zunächst dem Chef der Forschungsabteilung gemeldet wird. Anhand der Logfiles soll dieser dann ermitteln, wer als möglicher Spion in Frage kommt und wie der Täter vorgegangen sein könnte. Wichtigstes Ziel hierbei ist die Feststellung, ob der Spion vertrauliche Daten an Dritte weitergeben hat und ob und wie der Schaden behoben werden kann. Vor allem rechtliche Schritte sollen geprüft werden. Hier sei angemerkt, dass sich mit rein informatischen Methoden nur das Kopieren der Daten vom Server belegen lässt, nicht aber die Weitergabe an Dritte. Hierzu sind Ermittlungen im weiteren Umfeld des Mitarbeiters nötig.
Es fällt auf, dass diese Maßnahmen genau genommen schon nicht mehr in ein Notfallkonzept gehören, da sie nicht den Charakter von Sofortmaßnahmen haben. Zu unterscheiden sind die

Maßnahmen selbst und ihre Vorbereitung. So gehört die rasche Beweissicherung zum Notfallkonzept, die rechtliche Verfolgung des Vorfalls jedoch nicht.
Streng genommen wären die Maßnahmen des Notfallkonzeptes jetzt also bereits erschöpft. Der Vorfall der Datenspionage lässt sich besser mit Präventivmaßnahmen und langfristigen Maßnahmen (Rechtsverfolgung usw.) behandeln als mit einem herkömmlichen Notfallkonzept. Die Präventivmaßnahmen wurden im Rahmen der Szenariobeschreibung bereits geschildert, die langfristigen Maßnahmen zur Aufklärung des Vorfalls gehören zur Arbeit eines IRT.
Um die Möglichkeiten zur Verbesserung der Vorfallsbekämpfungsmaßnahmen im weiteren Sinne als nur im hier sehr engen Rahmen eines herkömmlichen Notfallkonzeptes durch ein IRT aufzuzeigen, sollen in diesem Szenario auch die Präventivmaßnahmen betrachtet werden. Durch die im nächsten Abschnitt geschilderten Arbeiten des IRTs erwachsen Hinweise für bessere Präventivmaßnahmen, ebenso wie bessere Inhalte für das Notfallkonzept.

5.1.4. Arbeit und Ergebnisse des IRTs

Dieser Abschnitt orientiert sich an den Dienstleistungen von IRTs, die in Kapitel 3 beschrieben wurden. Er zeigt auf, welche Arbeiten das IRT im vorliegenden Szenario leisten kann.

- Incident Analysis

Zunächst muss das IRT überprüfen, ob sich überhaupt ein Sicherheitsvorfall ereignet hat. Bekannt ist bislang ja nur, dass die Daten des Mastergadget 2003 vom Server herunterkopiert wurden. Dies ist laut Sicherheitspolitik nicht grundsätzlich verboten, da es für die Back-Ups notwendig ist. Allerdings ist das Kopieren auf Disketten ungewöhnlich genug, um einen Sicherheitsvorfall mit Verlust der Vertraulichkeit anzunehmen. Um festzustellen, ob sich ein solcher Vorfall ereignet hat, greift das IRT in diesem Szenario vor allem auf die Spuren zurück, die der korrupte Mitarbeiter hinterlassen hat. Zunächst ist es wichtig, dass dem IRT die Logfiles des Servers zugänglich gemacht werden. Daraus kann es ableiten, dass die Daten des Mastergadget 2003 und des Verschlüsselungsprogramms vom korrupten Mitarbeiter auf Disketten kopiert wurden. Auch damit liegt noch kein Verlust an Vertraulichkeit gemäß der Sicherheitspolitik vor, denn der Mitarbeiter hatte das Recht, die Daten zu lesen, und auch das Kopieren auf Disketten an sich war nicht verboten, sondern lediglich das Betreten des Serverraums.
Ein Verlust an Vertraulichkeit liegt in diesem Fall beispielsweise dann vor, wenn die Disketten mit den Daten das Firmengebäude verlassen. Wenn das IRT Untersuchungen in dieser Richtung anstellt, wird es schnell feststellen, dass sich die Disketten nicht mehr im Firmengebäude auffinden lassen. Hinzu kommt die Aussage der Torwache, dass der Mitarbeiter das Gebäude mit firmenfremden Disketten verlassen hat. Ab diesem Moment ist klar, dass ein Sicherheitsvorfall mit Verlust der Vertraulichkeit vorliegt.

Der zweite Schritt ist die genaue Analyse des Vorfallhergangs. Hierzu muss das IRT die Organisationsstruktur der Forschungsabteilung untersuchen. Der Mitarbeiter hatte illegitimen, physikalischen Zugang zum Serverraum, somit muss er einen Schlüssel für die Tür besessen haben. Da sowohl der Chef der Forschungsabteilung als auch der Administrator ihre Schlüssel die ganze Zeit bei sich trugen, kann es nur der Schlüssel des Stellvertreters gewesen sein. Hier zeigt die Analyse bereits eine zu verbessernde Schwachstelle auf: Der Schlüssel ist für Mitarbeiter zugänglich, für die er nicht zugänglich sein sollte. Bereits ein solch einfaches Beispiel zeigt, wie vielschichtig und verflochten die Erkenntnisse aus einer Vorfallsanalyse sein können. Bleibt noch die Frage, wie die Disketten das Gebäude der Firma verlassen haben und wohin sie gelangt sind. Da der Mitarbeiter diesbezüglich keine Spuren hinterlassen hat, können diese Fragen nur durch Auskunft des Mitarbeiters oder eventuell durch Spurensicherung in seinem Umfeld (z.B. Aufzeichnungen der Gespräche mit der Kontaktperson) beantwortet werden. Nehmen wir für das Szenario an, dass der Mitarbeiter unkooperativ ist und zu diesen Fragen schweigt. Dann kann der Vorfallsverlaufs nicht oder nur schwer aufgeklärt werden.
Eine weitere wichtige Größe, die ermittelt werden muss, ist die zeitliche Ausdehnung des Vorfalls. Diese lässt sich aus den Logfiles leicht ermitteln, da der Zeitpunkt des Zugriffs mitprotokolliert wird.
Was nicht zur Vorfallsanalyse im engeren Sinne gehört ist die Feststellung, welche Person den Vorfall verursacht hat und wer unerlaubter Weise Kenntnis von den vertraulichen Daten gewonnen hat. Diese Informationen gehören in den Bereich der rechtlichen Schritte.

- Reinigung

Cleaningmaßnahmen sind in diesem Szenario nicht erforderlich. Es wurden keine Daten geändert, gelöscht oder hinzugefügt, sondern lediglich gelesen und kopiert. Dennoch ist dies eine Erkenntnis, die das IRT zunächst aus der Vorfallsanalyse gewinnen muss. Ist diese bis zum oben beschriebenen Punkt abgeschlossen, steht für das IRT fest, dass auf Cleaning verzichtet werden kann.

- Vermeidung

Natürlich kann der Vorfall durch Vermeidungsmaßnahmen nicht mehr verhindert werden, da er bereits eingetreten ist. Deshalb soll sich dieser Punkt nicht mit Vermeidung an sich beschäftigen, sondern mit der Suche des IRTs nach zukünftigen Vermeidungsmaßnahmen, um weitere Vorfälle der Datenspionage zu verhindern.
Ein guter Ansatz ist grundsätzlich wie in diesem Szenario im Besonderen das Überprüfen der Sicherheitspolitik. Diese legt erst das gewünschte Sicherheitsniveau fest, das dann später in konkreten Maßnahmen durchgesetzt werden soll. In diesem Szenario haben die Sicherheitspolitik und ihre praktische Umsetzung einige markante Schwächen. Der wichtigste Punkt besteht darin, dass das Prinzip des generellen Verbots nicht beachtet wurde. Dieses

sieht vor, dass ein Benutzer eines Systems immer nur die minimalen Rechte hat, die er zum Erledigen seiner Aufgaben benötigt. So ist es zum Beispiel für keinen Mitarbeiter der Forschungsabteilung für seine Arbeit notwendig, Daten vom Server auf Disketten zu kopieren oder sich überhaupt am Server direkt, d.h. nicht über das Netz, einzuloggen. In einer Sicherheitspolitik mit dem Prinzip des generellen Verbotes wäre das Kopieren der Daten auf Diskette ebenso wie das direkte Einloggen somit verboten, und als Folge daraus müsste der Server nicht einmal ein Diskettenlaufwerk haben. Ein Beispiel für schlechte Umsetzung der Sicherheitspolitik bietet die Verteilung der Schlüssel. Zwar gibt es nur drei Schlüssel zum Serverraum, der damit zugangsbeschränkt ist, aber die Sicherheitspolitik wurde vom Stellvertreter des Chefs schlecht umgesetzt, sodass der korrupte Mitarbeiter sie durch Diebstahl des Schlüssels umgehen konnte. Ähnliches gilt für die Verschlüsselungssoftware. Sie war nur für die Arbeit innerhalb der Firma gedacht und sollte den Zugriff von Dritten auf die Daten des Mastergadget 2003 schützen. Aber da das Kopieren der Software samt Schlüssel problemlos möglich war, konnte die Sicherheitspolitik an dieser Stelle umgangen werden.
Der zweite wichtige Aspekt bei jeder Sicherheitspolitik besagt, dass die Sicherheitspolitik in der gesamten Organisation in vollem Umfang bekannt sein sollte. Dies umfasst auch die Art der Durchsetzung und eventuelle Sanktionen bei Verstößen. Der Verstoß gegen diesen Grundsatz zeigt sich im Szenario bei den Logfiles. Hätte der korrupte Mitarbeiter von ihnen gewusst, wäre es vermutlich nicht zum Vorfall gekommen.
Aus der Analyse der Sicherheitspolitik kann das IRT Maßnahmen ableiten, wie diese verbessert werden kann. Gleiches gilt für ihre Umsetzung in der Praxis. Aus beidem resultiert eine Vermeidung der Wiederholung des Vorfalls.
Zudem können Maßnahmen zur Vorfallsvermeidung durch eine Verbesserung der eingesetzten Technik erzielt werden. So könnte das einfache Türschloss am Serverraum beispielsweise durch eine Kombination mehrerer (teilweise elektronischer) Zugangskontrollmechanismen ersetzt werden, die eher als ein Schlüssel gewährleisten, dass nur die drei gewünschten Personen den Serverraum betreten.

- Gegenwehr

Maßnahmen zur Gegenwehr sind in diesem Szenario nur sehr begrenzt wirksam, da der Vorfall nicht mehr andauert. Wie beim Cleaning muss diese Tatsache allerdings zunächst festgestellt werden. Hier folgt sie aber unmittelbar aus der Vorfallsanalyse.
Wenn auch der Vorfall selbst abgeschlossen ist, so bleiben seine Folgen in Form einer Vertraulichkeitsverletzung dennoch bestehen, und diese ließen sich bekämpfen. Allerdings ist dafür nicht das IRT zuständig. Beispielsweise könnte die Firma den Mastergadget 2003 zum Patent anmelden und damit ihre Rechte gegenüber der Konkurrenz sichern.

- Rechtliche Schritte

Bei einem Vorfall der Datenspionage liegt ein großes Augenmerk auf der Rechtsverfolgung, denn ein Vertraulichkeitsschaden lässt sich nur durch rechtliche Sanktionen (z.B. Schadensersatz in Geld) einigermaßen wieder beheben, da Cleaning, Recovery usw. aus den angeführten Gründen zu keinem Ergebnis führen.
Analog zum in Kapitel 3 aufgezeigten Weg der Rechtsverfolgung muss das IRT zunächst den Weg des Angreifers feststellen. Dies ist in unserem Szenario kein Problem, da er größtenteils aus der Vorfallsanalyse folgt. Es ist bekannt, dass der Angriff aus der Firma selber erfolgt ist, und dass die Daten des Mastergadget 2003 auf Disketten kopiert wurden. Außerdem hat der korrupte Mitarbeiter am selben Tag unerlaubte Disketten bei sich gehabt. Es lässt sich somit die Vermutung anstellen, dass die Daten entweder auf Disketten aus dem Gebäude geschmuggelt wurden, oder sich noch auf Disketten im Gebäude befinden. Aus der Vorfallsanalyse ist allerdings bekannt, dass sich die Disketten nicht mehr im Gebäude befinden. Somit müssen sie aus dem Gebäude geschmuggelt worden sein. Unbekannt ist allerdings, wohin die Daten danach weitergegeben wurden. Da der Mitarbeiter zu dieser Frage keine Angaben macht, kann sie nur eventuell durch Spurensicherung im Umfeld des Mitarbeiters beantwortet werden. Für dieses Szenario wird angenommen, dass der Mitarbeiter Name und Adresse seiner Kontaktperson auf einem Zettel in seiner Wohnung verwahrt. Dann kann der Weg des Angreifers lückenfrei nachverfolgt werden.
Die zweite Frage ist die der Identität des Angreifers. Naheliegenderweise wird hier der korrupte Mitarbeiter die Rolle des Angreifers zugewiesen bekommen, denkbar wäre aber auch, den Konkurrenten juristisch, nicht informatisch, als Angreifer anzusehen. Dies ist besonders für die Frage wichtig, welche Person später zur Rechenschaft gezogen werden soll.
Als nächstes folgt die Spurensicherung beim Angreifer. Da der korrupte Mitarbeiter Namen und Adresse der Kontaktperson zu Hause aufbewahrt hat, können seine Hintermänner schnell ermittelt werden, woraus sich ergibt, welcher Konkurrent nun im Besitz der vertraulichen Daten ist. Dies ist wiederum von Bedeutung für die Schadensermittlung. Bei der zivilrechtlichen Verfolgung sind im Wesentlichen die einklagbaren Schäden von Belang, denn diese können im Rahmen des Schadensersatzes wieder gutgemacht werden. Andere, nicht ersetzbare Schäden (z.B. Imageverlust), können dagegen strafrechtlich relevant sein. Die genaue Schadensermittlung würde an dieser Stelle zu weit führen, sie lässt sich aus den geschilderten bedrohten Werten ableiten. Auch die Ermittlung einschlägiger Gesetze und die Erhebung der Anklage sollen hier nicht weiter vertieft werden.

5.1.5. Einfluss auf die Weiterentwicklung des Notfallkonzeptes

Wie geschildert kommt die Organisation mit einem herkömmlichen Notfallkonzept in diesem Szenario nicht sehr weit. Besser ist es, Vorfälle dieser Art durch Präventivmaßnahmen zu verhindern. Welcher Art diese Maßnahmen sein können, hat die Arbeit des IRTs aufgezeigt.
So ist beispielsweise die Erstellung einer verbesserten Sicherheitspolitik angezeigt, wobei die Prinzipien des generellen Verbots und der Kommunikation der Sicherheitspolitik in der

Organisation beachtet werden müssen. Ferner müssen Fehler bei der Umsetzung der Sicherheitspolitik wie etwa das Zugänglichmachen des Schlüssels zum Serverraum unterbunden und regelmäßig zum Beispiel durch Schreibtischinspektionen, wie sie in Großunternehmen durch die Beauftragten für Datenschutz und Informationssicherheit üblich sind, kontrolliert werden.
Das Notfallkonzept selber umfasste in unserem Szenario nur Maßnahmen organisatorischer Art, um die Vorfallsbekämpfung schnell einzuleiten. In der Praxis eines Vorfalls bieten sich Erkenntnisse, wie diese organisatorischen Maßnahmen noch verbessert werden können. Sie wurden im Szenario nicht konkret modelliert, spielen aber in der Praxis eine Rolle.

5.1.6. Fazit

Aus diesem Szenario lässt sich vor allem die Erkenntnis ableiten, dass ein Notfallkonzept alleine bei vielen Vorfällen unzureichend ist. Ferner müssen die Präventivmaßnahmen und die Sicherheitspolitik gut entwickelt sein, um Vorfälle der Datenspionage, die von korrupten Mitarbeitern ausgeführt werden, zu unterbinden.
Die Arbeit des IRTs hat in diesem Szenario kaum Einfluss auf das ohnehin nur rudimentäre Notfallkonzept gehabt. Dennoch hat seine Arbeit Möglichkeiten aufgezeigt, ähnliche Vorfälle in Zukunft zu unterbinden, die Schäden abzumildern oder die Aufklärungsmöglichkeiten zu verbessern.

5.2. Angriff von außen: unbekannter Wurm

Das zweite Szenario modelliert einen Vorfall aus einer Klasse, die in jüngerer Zeit an Bedeutung gewonnen hat. Ständig geraten neue Würmer in den Umlauf und dringen auch in Firmennetze ein. Zwar können die meisten Würmer bereits nach relativ kurzer Zeit wieder entfernt werden, doch bis dahin sind häufig schon beachtliche Schäden angerichtet.

5.2.1. Vorstellung des Szenarios

In diesem Szenario dingt ein bislang unbekannter Wurm plötzlich ins Netz der Organisation ein. Der Vorfall überrascht die Organisation vollkommen, da sich die Organisation auf die Sicherheit ihrer Firewalls verlassen hatte. Dennoch verbreitet sich der Wurm im Netz des Hauptquartiers und blockiert die Rechner und Netzleitungen. Zum Glück scheinen die Fluttore zu den Zweigstellen jedoch zu halten, denn die Ausbreitung des Wurms bleibt auf das Netz des Hauptquartiers beschränkt.
Während in der Organisation nach einem Gegenmittel gesucht wird, macht sich die Schadfunktion des Wurms bemerkbar: eine Stunde nach der Infektion eines Rechners werden nach einem Zufallsprinzip Daten auf den Rechnern durch den Wurm gelöscht, wodurch weiterer Schaden entsteht. Mit einem herunter geladenen Tool der Anti-Malware Industrie und einem Update des Virenscanners auf den Firewallrechnern kann der Wurm zwar entfernt und die Firewall angepasst werden, dennoch dringt er aber immer wieder neu ins Netz ein.

Erst als herausgefunden wird, dass der Wurm über das Notebook des Firmenchefs ins Netz eindringt, kann das Netz nach außen hin gegen den Wurm versiegelt werden.

In diesem Szenario sind im wesentlichen zwei Werte bedroht: Die Systemressourcen und die gespeicherten Daten. Die Ressourcen werden durch den Wurm beansprucht, und die Daten werden wahllos gelöscht. In beiden Fällen handelt es sich also um Verfügbarkeitsschaden, außerdem beeinträchtigt der Wurm natürlich die Integrität der Systeme, indem er sich in ihnen installiert, damit ihren Zustand unerlaubt verändert und auch Systemdaten löscht.
Hinzu kommen auch hier sekundäre Schäden. Bei Vorfällen mit Würmern ist oft ein großer Imageverlust zu vermelden, zudem erleidet die Organisation durch die Nichtverfügbarkeit des Netzes auch Umsatzeinbrüche.

5.2.2. Technischer Aufbau und Art des Vorfalls

Zunächst folgen die Kenngrößen, dann der Ablauf des Vorfalls.

- Systeme

Für diesen Vorfall soll ein homogenes Netz angenommen werden. Alle Rechner im Netz haben das gleiche Betriebssystem und im Wesentlichen die gleiche Hardware. Der Personalserver und der Fileserver heben sich nur durch mehr Speicherplatz auf der Festplatte von den Workstations ab. Zudem ist auf ihnen eine Serversoftware installiert, die die Serverfunktionalität ermöglicht. Beide Server verfügen außerdem über einen CD Brenner, mit dem die Backups erstellt werden.
Die Workstations sind absolut baugleich. Auch die installierte Software unterscheidet sich zwischen den Workstations nicht in relevanter Weise.
Das Betriebssystem der Rechner habe eine ungepatchte Schwachstelle, die als 08/15-vulnerability bekannt ist und die von einem neuen, bislang unbekannten Wurm ausgenutzt wird. Die Schwachstelle selber ist schon seit einiger Zeit bekannt, und der Hersteller des Betriebssystems hat auch einen Patch dagegen bereitgestellt.
Das Notebook des Firmenchefs unterscheidet sich nicht wesentlich von den Systemen im Netz. Es hat dasselbe Betriebssystem, auf dem der Wurm sich einnisten kann.
Der Wurm verschickt sich als Anlage in eMails und kann sich auf diese Weise im Netz des Hauptquartiers ausbreiten. Auch der Firmenchef versendet über eine drahtlose Verbindung regelmäßig eMails ins Hauptquartier, und der Wurm kann auch diese Verbindung nutzen.
Auf dem Notebook des Firmenchefs ist keine Firewall installiert und auch kein Malwarescanner. Deshalb kann der Wurm die Passage über das Notebook ungefiltert nutzen.

- Backups

Die Daten des Fileservers und des Personalservers werden einmal am Tag um 20.00 Uhr in einem Backup gesichert. Hierzu werden die Daten automatisch auf CD gebrannt. Anschließend werden die CDs vom Administrator entnommen und in einem gesonderten Tresor aufbewahrt. Dieser enthält die Backups der letzten zwei Wochen.
Bei den Backups handelt sich nicht um komplette Images der Serversysteme. Sie enthalten nur die Daten, die auf den Servern gespeichert werden. Zum Einspielen der Backups werden die vorhandenen Daten auf dem Server mit den Daten aus dem Backup überschrieben.
Von den Workstations werden keine Backups angelegt, da alle Mitarbeiter ihre wichtigen Daten auf dem Fileserver abspeichern sollen. Die lokalen Platten der Workstations dienen nur zum kurzfristigen Zwischenspeichern.

- Zugriffsrechte

Der Personalserver steht im Büro in der Personalabteilung, der Fileserver zusammen mit den Workstations im Rechenzentrum des Hauptquartiers. Der Fileserver hat keine Zugangsbeschränkung, da alle Mitarbeiter auf seine Daten zugreifen können und müssen. Dabei hat jeder Mitarbeiter ein eigenes Verzeichnis auf dem Server, das mit einem Passwort gegen unerlaubtes Lesen, Schreiben, Ausführen und Löschen geschützt ist. Zudem gibt es ein öffentliches Verzeichnis, das jeder Mitarbeiter lesen kann. Der Passwortschutz des Serversystems kann jedoch vom Wurm umgangen werden, da dieser sich auf dem System über die 08/15-vulnerability vollständige Zugriffsrechte auf alle Verzeichnisse geben kann.
Der Personalserver hat nur ein einzelnes Datenverzeichnis, das die Personaldaten enthält. Es ist ebenfalls passwortgeschützt und verfügt auch über die 08/15-vulnerability. Zudem wird er von einer Personalsachbearbeiterin auch als Workstation genutzt. Beide Server sind nicht physikalisch geschützt.
Die Firewalls und das Fluttor können nur vom Sicherheitsadministrator bedient werden, zudem sind sie nicht über das Netz administrierbar. Vielmehr muss sich der Sicherheitsadministrator am Rechner selber einloggen, um an der Firewall zu arbeiten.
Die Workstations haben Zugänge für den jeweiligen Mitarbeiter und den Administrator.

- Mitarbeiterkompetenzen

Der einzige Mitarbeiter, der zu allen Verzeichnissen und Rechnern unbegrenzten Zugang hat, ist der Firmenchef. Er kann sich auf allen Rechnern mit kompletten Zugriffsrechten anmelden. Zugriff zum Personalserver hat ansonsten lediglich die Personalsachbearbeiterinnen. Zu den Firewalls und dem Fluttor hat der Netzadministrator des Hauptquartiers Zugriff, der neben der normalen Administration auch die Sicherheitsadministration wahrnimmt. Er führt außerdem das Sichern der Backups durch.
Zu den einzelnen Workstations hat immer der jeweilige Mitarbeiter Zugriff. Zudem kann der Administrator über ein Administratorpasswort ebenfalls Zugang erlangen. Dabei sind die

Daten auf der Workstation für ihn ebenfalls zugänglich, da auf den Workstations keine wichtigen Daten gespeichert werden sollen, und diese somit nicht als besonders schützenswert angesehen werden.

- Sicherheitspolitik

Die Sicherheitspolitik ordnet an, dass die Daten auf den beiden Servern ständig verfügbar und integer zu halten sind. Dies soll mit Firewallschutz und den Backups umgesetzt werden. Die Daten sind außerdem vertraulich zu halten, was für dieses Szenario aber nicht modelliert werden muss, da der Wurm lediglich Verfügbarkeits- und Integritätsschaden anrichtet.
Jeder Mitarbeiter soll wichtige Daten auf dem Fileserver abspeichern, wo sie besonders geschützt sind (durch den erwähnten Passwortschutz). Um die Verfügbarkeit der Daten und Ressourcen zu gewährleisten, soll die Leitung über die beiden Firewalls als einziger Zugangspunkt zum Netz dienen (single point of access). Die Überbrückung des single point of access durch den Rechner der Firmenleitung stellt somit eine Verletzung der Sicherheitspolitik dar.
Die Sicherheitspolitik ist in der gesamten Organisation bekannt gemacht.

- Konfiguration der Firewalls

Die Firewalls arbeiten mit Erlaubnisregeln. Somit wird nur Netzverkehr durchgelassen, der gemäß einer Filterregel erlaubt ist. Alles, was nicht von einer Erlaubnisregel abgedeckt wird, wird von der Firewall geblockt. Die äußere Firewall erlaubt dabei mehr Netzverkehr als die innere, damit der Webserver von außen zugänglich ist.
Beide Firewalls erlauben Mailverkehr in beide Richtungen. MailAnlagen werden durch einen Virenscanner überprüft. Der Scanner hat jedoch noch keine Signatur des Wurms, da dieser noch ganz neu ist. Zunächst lässt die Firewall den Wurm somit hindurch, allerdings kann dies später durch ein Signaturupdate geändert werden.

- Konfiguration der Fluttore

Das Fluttor des Hauptquartiers ist ebenfalls anhand von Erlaubnisregeln konfiguriert. Seine Konfiguration gleicht der der Firewalls, erlaubt allerdings kein Websurfen. Auch das Fluttor erlaubt Mailverkehr über einen Virenscanner, der ebenfalls noch nicht über eine Signatur des Wurms verfügt.

- Weitere Kenngrößen

Der Wurm verbreitet sich über eMai, und zwar per Anlage. Die Anlage muss manuell geöffnet werden. Danach infiziert der Wurm das System, sofern es über die 08/15-vulnerability verfügt. Unmittelbar nach der Infektion verschickt der Wurm sich an alle Einträge des Adressbuchs über eine eMail mit variablem Inhalt, aber immer mit einer Anlage,

das den Wurm enthält. Eine Stunde nach der Infektion wählt ein Zufallsgenerator 80% der Dateien auf dem System aus und löscht sie.
Von jedem System aus verschickt der Wurm sich nur ein einziges Mal weiter, da er das System anschließend mit großer Wahrscheinlichkeit zerstört.
Die Organisation befindet sich gerade in einem Prozess der Systemaktualisierung. Alle Rechner der Firma werden auf eine neue Version des Betriebssystems umgestellt. In den Zweigstellen ist diese Umstellung bereits abgeschlossen, im Hauptquartier allerdings noch nicht. Die neue Version des Betriebssystems verfügt nicht mehr über die 08/15-vulnerability.

Nach der Darlegung der Kenngrößen folgt nun der Ablauf des Vorfalls im Szenario.
An einem Mittwochmorgen um 9.35 Uhr erhält ein Mitarbeiter des Hauptquartiers eine eMail. In dieser Mail wird der Mitarbeiter darüber informiert, die beigefügte Anlage würde die Prozessorleistung seines Systems um 35% erhöhen. Da der Mitarbeiter seinen Rechner für viel zu langsam hält, öffnet er die Anlage und infiziert sein System unbewusst mit einem neuen Wurm. Auch einige andere Mitarbeiter der Organisation erhalten etwa zeitgleich eine eMail mit derselben Anlage. Einige von ihnen öffnen es und infizieren damit ihre Systeme ebenfalls.
Kurz darauf beginnen die Wurminstanzen in den einzelnen Systemen, an alle Einträge in den Adressbüchern Wurmkopien zu verschicken. Dadurch wird das Netz des Hauptquartiers stark belastet, was einzelnen Mitarbeitern auffällt, als sie mit dem Fileserver kommunizieren wollen. Sie alarmieren den Administrator. Da dieser aufgrund der seiner Meinung nach sicheren Firewalls nicht auf die Idee kommt, dass sich ein Wurm im Netz befinden könnte, untersucht er den Fileserver. In der Zwischenzeit öffnen weitere Mitarbeiter die Anlagen und infizieren ihre Systeme.
Irgendwann erhält auch die Personalsachbearbeiterin eine eMail mit dem Wurm. Da ihr Büro sehr klein ist, arbeitet sie direkt am Personalserver, den sie nebenbei auch als Workstation nutzt. Sie öffnet die Anlage und infiziert so den Personalserver mit dem Wurm.
Der Administrator kann am Fileserver keinen Fehler feststellen. Er kehrt zu seinem Arbeitsplatz zurück und stellt fest, dass er in der Zwischenzeit zahlreiche seiner Meinung nach unsinnige Mails mit Anlagen erhalten hat. Jetzt kommt ihm der Verdacht, dass es sich um einen Wurm handeln könnte. Umgehend informiert er die Mitarbeiter darüber, vorerst keine Mails mit Anlagen mehr zu öffnen, da viele Würmer sich über Mailanlagen verbreiten. Er beauftragt ein IRT mit der weiteren Untersuchung.
Das IRT sucht auf den Internetseiten der anderen IRTs und der Anti-Malware Industrie nach Informationen über neue Würmer. Nach einiger Zeit wird es fündig und lädt sowohl eine neue Signatur für den Malwarescanner sowie ein Tool herunter, mit dem der Wurm entfernt werden kann. Leider macht sich in der Zwischenzeit die Payload des Wurms bemerkbar. Zahlreiche Workstations sind unbrauchbar gemacht, und auch der Personalserver wurde zerstört. Der Fileserver allerdings scheint nicht infiziert zu sein. Nach einem Studium der Informationen über den Wurm erkennt das IRT den Grund dafür: Der Wurm verbreitet sich

nur über Mail, und der Fileserver ist nicht per Mail erreichbar. Auch die Zweigstellen der Organisation scheinen vom Wurm nicht betroffen zu sein. Der Administrator schiebt diesen Glücksfall zunächst auf die Fluttore, dann erkennen er und das IRT aber, dass die Zweigstellen aus einem anderen Grund verschont geblieben sind: Die neue Version des Betriebssystems ist gegen den Wurm nicht mehr anfällig.
Gemäß dem Notfallkonzept wird das Netz des Hauptquartiers vom Internet und von den Netzen der Zweigstellen abgeschottet, indem die Verbindungen über Firewalls und Fluttore getrennt werden. Allerdings bleibt die unsichere Verbindung über den Rechner des Chefs bestehen, wovon der Administrator nichts weiß. Anschließend installiert der Administrator auf den Firewalls und dem Fluttor die Signatur des neuen Wurms. Das Tool, um den Wurm zu entfernen, kommt allerdings zu spät, da die meisten Rechner bereits zerstört sind. Das Notfallkonzept sieht vor, zunächst den Angriff zu beenden. Alle Workstations werden auf den Wurm gescannt und soweit noch möglich gesäubert. Als der Wurm aus dem Netz verschwunden ist, wird mit dem Wiederaufbau begonnen. Zunächst wird das System des Personalservers neu installiert, und die Daten werden vom letzten Backup eingespielt. Anschließend werden die Workstations wiederhergestellt, wobei nun auch der Patch gegen die 08/15-vulnerability installiert wird.
Noch während dieser Arbeiten tauchen überraschend neue Wurmkopien im Netz auf. Da die meisten Systeme mittlerweile gepatcht und die Mitarbeiter informiert sind, entsteht kein neuer Schaden. Dennoch muss sich irgendwo noch eine Sicherheitslücke befinden.
Erst nach einer umfangreichen Suche stellt sich heraus, dass die neuen Wurmkopien über die Workstation des Chefs eingedrungen sind. Der Chef wird auf seiner Dienstreise angerufen und ebenfalls gebeten, bis auf weiteres keine Mails mit Anlage mehr zu öffnen und außerdem sein Notebook auf den Wurm hin zu scannen. Durch diese Maßnahme wird festgestellt, dass der Wurm tatsächlich über diese drahtlose Verbindung eingedrungen ist. Nachdem der Chef darüber informiert wurde, installiert auch er einen entsprechenden Malwarescannerscanner für sein System mit der neuen Signatur und entfernt den Wurm mit dem entsprechenden Tool.
Nachdem das Netz des Hauptquartiers erneut sauber und einsatzbereit ist, kann es wieder mit den Zweigstellen und dem Internet verbunden werden. Tatsächlich meldet der Virenscanner der Firewall noch zahlreiche weitere Ausbreitungsversuche des Wurms, aber im Netz der Organisation ist der Vorfall beendet...

5.2.3. Bestehendes Notfallkonzept

Der Angriff eines Wurms (oder allgemein der Angriff von Malware) ist eine so häufig vorkommende Vorfallsklasse, dass es mittlerweile sogar schon allgemein vorgefertigte Notfallkonzepte dafür gibt. Zumindest gibt es zahlreiche Quellen, an denen sich eine Organisation bei der Inhaltsbestimmung orientieren kann. Auch IRTs geben hierzu häufig Hilfestellung.
Im vorliegenden Szenario soll das Notfallkonzept diesen Richtlinien folgen. Zwei Punkte wurden bereits im Vorfallshergang erwähnt: Das Trennen des lokalen Netzwerks von den

anderen Netzen und die Aufspürung und Beseitigung der Wurminstanzen von den einzelnen Rechnern. Beides dient der raschen Beendigung des Angriffs. Der zweite Punkt hat zusätzlich noch die Funktion, die Verfügbarkeit der Rechner wiederherzustellen. Damit sind erneut die Hauptaufgaben eines Notfallkonzepts hervorgetreten.
Im Folgenden soll nun das Notfallkonzept dieses Szenarios der Beispielfirma modelliert werden.

Im Rechnernetz des Hauptquartiers sind vor allem zwei wichtige, zu schützende Werte betroffen: Die Daten auf den Servern (insbesondere ihre Vertraulichkeit, Verfügbarkeit und Integrität), sowie die Verfügbarkeit der Rechner im Netz (Server und Workstations). Natürlich gibt es noch zahlreiche weitere Werte im Hauptquartier, diese werden jedoch durch einen Wurm nicht bedroht und sind daher für dieses Notfallkonzept nicht relevant.
Die Aufgabe des Notfallkonzepts besteht also darin, die beiden oben genannten Werte wieder herzustellen, wenn sie durch einen Angriff von außen beeinträchtigt wurden. Liegt ein solcher Fall vor, muss das Rechnernetz zunächst von allen Zugängen zu den anderen Netzen getrennt werden, indem die Verbindungen über die Firewalls und das Fluttor gekappt werden. Drahtlose Verbindungen zwischen dem internen Netz und der Außenwelt sind generell nicht zulässig, da sie die Filtermechanismen der Firewall umgehen.
Der Verkehr im internen Netz soll auf ein Minimum reduziert werden. Bei Bedarf sollen die einzelnen Rechner von der Netzleitung physikalisch getrennt werden, bis geklärt ist, um was für einen Vorfall es sich handelt. Wurde auf diese Weise der Angriff gestoppt, soll die Art des Angriffs aufgeklärt werden. Falls es sich um einen Malwareangriff handelt, werden von den Anti-Malware Herstellern ein entsprechendes Gegenmittel und bei Bedarf ein Signatur-Update der Malware beschafft. Mit dem Signatur-Update werden die Virenscanner in den Firewalls und dem Fluttor auf den neuesten Stand gebracht.
Falls ein Tool zum Aufspüren und Entfernen der Malware gefunden wurde, wird es benutzt. Nur falls dies nicht der Fall ist, werden die Rechner neu installiert. Anschließend werden die Back-Ups der beiden Server eingespielt. Sind alle Rechner im Netz wieder sauber und vollständig betriebsbereit, wird zunächst das interne Netz wieder zusammengesteckt. Ist auch die Aktualisierung von Firewalls und Fluttor abgeschlossen, kann das interne Netz auch wieder mit den anderen Netzen verbunden werden.

Es fällt auf, dass mit der Abarbeitung dieses Notfallkonzepts der Normalbetrieb praktisch schon wieder hergestellt ist. Dies ist eine Ausnahme, üblicherweise stellt ein Notfallkonzept nur den Minimalbetrieb des unbedingt notwendigen wieder her. Bei einem Wurmvorfall, wie er hier beschrieben wurde, gibt es jedoch nur selten langfristigere Auswirkungen, die sich aktiv bekämpfen lassen. Bei genauer Betrachtung sind natürlich auch hier Langzeitfolgen vorhanden (Imageverlust etc.), aber diese werden weder durch ein Notfallkonzept noch durch langfristige Incident Response Arbeit behandelt, sondern fallen eher in den Bereich des Marketings und der Werbung. Bei anderen klassischen Vorfällen wie etwa Bränden sind

sowohl Notfallkonzept wie auch langfristige, direkt mit dem Vorfall verknüpfte Maßnahmen nötig (z.B. Wiederaufbau von Gebäuden).

Die Schilderung des Vorfalls weicht an einigen Punkten vom Notfallkonzept ab, z.B. hätte die drahtlose Verbindung sofort unterbrochen werden müssen, und der Netzverkehr im internen Netz wurde auch nicht heruntergefahren. Dafür wurde das Öffnen weiterer Anlagen verboten, was nicht im Notfallkonzept stand. Ebenso waren das Installieren von Patches und das Alarmieren eines IRT nicht im Notfallkonzept verankert.
Solche Diskrepanzen ergeben sich auch in der Praxis häufig und liefern die Anhaltspunkte dafür, inwieweit ein Notfallkonzept noch verbessert werden kann. Im Weiteren wird darauf noch näher eingegangen, und es werden die Veränderungen vorgestellt, die das Notfallkonzept aufgrund der Erfahrungen mit diesem Vorfall erfahren könnte.

5.2.4. Arbeit und Ergebnisse des IRTs

Beim vorliegenden Szenario wurde ein IRT eingeschaltet, um bei der Umsetzung des Notfallkonzepts zu helfen. Bei der Ablaufschilderung wurde auf die genaue Arbeit des IRTs nur kurz eingegangen. An dieser Stelle sollen die möglichen Tätigkeiten eines IRT in diesem Szenario näher beschrieben werden, auch über die bloße Umsetzung des Notfallkonzepts hinaus. Dabei orientiert sich der Text erneut am Katalog der Dienstleistungen eines IRT.

- Incident Analysis

Die Analyse eines Vorfalls muss mit der Frage beginnen, ob überhaupt ein Sicherheitsvorfall vorliegt. Wenn wie in der Ablaufschilderung das IRT benachrichtigt wird, weil der abnormal starke Netzverkehr die Leitungen blockiert und der Verdacht eines Wurmbefalls besteht, so liegt eindeutig ein Sicherheitsvorfall vor. Er liegt nicht vor, weil Wurmverdacht besteht, sondern weil die zu schützenden Werte beeinträchtigt wurden.
Als nächstes ist die Art des Vorfalls festzustellen. Da bereits ein Verdacht besteht, werden die Seiten der Anti-Malware Industrie und der anderen IRT nach Hinweisen auf konkrete neue Würmer abgesucht. Erst wenn der Verdacht, dass ein neuartiger Wurm das Netz befallen hat, durch den Nachweis der Malware im Rechnernetz bestätigt wurde, ist die Art des Vorfalls geklärt.
Im vorliegenden Szenario ist der Wurm zwar neu, aber die Anti-Malware Industrie hat ihn dennoch bereits analysiert und Signatur und Gegenmittel bereitgestellt. Somit ist von Seiten des IRTs keine weitere Vorfallsanalyse mehr notwendig, nachdem der Wurm eindeutig identifiziert wurde.
Hätte die Anti-Malware Industrie hingegen noch kein Gegenmittel gefunden, hätte gemäß Notfallkonzept der Netzverkehr minimiert werden müssen (gegebenenfalls durch Abklemmen der Rechner), bis der Vorfall analysiert gewesen wäre. Auch in diesem Fall wäre die genaue Analyse vermutlich der Anti-Malware Industrie überlassen worden.

- Reinigung

Bei einem Wurmvorfall ist die Reinigung eine sehr wichtige Aufgabe, denn der Wurm bedroht sowohl die Verfügbarkeit als auch die Integrität der Systeme. Die Relevanz der Reinigung ist schon im bestehenden Notfallkonzept verankert, denn die Rechner im Netz sollen mit einem Tool von der Malware befreit oder komplett neu installiert werden.
Allerdings sind diese Reinigungsmaßnahmen unkritisch auszuführen, wenn das Notfallkonzept und die Sicherheitspolitik eingehalten werden. Da dies gemäß des Szenarioablaufs nicht der Fall ist (vom Notfallkonzept wird an verschiedenen Stellen abgewichen, die Verbindung über das Notebook an der Firewall vorbei verletzt die Sicherheitspolitik), kann der Wurm nicht endgültig entfernt werden, denn er dringt immer wieder ins Netzwerk ein. Mit einem verbesserten Notfallkonzept und einer strikten Einhaltung der Sicherheitspolitik könnte das Cleaning somit vereinfacht werden.

- Vermeidung

Im vorliegenden Szenario hat die Organisation bereits einiges zur Vorfallsverhinderung getan, indem die Firewalls, das Fluttor und der Virenscanner gemäß gängiger Richtlinien konfiguriert (generelles Verbot usw.) und im Regelfall auf dem neuesten Stand gehalten wurden. Das Szenario zeigt allerdings, dass schon eine kleine Unachtsamkeit einen Vorfall auslösen kann. So war die Signatur des neuen Wurms bereits bei den Anti-Malware Herstellern vorhanden. Wäre sie sofort nach dem Erscheinen vom Administrator installiert worden, wären die Firewalls weiterhin sicher gewesen.
An anderen Stellen wurden notwendige Vermeidungsmaßnahmen nicht umgesetzt. So waren die Betriebssysteme gegen eine bekannte Sicherheitslücke ungepatcht, und die Durchsetzung der Sicherheitspolitik war mangelhaft, da eine drahtlose Verbindung vom Netz nach draußen bestand.
Die Aufdeckung solcher Mängel ist eine Aufgabe und Dienstleistung des IRTs, und die Ergebnisse dieser Arbeiten sollten direkt in Sicherheitspolitik und Notfallkonzept einfließen. Unter Umständen können hier auch organisatorische Maßnahmen helfen, wie etwa die Benachrichtigung des Administrators über das Bereitstehen einer neuen Malwaresignatur. Nach einer solchen Nachricht kann der Administrator nicht nur den Virenscanner aktualisieren, sondern sich auch gleich über die neue Malware selber und die ausgenutzten Schwächen informieren.

- Gegenwehr

Im Szenarioablauf fallen die Gegenmaßnahmen teilweise mit dem Cleaning zusammen. Dies liegt in der Natur replikativer Malware: Wenn die Malware von einem Rechner entfernt wird, ist der Rechner anschließend sauber (Cleaning). Gleichzeitig kann die Malware sich dann von diesem Rechner nicht weiter ausbreiten (Gegenwehr).

Der Szenarioablauf enthielt aber noch weitere Gegenwehrmaßnahmen. Das Abkoppeln des Netzes vom Internet und von den Zweigstellen ist eine typische Maßnahme, um den Vorfall zu beenden und gehört damit auch ins Notfallkonzept.
Im Szenarioablauf wurden allerdings auch Gegenmaßnahmen vom Administrator und vom IRT ergriffen, die obwohl sinnvoll nicht im Notfallkonzept verankert waren. Dazu gehören das Aussprechen eines Verbots zum Öffnen von Anlagen und das Einspielen des Patches gegen die 08/15-vulnerability. Werden solche sinnvollen und richtigen Maßnahmen im Notfall intuitiv ergriffen, sollten sie für die Zukunft ins Notfallkonzept integriert werden. Diese Regel gilt allerdings nur, sofern die Maßnahme nicht zu speziell ist. So ist das Verbot zum Öffnen von Anlagen in einem Notfallkonzept gegen Wurmbefall sinnvoll, da viele Würmer sich als Mailanlage verschicken. In einem allgemeinen Notfallkonzept für Malwareangriffe könnte diese Maßnahme aber zu speziell sein.

- Rechtliche Schritte

Bei Malwareangriffen mit replikativer Malware werden nur selten rechtliche Schritte von einer einzelnen Organisation ergriffen. Die damit verbundenen Probleme wurden im Abschnitt 3.6. dargestellt. Für dieses Szenario sollen weitreichende rechtliche Schritte nicht betrachtet werden, da sie auf das Notfallkonzept keinen Einfluss haben und langfristigere Maßnahmen wie dargestellt nicht zur Vorfallsbekämpfung notwendig sind.
Natürlich ist in einem realen Vorfall eine Rechtsverfolgung eines Wurmautors oder der Person, die den Wurm freigesetzt hat, sinnvoll und richtig. Denn nur durch rechtliche Schritte können andere Personen von solchen Angriffen abgehalten werden. Auch im Szenario könnte das IRT Spurensicherung betreiben und die bereits geschilderte Kette der Rechtsverfolgung in Gang setzen. Ähnlich wie im ersten Szenario könnte daraus die Erlangung von Schadensersatz anstrebt werden. Der Ablauf würde aber dem aus dem ersten Szenario zu sehr ähneln, als dass er hier noch einmal dargestellt werden müsste.

5.2.5. Einfluss auf die Weiterentwicklung des Notfallkonzeptes

Welchen Einfluss die Arbeit des IRTs auf das Notfallkonzept in diesem Szenario haben kann, wurde bereits an mehreren Stellen angedeutet.
Im Großen und Ganzen hat das bestehende Notfallkonzept für die unmittelbare Bekämpfung des Vorfalls ausgereicht, denn der Angriff konnte beendet und der angerichtete Schaden behoben werden. Dennoch gibt es einige Schwachstellen, die durch den Vorfall und seine Bekämpfung aufgedeckt wurden.
So könnte beispielsweise das sofortige Einspielen von Patches ins Notfallkonzept aufgenommen werden. Noch besser wäre es, das regelmäßige Einspielen neuer Patches zusätzlich in den Normalbetrieb aufzunehmen. Durch beide Maßnahmen könnten Notfälle entweder verhindert oder schneller bekämpft werden.
Fraglich ist, ob das Verbot zum Öffnen von Anlagen in das Notfallkonzept aufgenommen werden sollte. Für Wurmvorfälle wäre dies sinnvoll, für zahlreiche andere Vorfälle mit

Malware allerdings nicht. Zur Beantwortung der Frage muss klargestellt werden, ob das Notfallkonzept allgemeine Angriffe oder nur Wurmangriffe abdecken soll.
Bei der Bearbeitung des Vorfalls haben sich Administrator und IRT die Arbeit geteilt. Eine Alarmierung eines eventuell firmeneigenen IRT könnte ebenfalls als Maßnahme ins Notfallkonzept übernommen werden. Ein qualifizierter Administrator könnte die notwendigen Arbeiten unter Umständen auch alleine ausführen, würde dazu aber viel mehr Zeit benötigen als ein ganzes Team, deshalb wäre eine Anpassung des Konzepts hier sinnvoll.
Neben dem Notfallkonzept müssen auch die Sicherheitspolitik und ihre Umsetzung verbessert werden (vgl. erstes Szenario). Wäre beispielsweise der Personalserver nicht nebenbei als Workstation genutzt worden, wäre er nicht vom Wurm infiziert worden. Hätte ein generelles Verbot vom Öffnen unerwarteter Anlagen bestanden, hätte der Angriff vielleicht sogar verhindert werden können. Auf Seiten der Umsetzung ist vor allem die drahtlose Verbindung des Chefrechners nach draußen zu bemängeln. Falls die neuen Vorschläge zur Sicherheitspolitik (Patches usw.) übernommen werden, muss deren Umsetzung ebenfalls gewährleistet sein. So müssen die Patches dann auch tatsächlich installiert werden.

5.2.6. Fazit

Während das erste Szenario hauptsächlich die langfristigen Maßnahmen zur Vorfallsbekämpfung sowie die langfristigen, nicht mit dem konkreten Vorfall verflochtenen Maßnahmen fokussierte, hat sich das zweite Szenario fast ausschließlich mit den kurzfristigen Maßnahmen eines Notfallkonzepts beschäftigt.

Es wird eine Dreistufigkeit der Gegenmaßnahmen deutlich, vgl. Abbildung 11:

Kurzfristige Maßnahmen	Langfristige Maßnahmen	Andauernde Maßnahmen
Notfallkonzept, Spontanreaktionen...	Wiederaufbau von zerstörter Infrastruktur, Rechtliche Schritte, usw.	Solide Sicherheitspolitik, Risikomanagement, Schutzmaßnahmen, usw.
immer mit dem konkreten Vorfall verbunden, reaktiv, Wirkung zeigt sich sofort	Mit dem konkreten Vorfall verbunden, reaktiv, aber ohne sofortige Wirkung	Nicht mit dem konkreten Vorfall verbunden, präventiv, Erfolg zeigt sich dann beim konkreten Vorfall

Abbildung 11: Dreistufigkeit der Gegenmaßnahmen

Die dritte Stufe, die andauernden Maßnahmen, war in beiden Szenarien von Belang. Prinzipiell sind bei jeder Vorfallsbekämpfung alle drei Stufen vorhanden, es gibt allerdings starke Variationen, wie stark sie bei einem konkreten Vorfall eine Rolle spielen.

5.3. Angriff von außen: Trojaner

Im dritten Szenario der Arbeit wird ein weiterer Angriff von außen durchgespielt: Die Auswirkung eines trojanischen Pferdes auf einem Rechner der Firma. Da der Trojaner Datenspionage betreiben soll, verbindet dieses Szenario in gewisser Weise Teile aus den ersten beiden Szenarien: Die Datenspionage aus dem ersten und den Angriff von außen aus dem zweiten Szenario.

Die erforderlichen Gegenmaßnahmen bei einem Trojaner unterscheiden sich jedoch grundlegend von den Gegenmaßnahmen in den ersten beiden Szenarien: Bei einem Trojaner ist die Entdeckung von zentraler Bedeutung. Die Beseitigung des Trojaners nach seiner Entdeckung ist oftmals ein wesentlich kleineres Problem.

5.3.1. Vorstellung des Szenarios

Während im zweiten Szenario ein großer Augenmerk auf dem Eindringen von Malware ins System gelegen hat, wird dieser Punkt in diesem Szenario eine geringere Bedeutung haben. Der Trojaner befindet sich im fiktiven Computerspiel „Krassgeballer“, das frei aus dem Internet herunter geladen werden kann. Bei dem Spiel muss der Spieler seine vom Computer oder anderen Mitspielern gesteuerten Gegner abschießen. Dazu kann das Spiel über das Netz mit anderen Instanzen des Spiels verbunden werden.

Während das Spiel gespielt und Daten über das Netz zu seinen anderen Instanzen verschickt werden, werden gleichfalls die Rechner, auf denen das Spiel läuft, durch die trojanische Funktion des Spiels nach Daten, Passwörtern, bekannten und häufig benutzten Dokumentformen sowie Daten über die Systemkonfiguration abgesucht und an den Autor des Spiels versandt. Dieser untersucht sie stichprobenartig nach Daten, die er interessant findet. Er hat dabei nicht vor, Profit aus den Daten zu ziehen, sondern möchte mit dieser Aktivität nur seine Neugier befriedigen und herausfinden, „was andere Leute so auf ihrem Rechner haben“.

Ähnlich wie im ersten Szenario handelt es sich auch hier um einen Fall der Datenspionage. Die primär bedrohten Werte sind also ebenfalls die Daten auf den betroffenen Rechnern, wobei Vertraulichkeitsschaden entsteht. Durch das Versenden der ausspionierten Daten entsteht zudem ein begrenzter Verfügbarkeitsschaden an Netzwerkressourcen. Die Integrität von Daten und Netzwerk ist nicht betroffen. Solange der Autor des Trojaners die Daten nicht anderweitig nutzt, treten kaum sekundäre Schäden auf (vgl. erstes Szenario, Unterabschnitt 5.1.1.). Lediglich ein Schaden durch Imageverlust bei Bekannt werden des Vorfalls käme in Betracht.

5.3.2. Technischer Aufbau und Art des Vorfalls

Wiederum folgen zunächst die Kenngrößen, dann die Ablaufbeschreibung des Vorfalls.

- Systeme

Der Vorfall ereignet sich im Hauptquartier der Firma und greift nicht auf die Systeme der Zweigstellen über, somit sind nur die Systeme des Hauptquartiers von Belang. Für den Vorfall wird ein homogenes Netz angenommen, also haben alle Workstations im Netz das gleiche Betriebssystem und eine gleiche oder zumindest sehr ähnliche Hardwareausstattung. Auf allen läuft ein Betriebssystem, unter dem das Spiel Krassgeballer gespielt werden kann.
Die Passwörter, Systemdaten und Dokumente sind durch eine Benutzerverwaltung geschützt. Ein Benutzer kann nur sein eigenes Passwort ändern und hat keinen Einfluss auf die Konfiguration des Betriebssystems. Nur angemeldete Benutzer können zudem die Dokumente einsehen und bearbeiten. Die Systemkonfiguration kann nur vom Administrator angezeigt und geändert werden. Der in Krassgeballer integrierte Trojaner nutzt jedoch eine im Betriebssystem bestehende Schwachstelle aus, um Passwörter, Systemdaten und Dokumente auszulesen. Gegen diese Schwachstelle gibt es einen Patch, der allerdings noch nicht installiert ist.
Der Personalserver und der Fileserver sind in diesem Szenario baugleich mit den Workstations und haben das gleiche Betriebssystem. Lediglich die Festplatte ist größer, um den Platz für die Serverfunktionalitäten zu bieten. Somit sind auch die Server anfällig für den Trojaner.
Der Trojaner ist in Krassgeballer integriert und wird gestartet, wenn auch das Spiel gestartet wird. Er nistet sich nicht im System ein und hat auch keine Tarnfunktion, sondern befindet sich in einer Programmroutine des Spiels selber. Somit verschwindet der Trojaner vom System, sobald das Spiel gelöscht wird. Und seine Ausführung wird beendet, sobald das Spiel beendet wird.
Um nicht ohne weiteres aufzufallen, erfolgt die Versendung der ausspionierten Daten über ein vom Autor selbst entworfenes Kommunikationsprotokoll, das auf dem TCP/IP Protokollstapel basiert. Die Unterstützung dieses Protokolls übernimmt der Trojaner selber.
Der Trojaner ist relativ neu und bislang noch weitgehend unbekannt. Deshalb existiert von der Anti-Malware Industrie noch keine Scannersignatur.

- Backups

Für dieses Szenario spielen die Backups keine Rolle, da die Systeme nicht verändert oder unverfügbar gemacht werden. Lediglich zum Entfernen des Trojaners wäre ein Rückgriff auf Backups in Form von Images der Systeme denkbar.

- Zugriffsrechte

Auf seiner Workstation hat jeder Mitarbeiter Benutzerrechte. Für die administrativen Aufgaben, insbesondere das Ändern der Systemkonfiguration, werden Administratorrechte benötigt, die die normalen Benutzer nicht haben. Auf den Workstations werden Dokumente gespeichert, die gerade in Bearbeitung sind. Momentan nicht benötigte oder sehr

umfangreiche Dokumente lagern auf dem Fileserver. Dieser steht in einem separaten Serverraum und wird nicht als Workstation benutzt. Auf ihm hat analog zum zweiten Szenario jeder Mitarbeiter ein passwortgeschütztes Verzeichnis mit seinen Dokumenten. Zudem gibt es wiederum ein öffentliches Verzeichnis, das ohne Passwort gelesen werden kann.
Der Personalserver befindet sich im Büro der Personalsachbearbeiterin und wird von dieser neben der Serverfunktionalität auch zum Erledigen der normalen Arbeiten benutzt. Analog zum zweiten Szenario verfügt er über ein großes Datenverzeichnis, in dem die Personaldaten abgelegt sind. Diese werden in Form von vielen kleineren Dokumenten gespeichert, eines für jeden Mitarbeiter. Zum Öffnen dieser Dokumente ist eine Datenbanksoftware nötig, die auf dem Personalserver installiert ist und in der Firma selbst entwickelt wurde. Die Software öffnet die Dokumente nur, wenn ein korrektes Passwort eingegeben wird, das den Benutzer als Personalsachbearbeiter ausweist. Dieses Passwort wird nicht in den Dokumenten, sondern in den Dateien der Software selbst in verschlüsselter Form gespeichert.
Auch auf den beiden Servern sind Administratorrechte erforderlich, um die Systemkonfiguration auszulesen oder zu ändern.

- Mitarbeiterkompetenzen

Jeder Mitarbeiter hat auf seiner Workstation Benutzerrechte und kann zudem auf sein Verzeichnis sowie das öffentliche Verzeichnis auf dem Fileserver zugreifen. Die Benutzerrechte sind weiter gefasst als normal und erlauben auch das Installieren von Software. Die Personalsachbearbeiterin hat ebenfalls Benutzerrechte auf dem Personalserver. Sie kennt zudem das Passwort für die Datenbanksoftware, das außer ihr nur dem Firmenchef und ihrer Krankenvertretung bekannt ist.
Der Administrator des Hauptquartiers hat auf allen Rechnern vollständige Administratorrechte. Auf den Workstations kann er die Konfiguration ändern und auch die Dokumente einsehen
Alle Mitarbeiter mit Benutzerrechten dürfen auf ihren Rechnern neue Software installieren. Dies ist notwendig, weil die einzelnen Mitarbeiter die in der Firma entwickelten Softwareprodukte auf ihren Workstations testen sollen.
Die Firewalls und das Fluttor werden vom Administrator gepflegt und konfiguriert. Neben ihm hat nur der Firmenchef Zugriff auf die Konfiguration dieser Systeme.

- Sicherheitspolitik

Die Daten auf den Workstations und den beiden Servern sind vertraulich, verfügbar und integer zu halten. Dies soll ähnlich wie im zweiten Szenario durch die Firewalls, das Fluttor und den Passwortschutz gewährleistet werden.
Die wichtigen Dokumente sollen nur zur Bearbeitung auf den Workstations gespeichert werden. Danach sollen sie wieder auf dem Fileserver abgelegt werden, wo ständig die

aktuellsten Versionen verfügbar sein sollen. Es ist allerdings nicht verboten, Bearbeitungskopien auf den Workstations zu behalten.
Die Personaldaten sollen nur der Personalsachbearbeiterin und dem Firmenchef zugänglich sein. Es ist der Personalsachbearbeiterin verboten, die Personaldaten auf dem Server anderen zugänglich zu machen oder zu versenden. Auf die (nicht näher modellierten) Backups dieser Daten hat der Administrator nur soweit Zugriff, wie es zum Anlegen des Backups und zum wieder einspielen notwendig ist.
Das Herunterladen und Installieren von Software aus dem Internet ist erlaubt. Damit dadurch keine Unsicherheiten entstehen, werden heruntergeladene Daten beim Passieren der Firewalls oder des Fluttors an einen Content Scanner übergeben, der immer mit den aktuellsten Malwaresignaturen zu konfigurieren ist.
Die Sicherheitspolitik ist in der Firma bekannt gemacht worden.

- Konfiguration der Firewalls

Die Firewalls sind nach dem Prinzip des generellen Verbots konfiguriert. Vom Internet ins Firmennetz wird nur ausgewählter Netzverkehr über Erlaubnisregeln durchgelassen. Allerdings wird jeglicher Verkehr aus dem Firmennetz ins Internet heraus ungefiltert durchgelassen, da für diese Kommunikationsrichtung eine generelle Erlaubnisregel aktiviert wurde. Deshalb werden die vom Trojaner versendeten TCP Datenplakate von der Firewall nach außen durchgelassen.
Einmal täglich verbindet sich das jeweilige Firewallsystem für kurze Zeit mit dem Anti-Malware Hersteller und lädt automatisch die neusten Signaturen herunter und installiert sie. Während diesem kurzen Vorgang ist der Netzverkehr über diese Systeme gesperrt. Da das Herunterladen und Installieren jedoch nachts geschieht, wird der Betrieb dadurch nicht beeinträchtigt.
Da der Trojaner noch sehr neu und relativ unbekannt ist, verfügen der Anti-Malware Hersteller und somit auch die Firewalls über keine Signatur des Trojaners.
Die Firewall protokolliert den Netzverkehr, der sie passiert hat. Dabei werden Informationen über verwendete bekannte Protokolle und Ports, sowie Quell- und Zieladressen geloggt.

- Konfiguration des Fluttors

Die Konfiguration des Fluttors gleicht der der Firewalls, allerdings gelten die implementierten Filterregeln für beide Kommunikationsrichtungen. Das automatische Herunterladen von Signaturen findet hier ebenfalls statt.

- Weitere Kenngrößen

Das Kommunikationsprotokoll des Trojanerautors verwendet einen TCP Port, der normalerweise nicht von TCP basierten Protokollen genutzt wird. Der Autor erwartet Verkehr auf diesem Port, und der Trojaner versendet die Daten ebenfalls auf diesem Ports.

Die Daten, die das Spiel während einer Spielrunde über das Netz verschickt, verwendet dasselbe Protokoll und denselben Port.

Nach der Festlegung der Kenngrößen folgt nun die Beschreibung vom Ablauf des Vorfalls.
An einem Dienstagmorgen entdeckt eine Mitarbeiterin des Hauptquartiers ein neues Spiel namens Krassgeballer auf einer Internetseite. Da das Spiel nichts kostet, gemäß der Anpreisung „ganz toll“ sein soll und die Mitarbeiterin gerade privaten Stress hat, lädt sie das Spiel herunter, um sich ein wenig abzureagieren.
Während der Mittagspause probiert sie das Spiel aus. Es gefällt ihr sehr gut, und sie entdeckt zudem, dass das Spiel auch eine Netzfunktion hat. Sie zeigt es ihren Kollegen. Einige sind ebenfalls begeistert davon und laden es herunter. Zu den begeisterten Spielern gehört auch die Personalsachbearbeiterin.
Während der folgenden Tage spielen zahlreiche Mitarbeiter während ihrer Mittagspause das Spiel über das Netz. Einige spielen es alleine auch während der Arbeitszeit, wenn sie sich unbeobachtet fühlen. Die Firmenleitung erfährt zwar recht schnell von dem neuen Spiel, schreitet aber nicht ein, da es die Motivation der Mitarbeiter erheblich verbessert.
Während der Spielrunden sendet der im Spiel integrierte Trojaner Daten und Dokumente von den Workstations und auch vom Personalserver an den Autor des Trojaners. Die Dokumente von den Workstations sind im Format gängiger Anwenderprogramme und können vom Autor des Trojaners problemlos geöffnet werden. Die Daten des Personalservers allerdings sind für ihn nicht lesbar, da er nicht über das firmeninterne Datenbanksystem verfügt.
Mit den ausspionierten Dokumenten und Systemdaten könnte der Trojanerautor problemlos der Firma großen Schaden zufügen, indem er die Dokumente der Konkurrenz zugänglich macht oder auf das Firmennetz selber einen Verfügbarkeitsangriff startet.
Tagelang merkt niemand in der Firma, dass ständig Daten ausspioniert werden. Erst als der Administrator die Logfiles der Firewalls durchsieht, bemerkt er einen sonderbar hohen TCP Verkehr aus dem internen Netz heraus. Er befragt einige Mitarbeiter, aber keiner in der Firma hat wissentlich soviel TCP Verkehr abgesetzt. Daraufhin verfolgt der Administrator den Verkehr zu dessen Ursprungssystemen zurück und stellt Vergleiche an. Da auf allen diesen Systemen Krassgeballer installiert ist, bittet er die Mitarbeiter, das Spielen für einige Zeit einzustellen. Als daraufhin der TCP Verkehr zurückgeht, fällt sein Verdacht darauf, dass das Spiel mit irgendjemandem im Internet kommuniziert.
Er untersucht die vom Spiel versendeten Datenpakete auf deren Inhalt. Da ihm das Protokoll unbekannt ist, benötigt er einige Zeit, um das Format zu entschlüsseln. Vier Wochen nach Installation der ersten Instanz von Krassgeballer entdeckt der Administrator, dass das Spiel offenbar Dokumente von den Systemen nach außen verschickt. Sofort meldet er den Vorfall an die Firmanleitung, die daraufhin das Ausführen von Krassgeballer verbietet und ein IRT mit der Bearbeitung des Vorfalls beauftragt, wie es im Notfallkonzept vorgesehen ist...

5.3.3. Bestehendes Notfallkonzept

Wie bereits im ersten Szenario diskutiert kann der Hauptpunkt eines Notfallkonzepts, die Wiederherstellung der Verfügbarkeit, bei einem Vorfall der Datenspionage ignoriert werden. Anders als im ersten Szenario ist das zweite Ziel eines Notfallkonzepts, die möglichst rasche Beendigung des Vorfalls, hier von großer Bedeutung. Zum Zeitpunkt der Entdeckung dauert der Vorfall noch an, und um weitere Schäden zu vermeiden, muss er zunächst beendet werden.

Das Notfallkonzept für Datenspionage in diesem Szenario soll wie folgt aussehen: Das Ziel ist die Abstellung des Vorfalls. Dazu sollen bei netzbasierter Spionage zunächst die Verbindungen gekappt werden, über die die Spionage erfolgt. Falls diese nicht bekannt sind, werden alle Verbindungen nach außen gekappt, indem Firewalls und Fluttore auf „alles blocken“ eingestellt werden.

Als nächstes wird der Vorfall soweit aufgeklärt, dass eine Fortsetzung der Spionage beim Wiedereröffnen der Leitungen nicht eintritt. Dazu muss geklärt werden, wo sich der Spion bzw. sein Ansatzpunkt befindet und welche Werkzeuge er eingesetzt hat. Anschließend sind der Spion und seine Werkzeuge aus dem Netz bzw. der Firmenumgebung zu entfernen. Ist dies erfolgt, werden die Netzzugänge wieder geöffnet und die langfristige Bearbeitung des Vorfalls eingeleitet.

Dieses Notfallkonzept ist sehr allgemein, da es für alle Vorfälle der Datenspionage gelten soll. Wie im ersten Szenario unter 5.1.3. ausführlich diskutiert sind bei Datenspionage die langfristigen Gegenmaßmaßnahmen eher bedeutsam als das Notfallkonzept. Für dieses Szenario soll angenommen werden, dass noch kein Langzeitplan existiert. Welche Maßnahmen ausgewählt und durchgeführt werden, zeigt der Abschnitt über die Arbeit des IRTs in diesem Szenario.

5.3.4. Arbeit und Ergebnisse des IRTs

Der Abschnitt über die Arbeit und die Ergebnisse des IRTs folgt der gewohnten Gliederung.

- Incident Analysis

Bei einem Trojanerangriff gestaltet sich die Vorfallsanalyse oftmals besonders schwer. Das liegt daran, dass die meisten Trojaner über Tarnungsmechanismen verfügen. Mit diesen tarnen sie entweder sich selber oder den von ihnen versandten Netzverkehr. Aber selbst wenn ein Trojaner nicht über spezielle Tarnungsmechanismen verfügt, ist seine Entdeckung in der Regel schwierig. Er breitet sich nicht über das Netz aus, und wenn der Trojaner mit Netzverkehr sparsam umgeht, kann er oft eine sehr lange Zeit in einem System verweilen, ohne dort aufzufallen.

Im Szenario hat der Trojaner jedoch eine große Menge Netzverkehr verursacht, weil er auf mehreren Systemen parallel aktiv war und sein Verkehr über einen einzelnen Punkt geleitet wurde: die Firewall. Somit liegt mit Sicherheit eine Anomalie vor. Des Weiteren stellt sich

wiederum die Frage, ob es sich auch um einen Sicherheitsvorfall handelt. Dies ist hier bereits vor der Arbeitsaufnahme des IRTs zu bejahen, denn der Administrator hat bereits entdeckt, dass Krassgeballer vertrauliche Daten ausspioniert hat.
Nach der Feststellung eines Sicherheitsvorfalls beginnt die eigentliche Vorfallsanalyse. Da es sich bei Krassgeballer offenbar um Mallware handelt, wird das IRT sich zunächst an die Hersteller von Anti-Malware wenden, um möglichst viel über die Malware zu erfahren und um an Signaturen und Reinigungstools zu gelangen. Im Szenario wurde der Trojaner als relativ unbekannt modelliert, weshalb diese Suche nichts ergibt. Folglich muss das IRT die Funktionsweise des Trojaners selbst untersuchen und Entfernungsmechanismen erarbeiten.
Die Funktionsweise lässt sich leicht in einem Testnetz untersuchen. Es wird festgestellt, dass Daten vom Rechner, auf dem Krassgeballer gestartet wurde, versandt werden. Dies hält nur solange an, wie auch das Spiel aktiv ist. Auch das Format der versandten Pakete kann schnell analysiert werden, da diese Arbeit zu großen Teilen schon vom Administrator erledigt wurde.
Ein Punkt ist bei einem wie hier relativ lange andauernden Vorfall von besonderer Brisanz: die Abschätzung des angerichteten Schadens. Zwar kann der Zeitraum, während dem Daten ausspioniert wurden, einfach festgestellt werden (es muss nur ermittelt werden, wann Krassgeballer zum ersten Mal im Netz gestartet wurde). Welche und wie viele Daten ausspioniert wurden, kann allerdings nur schwer festgestellt werden. Dennoch ist diese Aufgabe lösbar. Administrator und IRT müssen dazu die Logfiles der Firewall analysieren, denn diese protokolliert jeglichen Netzverkehr, der sie passiert hat. Diese Arbeit dauert allerdings sehr lange, und es ist fraglich, ob sie sich lohnt. Zudem müssten die Erkenntnisse über die ausspionierten Daten noch in finanziellen Schaden umgerechnet werden. Dies ist allein schon deshalb nahezu unmöglich, weil über die Motive des Täters nichts bekannt ist.
Somit werden sich Firma und IRT mit der technischen Aufklärung des Vorfalls begnügen.

- Reinigung

Reinigung spielt bei Trojanervorfällen wie bei allen Vorfällen mit Malware eine große Rolle. Ebenso wie bei der Vorfallsanalyse stellen aber auch bei der Reinigung die Tarnungsmechanismen eines Trojaners ein Problem dar. Denn nach Anwendung der Reinigungsmechanismen muss sichergestellt sein, dass der Trojaner auch wirklich vom System entfernt wurde.
Die Reinigung im vorliegenden Szenario gestaltet sich allerdings dann relativ einfach, wenn die Vorfallsanalyse gründlich durchgeführt wurde. Dann ist dem IRT bekannt, dass der Trojaner in Krassgeballer sich nicht im System tarnt und das Spiel zur dauerhaften Beendigung des Vorfalls einfach nur vom System gelöscht werden muss. Krassgeballer nimmt keine Änderungen an den Dateien des Systems vor und löscht auch keine von ihnen. Somit ist eine Entfernung des Spiels zur Reinigung ausreichend.

- Vermeidung

Die Vermeidungsmaßnahmen sollen eine Wiederholung des Vorfalls verhindernn. Im Szenario muss also dafür gesorgt werden, dass Krassgeballer nicht erneut auf Systeme im Netz gelangt.

Dazu ist zunächst eine umfassende Reinigung durchzuführen. Krassgeballer muss also von allen Systemen im Netz entfernt worden sein, wenn die Umsetzung der Verhinderungsmaßnahmen beginnt. Da Krassgeballer sich nicht selbständig ausbreitet, ist die nahe liegendste Verhinderungsmaßnahme, die Neuinstallation von Krassgeballer im Netz zu verbieten. Diese Maßnahme garantiert allerdings keine Sicherheit, da sie sich nicht vollkommen durchsetzen lässt. Verlässlicher ist die Maßnahme, das von Krassgeballer verwendete Protokoll auf der Firewall zu sperren. Dies ist nur dann möglich, wenn das Protokoll vorher analysiert wurde und sich die Ergebnisse der Analyse in Filterregeln für die Firewalls umsetzen lässt. Ist dies nicht möglich, sollte über die Anschaffung einer anderen Firewall mit detaillierteren Filtermechanismen nachgedacht werden.

Eine weitere wichtige Maßnahme zur Verhinderung ist der Einbau der Malwaresignatur von Krassgeballer in den Malwarescanner der Firewalls und des Fluttores. Diese sind zwar noch nicht verfügbar, werden aber in einiger Zeit erscheinen. Diese Zeit kann noch verkürzt werden, indem den Herstellern der Signaturen die Ergebnisse der Vorfallsanalyse zugänglich gemacht werden. Diese Zugänglichmachung umfasst nur die technischen Aspekte des Trojaners, nicht aber die Schadensabschätzung. Mit einer Signatur wird Krassgeballer an der Firewall erkannt und geblockt. Mit ihr kann allerdings nicht verhindert werden, dass der Trojaner auf einem anderen Weg erneut ins Netz gelangt, etwa über Disketten.

Aufgrund der Überlegungen ist eine Kombination aller Maßnahmen angezeigt, um eine neue Datenspionage durch Krassgeballer zu verhindern.

Alle hier aufgezählten Verhinderungsmaßnahmen sind langfristiger Natur und nicht mehr Teil des Notfallkonzepts. Ihre Wirksamkeit kann erst aus den Maßnahmen der Vorfallsanalyse abgeleitet werden. Somit folgen sie als Ergebnis aus der Arbeit des IRTs.

Die diskutierten Verhinderungsmaßnahmen sollten nicht nur im Hauptquartier, sondern auch in den Zweigstellen umgesetzt werden. Die Übertragung der Maßnahmen dorthin hat nur geringen Aufwand und bietet der ganzen Firma einen guten Schutz.

- Gegenwehr

Zu den wichtigsten Maßnahmen der Gegenwehr im vorliegenden Szenario zählt die Schadensbegrenzung. Diese ist besonders heikel, da der Schaden wie diskutiert nur schwer abgeschätzt werden kann. Somit kann ein eventuell sehr hoher Schaden die Firma überraschend treffen.

Da das Ausspionieren der Daten nachträglich nicht ungeschehen gemacht werden kann, müssen andere Maßnahmen ergriffen werden. Durch die Analyse der Logfiles, genauer der geloggten Adressen, können Rückschlüsse darauf gezogen werden, welche Daten ausspioniert

wurden, da nur Daten von den betroffenen Rechnern in Frage kommen. Die Menge der möglichen ausspionierten Daten wird zudem durch die Menge der überhaupt im Netz vorhandenen Daten begrenzt. Die Maßnahmen zur Schadensbegrenzung sollten darauf abzielen, den Wert der Daten für den Angreifer, bzw. die Abhängigkeit der Firma von diesen Daten zu senken. Handelt es sich bei den Daten beispielsweise um Informationen über die sicherheitsrelevante Schnittstelle einer Software, so macht die Entwicklung einer anderen Schnittstelle diese Daten für den Angreifer wertlos. Selbiges gilt dann, wenn Passwörter ausspioniert wurden und ein Ferneinloggen möglich ist. Dann sollten diese möglichst rasch geändert werden. Diese Maßnahme gleicht dem Austauschen eines Türschlosses, für das der Schlüssel gestohlen wurde.
Durch solche Maßnahmen lässt sich nicht jeder Schaden verhindern. Im Regelfall wird eine Schadensbegrenzung sogar nur sehr eingeschränkt möglich sein. Wenn es sich um Forschungsdaten eines neuen Produktes handelt, kann der Wert der Daten nicht gesenkt werden. Dasselbe gilt für Daten über Prozessabläufe, die nicht ohne weiteres geändert werden können.
Auch diese Maßnahmen zur Gegenwehr sind von langfristiger Natur und nicht Teil des Notfallkonzepts. Sie ergeben sich in diesem Szenario ebenso wie die Verhinderungsmaßnahmen erst aus der Vorfallsanalyse und können somit unmöglich bereits im Vorfeld festgelegt worden sein.

- Rechtliche Schritte

In diesem Szenario stellt sich die Frage, gegen welche Person rechtliche Schritte eingeleitet werden sollten. Zunächst bietet sich der Autor des Trojaners an. Dieser wird jedoch nur schwer aufzufinden sein. Ein Anhaltspunkt wäre die Website, von der Krassgeballer herunter geladen worden ist. Allerdings muss sie nicht zwangsläufig auch zu der dahinter stehenden Person führen. Wie bereits im Unterabschnitt 3.6. über die rechtlichen Schritte diskutiert, ist die Spurensicherung schwierig.
Der Autor des Trojaners muss nicht zwangsläufig der Initiator des Angriffs sein. In diesem Szenario war dies zwar der Fall, aber in der Praxis kommt es häufig vor, dass fertiggestellte Malware von einer anderen Person als dem Autor zum Einsatz gebracht wird. Fallen Autor der Malware und Initiator des Angriffs auseinander, sollten gegen beide rechtliche Schritte geprüft werden.
Eine weitere in Frage kommende Person wäre die Mitarbeiterin, die Krassgeballer im Netz verbreitet hat. Allerdings war das Herunterladen und Installieren von Software aus dem Internet nicht verboten. Und da die Firewall Krassgeballer ohne weiteres durchgelassen hat und die Benutzung des Programms auch von der Firma nicht verboten wurde, kann der Mitarbeiterin kein Vorwurf gemacht werden.
Bliebe noch der Firewalladministrator. Es ist zu klären, ob er die Konfiguration der Firewall ordnungsgemäß durchgeführt hat. Die fehlende Scannersignatur kann ihm nicht vorgeworfen werden, denn alle verfügbaren Signaturen werden ohnehin automatisch installiert. Auch die

Konfiguration an sich war nach der Sicherheitspolitik nicht fehlerhaft, da TCP Verkehr nach außen zulässig sein sollte.

5.3.5. Einfluss auf die Weiterentwicklung des Notfallkonzeptes

Das Notfallkonzept im vorliegenden Szenario hat die wesentlichen Punkte des Vorfalls gut abgedeckt. Es hat erfolgreich zu einer schnellen Abstellung des Vorfalls geführt, nachdem dieser erst einmal entdeckt war. Somit war eine Verbesserung des Notfallkonzepts durch die Arbeit des IRTs nicht notwendig und auch nicht zu erwarten.
Allerdings haben sich aus der Arbeit des IRTs, vor allem aus der Vorfallsanalyse, zahlreiche langfristige Maßnahmen ergeben. Teilweise hatten sie präventiven, teilweise auch behebenden Charakter einer Schadensbegrenzung. Diese Erkenntnis hat nun indirekt doch wieder Einfluss auf das Notfallkonzept. Sie hebt die Relevanz der Vorfallsanalyse besonders hervor, und die Ermöglichung einer detaillierten Vorfallanalyse unter anderem durch die Sicherung der Spuren ist Teil eines Notfallkonzeptes, war aber im vorliegenden Notfallkonzept noch nicht enthalten. Dort war die Vorfallsanalyse bislang nur insoweit enthalten, dass herausgefunden werden sollte, wann die Leitungen gefahrlos wieder geöffnet werden können.

5.3.6. Fazit

In diesem Szenario war von vorn herein ein erfolgreiches Notfallkonzept modelliert worden. Das Szenario hat gezeigt, dass sich dennoch Verbesserungsmaßnahmen ergeben können, auch wenn der Vorfall durch das Notfallkonzept insgesamt gut verarbeitet wurde. Zudem ist erneut die Priorität langfristiger Maßnahmen klar geworden, die über das Notfallkonzept hinausgehen. Zwischen kurzfristigen und langfristigen Maßnahmen bestehen Wechselwirkungen, und die einen können nicht nur Einfluss auf die anderen haben, sondern bei der Abarbeitung können sich auf Verbesserungsmöglichkeiten für den jeweils anderen Bereich ergeben.

5.4. Unfall: Brand im HQ Rechenzentrum

Das vierte Szenario modelliert einen Unfall, einen Brand im Rechenzentrum. Wie bereits im ersten Kapitel dargestellt, geht eine Vielzahl von Vorfällen auf Unfälle zurück und nicht auf Angriffe. Ein Brand ist ein klassischer Unfall, der in der Realität häufig vorkommt, weshalb für ihn unbedingt ein Notfallkonzept vorhanden sein sollte.

5.4.1. Vorstellung des Szenarios

Für dieses Szenario wird erneut das Rechenzentrum des Firmenhauptquartiers mit der bekannten Architektur verwendet. Dabei wird die bereits bekannte Modellierung um die physikalischen Schutzmaßnahmen ergänzt, wie beispielsweise Brandschutztüren. Zudem wird die Bauweise des Rechenzentrums näher modelliert.

Das Feuer entsteht in einem größeren Raum des Rechenzentrums durch einen Sonnenstrahl, der durch eine unachtsam liegen gelassene Linse gebrochen ein Papierdokument in Brand setzt. Innerhalb des großen Raumes breitet es sich schnell aus, greift jedoch aufgrund der Brandschutzmaßnahmen nicht auf das gesamte Rechenzentrum über.
Ein wichtiger Aspekt dieses Szenarios liegt darin, dass ein IRT bei einem Vorfall der hier modellierten Art an die Grenzen seiner Zuständigkeit gelangt. Das Aufgabenfeld der IRTs wird in der Regel auf die Vorfälle begrenzt, die durch die Arbeit an einem Rechner oder Rechnernetz selber entstehen. Physikalische Einflüsse, deren Ausgangspunkt außerhalb der digitalen Welt liegen, werden von den meisten IRTs zwar angesprochen, aber selten wird ihre unmittelbare Bekämpfung direkt als Dienstleistung angeboten. Vielmehr liegt die Aufgabe des IRTs in der Behebung der Schäden, soweit sie den digitalen Bereich betreffen. Die Vorfallsanalyse und die Beseitigung der physikalischen Schäden werden von anderen Stellen übernommen.
Die IT bezogenen Werte, die durch den Brandunfall bedroht werden, umfassen hauptsächlich die Hardware der Rechner und die auf ihnen gespeicherten Daten. Beim entstehenden Schaden handelt es sich um Herabsetzung der Verfügbarkeit, denn die Rechner und Daten werden durch das Feuer beschädigt oder zerstört. Ein Vertraulichkeitsverlust muss aus nahe liegenden Gründen nicht diskutiert werden. Er könnte aber nach dem Vorfall entstehen, wenn die Schutzmaßnahmen durch das Feuer zerstört wurden. Ein Integritätsverlust käme in Betracht, wenn das Hauptquartier etwa Daten für Filialen speichert. Durch Verlust dieser Daten wäre der Datenbestand der Filialen nach dem Brand inkonsistent, was einen Integritätsverlust bedeutet.
Neben den Schäden an den IT Systemen und Daten sind hier wesentlich physikalische Werte bedroht. Dazu gehören das Gebäude des Rechenzentrums selber, die Einrichtungsgegenstände und auch physikalische Dokumente, wie etwa Ordner mit Papierakten. Zudem gehören maßgeblich die Mitarbeiter der Firma zu den bedrohten Werten, denn sie können durch das Feuer verletzt oder getötet werden.
Aus diesen möglichen primären Schäden leiten sich eine ganze Reihe von sekundären Schäden ab. Der Wiederaufbau zerstörter oder beschädigter Gebäude oder die Arbeiten, um die ausgebrannten Räume wieder nutzbar zu machen, erfordern nicht nur Geld, sondern auch Zeit. Während dieser Zeit können nur erschwert Gewinne erwirtschaftet werden. Falls Mitarbeiter durch den Brand dauerhafte Schäden davontragen, sind sie nicht mehr zur vollen Arbeitsleistung fähig. Auch ein Imageverlust nach einem Brand ist ein wahrscheinlicher sekundärer Schaden.

5.4.2. Technischer Aufbau und Art des Vorfalls

- Systeme

Für die Systeme müssen in diesem Szenario vor allem die physikalischen Aspekte modelliert werden und nicht so sehr die digitalen. Auch die Anordnung der Rechner im Rechenzentrum sei unter der Kenngröße Systeme beschrieben.
Wie in den vorangegangenen Szenarien umfasst das Rechenzentrum im Wesentlichen den Fileserver, den Personalserver und eine Reihe von Workstations. Die wichtigen und wertvollen Daten, mit denen die Mitarbeiter arbeiten, sind auf dem Fileserver gespeichert. Auf den Workstations werden die Daten während der Arbeit zwischengespeichert, sollen aber von jedem Mitarbeiter nach Beendigung der Arbeit an ihnen auf den Fileserver zurück geschrieben werden. Auf dem Personalserver sind die Personaldaten gespeichert, und er dient gleichzeitig der Personalsachbearbeiterin als Workstation. Die Firewallrechner und das Fluttor sind im Wesentlichen baugleich mit den Workstations.
Alle Rechner haben lokale Festplatten im Gehäuse, auf denen die Daten gespeichert werden. Die Hardware besteht im Wesentlichen aus Metall und brennbarem Kunststoff. Beim Verbrennen der Hardware entstehen giftige Stoffe, die beim Einatmen dauerhafte Gesundheitsschäden hervorrufen können. Die genauen Auswirkungen dieser Stoffe seien hier nicht modelliert, da keine gesundheitliche Studie vorgenommen werden soll. Die Leitungen des Rechnernetzes sind in Kunststoffstoffrohren unter dem Boden des Rechenzentrums verlegt. Dieser Raum unter den Bodenplatten ist etwa 30cm hoch und beinhaltet neben den Datenleitungen auch Stromleitungen und an einigen Stellen Wasserrohre.
Die Workstations befinden sich alle in einem gemeinsamen großen Raum im ersten Stock des Firmengebäudes. Die Parzellen der Mitarbeiter sind durch leichte Stellwände voneinander getrennt, die im Wesentlichen aus Korkplatten bestehen. Die Mitarbeiter befestigen an ihnen Dokumente und andere Papiere. Der Fußboden besteht aus Linoleumplatten, die mit Teppichläufern belegt sind. Unter dem Linoleum befindet sich der Hohlraum mit den Leitungen, darunter wiederum ein fester Boden aus Stahlbeton. Die Wände sind gestrichen, aber nicht verputzt oder tapeziert, ebenso die Decke. Dieses Großraumbüro, das bereits ein sehr alter Bau ist, verfügt nicht über Rauchmelder oder eine Sprinkleranlage. Die äußeren Türen des Raums sind Brandschutztüren, die einem Feuer innerhalb des Raumes standhalten können, wenn sie geschlossen sind. Eine dieser Brandschutztüren führt auf den Flur, eine zweite in einen separaten Raum, in dem der Fileserver steht. Dieser Raum hat die gleiche Architektur wie das Großraumbüro, ist nur wesentlich kleiner. Dieser Serverraum ist nur durch diese Brandschutztür zu erreichen, somit muss das Großraumbüro des Rechenzentrums durchquert werden, um zum Fileserver zu gelangen. Eine dritte Brandschutztür führt in einen weiteren, separaten Raum, in dem sich die Firewalls, der Webserver auf einem eigenen Rechner und der Rechner mit dem Fluttor befinden. Auch dieser Raum kann nur durch das Großraumbüro betreten werden.

Auf dem Flur liegen zahlreiche Räume, hauptsächlich die Büros der Firmenverwaltung. Diese Räume sind vom Flur durch normale Türen getrennt, nicht durch Brandschutztüren. Einer der Räume ist das Büro der Personalsachbearbeiterin, in dem auch der Personalserver steht. Der Flur führt zudem durch eine weitere Brandschutztür ins Treppenhaus. Diese Brandschutztür ist neben der zum Rechenzentrum die einzige Brandschutztür, die vom Flur abzweigt.
Vom Treppenhaus führt eine Treppe ein Stockwerk nach unten in die Eingangshalle der Firma.
Im Großraumbüro halten sich während der Arbeitszeit immer einige Mitarbeiter auf. Die Personalsachbearbeiterin befindet sich meistens in ihrem Büro. Im Raum mit dem Fileserver und im Raum mit den Firewalls hält sich im Regelfall niemand auf. In allen Räumen befindet sich außerdem jede Menge Büroausstattung, die größtenteils brennbar ist.

- Backups

Backups werden von den Personaldaten und von den Daten auf dem Fileserver angelegt. Sie werden in Form von Festplattenimages auf CDs abgespeichert. Da diese CDs aus Kunststoff bestehen, können sie leicht durch Feuer zerstört werden.
Die Backups werden zweimal pro Woche angelegt, immer montags und donnerstags um 20.00 Uhr, nach dem Ende der normalen Arbeitszeit. Für das Anlegen der Backups ist der Administrator zuständig. Er brennt die Backups auf einem jeweils in den Servern integrierten CD Brenner und lagert sie in einem speziellen Lagerraum im Keller der Firma. Dort werden die Backups eines halben Jahres aufbewahrt, danach werden sie vernichtet.
Zum Wiedereinspielen eines Backups muss das Image des jeweiligen Servers auf die Platte zurückgespielt werden. Dies setzt voraus, dass die Platte noch intakt ist. Zudem kann ein Austausch der Festplatte das Backup eventuell unbrauchbar machen, da das Image und die neue Festplatte nicht mehr zusammenpassen.

- Zugriffsrechte

Es gelten im Wesentlichen die Zugriffsrechte, die bereits in den vorangegangenen Szenarien modelliert wurden. Jeder Mitarbeiter hat auf seiner jeweiligen Workstation Benutzerrechte. Zudem hat er auf dem Fileserver ein eigenes passwortgeschütztes Verzeichnis und außerdem Zugriff auf ein öffentliches Verzeichnis. Auf dem Personalserver hat die Personalsachbearbeiterin Benutzrechte.
Der Administrator hat auf allen Rechnern im Netz Administratorrecht, aber keine Benutzerrechte. Als einziger hat er Zugriff auf die Firewalls und das Fluttor. Der Webserver wird von einem speziellen Mitarbeiter betreut, der deshalb ein Administratorrecht auf dem Rechner des Webservers hat.

- Mitarbeiterkompetenzen

Die Modellierung spezieller Mitarbeiterkompetenzen ist in diesem Szenario nur soweit erforderlich, dass es nur einen Administrator gibt, der regelmäßig die Backups anlegt. Falls dieser Administrator ausfällt, übernimmt ein Mitarbeiter seine Stellvertretung. Allerdings ist dieser Mitarbeiter nicht in den administrativen Tätigkeiten ausgebildet und sammelt in der Regel lediglich die Informationen über Vorkommnisse im Netz für den eigentlichen Administrator und übergibt sie ihm, sobald dieser wieder zur Verfügung steht. Auch das Anlegen der Backups liegt während dieser Zeit brach.

- Sicherheitspolitik

Die Sicherheitspolitik zur Brandvermeidung umfasst in erster Linie ein absolutes Rauchverbot innerhalb des Rechenzentrums und den meisten anderen Teiles des Gebäudes. Lediglich in der Kantine im Erdgeschoss ist es gestattet. Außerdem ist das hantieren mit offenem Feuer im Rechenzentrum ebenfalls nicht gestattet. Verboten sind also beispielsweise Kerzen, das Benutzen von Feuerzeugen, Streichhölzern usw.
Ferner sind die Brandschutztüren stets beschlossen zu halten. Die Sicherheitspolitik ist in der Firma kommuniziert worden, allerdings wird ihre Einhaltung nicht durch besondere Maßnahmen durchgesetzt.

- Konfiguration der Firewalls

Da in diesem Szenario kein Netzverkehr modelliert wird, ist eine Ausgestaltung der Firewallkonfiguration nicht nötig.

- Konfiguration der Fluttore

Auch die Konfiguration der Fluttore braucht nicht betrachtet zu werden.

- Weitere Kenngrößen

Die Firma hat eine Feuerversicherung abgeschlossen, die Gebäudeschäden abdeckt. Zudem ist ein Umbau der Räumlichkeiten geplant, der einen besseren Feuerschutz ermöglichen soll. Geplant sind unter anderem Sprinkleranlagen, Rauchmelder sowie der Verteilung von Handfeuerlöschern im Rechenzentrum.

An einem Mittwochmorgen im Hochsommer sitzt ein Mitarbeiter der Firma am Frühstückstisch mit seinen beiden Kindern. Diese bearbeiten in der Schule gerade das Thema der Lichtbrechung, und um seinen Kindern dazu Anschauungsunterricht zu geben, verspricht der Familienvater, seinen Kindern nach der Arbeit eine Lupe mitzubringen.
Auf dem Weg in die Firma hält der Mitarbeiter kurz an einem Kiosk und kauft eine kleine Kunststofflupe. In der Firma angekommen legt er seine Tasche mit seinem Tagesgepäck wie gewohnt hinter sich auf einen kleinen Abstelltisch, auf dem er auch seine Dokumente

aufbewahrt, wenn er an ihnen arbeitet. Als es Zeit für die Frühstückspause wird, nimmt er sein zu Hause geschmiertes Butterbrot aus der Tasche und begibt sich zu seinen Kollegen in die Teeküche, die sich in einer Ecke des Büros befindet. Beim Herausnehmen des Brotes rollt die Lupe aus der Tasche und bleibt auf den Dokumenten liegen. Da der Arbeitsplatz des Mitarbeiters sich unter einem Fenster befindet, fallen die Strahlen der Sonne durch die Lupe direkt gebündelt auf den Dokumentenstapel. Nach kurzer Zeit fangen die Dokumente Feuer.
Da die Kollegen sich in der Teeküche befinden, bemerkt zunächst niemand das Feuer, zumal ein Großteil des Rauches durch die geöffneten Fenster nach draußen entweicht. Schnell steht die gesamte Parzelle in Brand. Als die Mitarbeiter den Brand schließlich doch bemerken, ist es für einfache Löschversuche zu spät, da nirgendwo Feuerlöscher zur Verfügung stehen. Also wird, wie angeordnet, der Pförtner alarmiert und das Büro schnellstens verlassen. Die Brandschutztüren fallen automatisch zu, weshalb die recht panischen Mitarbeiter nicht darauf achten müssen, diese hinter sich zu schließen.
Der Pförtner alarmiert die Feuerwehr. Sicherheitshalber wird auch der Rest des Gebäudes geräumt. Da an jedem Morgen der Berufsverkehr die Straßen blockiert, benötigt die Feuerwehr zum Anrücken fast eine halbe Stunde. Zu diesem Zeitpunkt steht das Großraumbüro bereits komplett in Flammen. Zwar kann die Feuerwehr den Brand relativ schnell unter Kontrolle bringen und schließlich löschen, doch der große Raum des Rechenzentrums ist völlig zerstört. Die Firmenleitung beauftragt ein IRT und andere Sachverständige mit der Aufklärung des Vorfalls und der Schadensbehebung.

5.4.3. Bestehendes Notfallkonzept

Bei Notfallkonzepten für Brandunfälle tritt der Aspekt der unmittelbaren Notfallbekämpfung in den Vordergrund. Durch ein Feuer können zahlreiche Werte innerhalb kürzester Zeit vernichtet werden, und im Gegensatz zu den in den ersten drei Szenarien modellierten Vorfällen stehen hier auch Menschenleben auf dem Spiel, die vorrangig vor allen anderen Werten zu schützen sind.
Der Aspekt der Wiederherstellung der Verfügbarkeit ist dennoch ebenfalls von großer Bedeutung, da durch das Feuer die Verfügbarkeit einzelner Systeme oder des gesamten Rechnernetzes als ganzes stark herabgesetzt sein kann. Dabei brauchen die Systemteile nicht einmal zerstört oder beschädigt worden zu sein. Es genügt zur Herabsetzung der Verfügbarkeit einer Ressource beispielsweise bereits, dass das Feuer den Zugangsweg zu dieser Ressource blockiert.
Neben den Maßnahmen des Notfallkonzepts sind auch langfristige Maßnahmen zur Bearbeitung des Vorfalls zu ergreifen. Beispielweise müssen die ausgebrannten Gebäudeteile von Giftstoffen gereinigt werden. Ferner müssen die Gebäudeteile stabilisiert oder schlimmstenfalls neu aufgebaut werden. Falls Mitarbeiter verletzt oder getötet wurden, müssen Ersatzkräfte eingestellt werden. Zahlreiche weitere Beispiele ließen sich finden.

Ferner können aus dem Vorfall Erfahrungen gewonnen werden, wie der Brandunfall sich in Zukunft vermeiden ließe. Somit existiert hier ein Vorfall, bei dem alle drei Stufen von Gegenmaßnahmen eine große Bedeutung haben (vgl. Abbildung 11 in Abschnitt 5.2.6.).
Es folgt nun die Darstellung des Notfallkonzepts für dieses Szenario. Da bei einem Brandvorfall in der Regel die Zeit eine besonders große Rolle spielt, ist der Brand zunächst dem Pförtner zu melden, der in der Firma unter anderem die Aufgabe hat, entsprechende Meldungen schnell in der ganzen Firma zu verbreiten. Die Mitarbeiter sollen den Brand bei unmittelbarer Gefahr bekämpfen, ansonsten ist der vom Brand betroffene Gebäudeteil zu evakuieren (Motto: „Das Leben geht vor“). Bei größeren Bränden sollen alle Mitarbeiter das Gebäude verlassen.
Der Pförtner alarmiert nicht nur den Rest der Firma, sondern verständigt auch die Feuerwehr. Sobald die Löscharbeiten beendet sind und das Gebäude wieder begehbar ist, sollen die Aufklärungsarbeiten beginnen. Vor allem die Brandursache soll geklärt werden, damit das Gebäude oder der Gebäudeteil in Zukunft besser vor Feuer geschützt werden kann. Parallel dazu sollen die betroffenen Infrastrukturteile wieder einsatzbereit gemacht werden. Eventuell sollen mit Ersatzrechnern Notnetze in anderen Gebäudeteilen aufgebaut werden. Falls die Server beschädigt oder zerstört sind, sollen mit Ersatzmaschinen und den Backups ebenfalls Notserver eingerichtet werden.
Nach Abarbeitung dieses Notfallkonzepts beginnt die zweite Stufe der Gegenmaßnahmen, die langfristige Vorfallsbearbeitung. Sie umfasst vor allem die oben beschriebenen Maßnahmen zur Gebäudesicherung und den Ersatz ausgefallener Mitarbeiter. Ziel dieser Stufe ist die allmähliche Wiederherstellung des Normalzustandes. Schließlich werden am Schluss die Erkenntnisse aus der Vorfallsbearbeitung ausgewertet, um eine bessere Brandprävention und –Bekämpfung zu etablieren.

5.4.4. Arbeit und Ergebnisse des IRTs

- Incident Analysis

Die Vorfallsanalyse, wie auch die meisten anderen Dienstleistungen, wird sich das IRT mit anderen Einrichtungen teilen. Das IRT wird den Vorfall nur insoweit untersuchen, wie er Einfluss auf die IT Systeme hat. Da aus nahe liegenden Gründen bekannt ist, dass es sich um einen Brandvorfall handelt, kann die Ermittlung der Vorfallsursache durch das IRT entfallen. Die Ermittlung der Brandursache ist natürlich wichtig, wird aber nicht vom IRT durchgeführt und hat keinerlei Auswirkungen auf die IT Systeme. Für den dort entstandenen Schaden ist es egal, wodurch der Brand verursacht wurde.
Das IRT wird also untersuchen, welche Teile des IT Netzes beschädigt wurden. Diese Untersuchung legt ihren Schwerpunkt zunächst auf die Hardware. Wenn bekannt ist, welche Rechner, Netzleitungen und anderen Hardwarekomponenten beschädigt sind, kann in einer zweiten Stufe der Analyse ermittelt werden, welche Funktionen das Netz noch wahrnehmen kann und welche nicht. Auch die Fähigkeit, das gewünschte Sicherheitsniveau wahren zu

können, ist dabei eine wichtige Funktion. Denn der Brandvorfall wird im Regelfall über die Presse publiziert und könnte Angreifern einen Anlass zu einer Attacke geben. In diesem Szenario sind die Firewalls und das Fluttor vom Vorfall nicht betroffen, so dass gegen Angriffe aus dem Internet und gegebenenfalls den Zweigstellen noch immer das übliche Sicherheitsniveau existiert. Andererseits bestehen von anderen Seiten durchaus Gefahren für weitere Sicherheitsvorfälle, die es ohne den Brand nicht gegeben hätte. Beispiele hierfür sind die Möglichkeit von Plünderungen in den ausgebrannten Gebäudeteilen (eventuell durch die Mitarbeiter), verstärkte Gefahr durch Angriffe von innen (falls die Notrechner ein geringeres Sicherheitsniveau haben als das normale Netz) oder die Gefahr des Vertraulichkeitsverlusts geheimer Daten, weil diese ohne den physikalischen Schutz des Gebäudes leichter zugänglich sind. Weitere Beispiele ließen sich finden. Die Analyse ergibt, dass lediglich die Workstations im Großraumbüro vom Brand zerstört wurden, da die Server, Firewalls und das Fluttor hinter den Brandschutztüren in Sicherheit sind und auch während der Löscharbeiten unbeschädigt blieben. Allerdings sind Fileserver, Firewalls, Webserver und Fluttor aufgrund der Bauweise des Rechenzentrums nach dem Vorfall nicht mehr physikalisch zugänglich.
Neben der Arbeit des IRTs leisten auch andere Institutionen ihren Beitrag zur Vorfallsanalyse. So wird etwa die Polizei die Brandursache untersuchen. Auch die Statik der Gebäude muss untersucht werden. Die Firma selbst wird eine Inventur der beschädigten Einrichtung vornehmen. Mitarbeiter müssen auf körperliche und seelische Schäden und Folgeschäden untersucht werden. Diese Punkte haben jedoch nur wenig Einfluss auf die Sicherheit des IT Netzes und sollen hier nicht vertieft werden.

- Reinigung

Die Reinigung der Systeme im Sinne des Abschnitt 3.2. ist hier nicht zielführend, da der Zugriff auf die Systeme nicht digital erfolgte. Die Wahrscheinlichkeit, dass das Feuer Daten auf einem Speichermedium verändern kann, ohne das Medium zu zerstören, ist äußerst gering.
Allerdings müssen zahlreiche Systeme wiederhergestellt werden. Da die Hardware aber durch den Brand zerstört wurde, fällt diese Maßnahme in den Bereich der Gegenmaßnamen. Lediglich eine einfache Neuinstallation oder das Einspielen eines Backups wäre eine Reinigungsmaßnahme.
Außerhalb der Zuständigkeit des IRTs müssen allerdings physikalische Reinigungsmaßnahmen vorgenommen werden. Beispielsweise müssen die Firmengebäude von Giftstoffen und Brandschutt gereinigt werden.

- Vermeidung

Ähnliches wie für die Reinigung gilt auch für die Vermeidung. Mit „digitalen“ Maßnahmen kann nur sehr wenig getan werden, um einen weiteren Brandvorfall zu verhindern. Das IRT kann allerdings gemeinsam mit Brandschutzberatern aufgrund der bekannten chemischen

Zusammensetzung von Rechnersystemen Vorschläge für physikalische oder organisatorische Präventivmaßnahmen abgeben. Dazu muss es eng mit der Firma zusammenarbeiten, um die momentanen Prozessabläufe und architektonischen Gegebenheiten in der Firma zu verstehen. Auf jeden Fall leistet das IRT hier höchstens unterstützende Arbeit.
Die meisten Präventivmaßnahmen, die für eine bessere Brandvermeidung geeignet sind, sind physikalischer Natur und ergeben sich aus der Untersuchung, wie der Brand entstanden und abgelaufen ist. So könnten beispielsweise im Rechenzentrum Feuerlöscher verteilt werden, mit denen sich ein größerer Brand verhindern ließe. Demselben Zweck diente eine Anlage, um den Raum nach der Evakuierung der Mitarbeiter mit Kohlendioxid zu fluten. Sprinkleranlagen sind aufgrund der vielen elektronischen Geräte eher ungeeignet. Anzudenken wäre auch, den einzelnen großen Raum in mehrere kleine Räume aufzuteilen, die durch weitere Brandschutztüren voneinander getrennt sind. Auch könnte die Menge brennbaren Materials in den Räumen verringert werden. So könnten etwa die Korkwände durch Metallaufsteller ersetzt werden, an denen die Notizen statt mit Stecknadeln mit Magneten befestigt werden könnten.
Andere Präventivmaßnahmen wären organisatorischer Art. So könnte das Lagern brandgefährdender Gegenstände (wie etwa Brenngläsern) im Rechenzentrum generell verboten werden. Das bereits vor dem Vorfall erteilte Rauchverbot fällt ebenfalls in diese Kategorie.

- Gegenwehr

Die wichtigste Maßnahme der Gegenwehr ist das Aufbauen des Notnetzes, bei dem das IRT die Firma sehr gut unterstützen kann. Vor allem muss ein ausreichendes Sicherheitsniveau auch im Notnetz gewährleistet sein. Es kann aber wie im Abschnitt 1.5. angesprochen eventuell niedriger als das normale Sicherheitsniveau sein.
Maßnahmen zur unmittelbaren Notfallbekämpfung werden in diesem Szenario nicht vom IRT ergriffen, sondern hauptsächlich von der Feuerwehr. Aber auch die im Notfallkonzept verankerte Kommunikation der Notfallsituation gehört in diese Kategorie.
Eine Gegenwehrmaßnahme, die nicht mehr Teil des Notfallkonzeptes ist, ist etwa der Wiederaufbau der Gebäudeteile.

- Rechtliche Schritte

Auch die rechtlichen Schritte sind in diesem Szenario zwar wichtig, aber nicht Aufgabe des IRTs. Die digitale Spurensicherung, wie in Abschnitt 3.6. beschrieben, macht hier keinen Sinn, da der Vorfall nicht über die IT Systeme verursacht wurde.
Vielmehr wird das ausgebrannte Rechenzentrum auf physikalische Spuren untersucht werden, die zu demjenigen führen, der den Brand verursacht hat. An dieser Stelle soll für das Szenario nicht modelliert werden, ob diese Suche erfolgreich ist. Üblicherweise lässt sich aber zumindest die Brandursache in ähnlichen Vorfällen recht häufig ermitteln.

5.4.5. Einfluss auf die Weiterentwicklung des Notfallkonzeptes

Dieses Szenario bietet vor allem zwei Neuerungen, die es in den ersten drei Szenarien noch nicht gab. Einerseits spielen alle drei zeitlichen Stufen von Gegenmaßnahmen aus Abbildung 11 eine Rolle, andererseits hat das IRT bei der Bearbeitung des Vorfalls nur unterstützende Funktion. Somit können die Gegenmaßnahmen auf allen Zeitstufen durch die Vorfallsbearbeitung noch verbessert werden, und diese Vorschläge kommen größtenteils nicht vom IRT.

Auf der Stufe der langfristigen Präventivmaßnahmen, die nicht mit dem konkreten Vorfall verflochten sind, sind vor allem die schon geschilderten physikalischen Maßnahmen als Verbesserungsmöglichkeiten zu nennen. Wie bei den Vermeidungsmaßnahmen erwähnt, sind dies etwa Feuerlöscher, Kohlendioxidanlagen, Raumumgestaltung usw. Auch die organisatorischen Maßnahmen zählen hierzu.

Wurden diese Maßnahmen umgesetzt, kann ihr Gebrauch im Notfallkonzept verankert werden. Somit wird die unmittelbare Notfallbekämpfung mit Feuerlöschern und nach der Evakuierung mit Kohlendioxid ins Notfallkonzept aufgenommen. Ein Umbau der Räumlichkeiten kann auch den nicht näher modellierten Evakuierungsplan beeinflussen.

Bleiben noch die langfristigen Maßnahmen. Hier können hauptsächlich die Abläufe im Einzelfall verbessert werden, falls etwa der Wiederaufbau eines Gebäudeteils sich aus irgendeinem Grund verzögert. Da diese Aspekte hier nicht modelliert wurden, soll aber nicht näher darauf eingegangen werden.

5.4.6. Fazit

Die Haupterkenntnis aus diesem Szenario besteht in zwei Teilen. Zum einen gibt es Vorfälle, in denen die IT massiv bedroht ist, deren Bearbeitung ein IRT aber schnell an seine Grenzen führt. Zum anderen können Notfallkonzept und andere Gegenmaßnahmen nicht nur durch überwiegend das IRT, sondern auch von anderer Seite beeinflusst und verbessert werden. Ansonsten liegt hier ein Beispiel dafür vor, dass auf jeder der drei zeitlichen Ebenen Gegenmaßnahmen ergriffen werden müssen, wenn der Vorfall effektiv bearbeitet werden soll. Dies liegt vor allem daran, dass ein Brandvorfall nicht auf die IT und ihr unmittelbares Umfeld begrenzt ist (wie dies in den Vorfällen der ersten drei Szenarien der Fall war), sondern die Firma als ganzes bedroht. Mitarbeiter und physikalische Infrastruktur etwa waren in den ersten drei Szenarien nicht betroffen.

5.5. Unfall: Epidemie unter den Mitarbeitern

Das fünfte Szenario modelliert einen weiteren Unfall in der Firma: eine Epidemie unter den Mitarbeitern. Ähnlich wie der Brandvorfall aus dem letzten Szenario stellt auch die Epidemie ein natürliches Ereignis dar. Anders als in den bisherigen Szenerien werden aber nicht die Infrastruktur oder IT Systeme direkt bedroht, sondern die Mitarbeiter der Firma.

5.5.1. Vorstellung des Szenarios

In der Umgebung des Hauptquartiers der Firma grassiert eine neue, bislang unbekannte Krankheit. Die Ärzte haben ihr den Namen „Büroschlaf“ gegeben, weil hauptsächlich Personen, die in Büros und großen Räumen zusammen arbeiten, davon betroffen sind und eines der Symptome ein massiver Erschöpfungszustand ist.

Die übrigen Symptome der Krankheit sind hohes Fiber von teilweise 40 Grad, Durchfall, Schwindelgefühl und Appetitlosigkeit. Die Krankheit war ursprünglich eine Erkrankung des Weideviehs, was aber zu Beginn des Szenarios noch niemand weiß. Der Erreger, ein Virus, befällt den Menschen, wenn er das Fleisch infizierter Tiere isst oder mit diesen Tieren für längere Zeit Kontakt hat. Anschließend wird er durch Kontakt auch von Mensch zu Mensch übertragen. Allerdings hat die Krankheit bei den Weidetieren wesentlich schwächere Symptome, so dass ein erkranktes Tier unter den gesunden Tieren so gut wie nicht auffällt.

Der primär bedrohte Wert in diesem Szenario ist die Gesundheit der Mitarbeiter. Davon unmittelbar abhängig sind die Moral und die Arbeitskraft der Mitarbeiter. Ein Schaden an der Gesundheit der Mitarbeiter lässt sich allerdings nur schwer in die Kategorien von Vertraulichkeit, Verfügbarkeit und Integrität einordnen, da diese Kategorien eher für IT Systeme, Ressourcen und Daten geschaffen wurden und eine Übertragung auf menschliche Lebewesen unangebracht erscheint. Am ehesten ist der Ausfall eines Mitarbeiters als Verfügbarkeitsschaden zu klassifizieren, allerdings wird der Mitarbeiter durch eine solch starre Klassifikation von einer Person auf eine einfache Ressource reduziert. Eventuell mag daran gedacht werden, durch den Eingriff der Krankheit in den menschlichen Körper auch von einem Integritätsschaden zu sprechen.

Der Gesundheitsschaden und der daraus resultierende Arbeitsausfall führen zu sekundären Schäden. Verlust von Gewinnen und Kunden durch mangelnde Betreuung der Geschäftsprozesse sind als erstes zu nennen, aber es können noch weitere sekundäre Schäden auftreten. Durch den Ausfall der Mitarbeiter kann die Infrastruktur und damit auch das Netz der IT Systeme weniger gut gewartet werden, was das Sicherheitsniveau senken kann. Dies kann zu Sicherheitsverletzungen führen, wenn etwa ein Angreifer die Situation ausnutzt oder ein durch einen anderen Vorfall entstandener Schaden wegen mangelnder Arbeitskraft nicht verhindert oder behoben werden kann. Zudem kann der Ausfall von Mitarbeitern auch das Notfallkonzept eines beliebigen Vorfalls nutzlos werden lassen, wenn für die Durchführung des Konzepts nicht mehr genug Mitarbeiter zur Verfügung stehen.

Aus diesen Überlegungen folgt die Erkenntnis, dass eine Epidemie besonders dann für die Firma gefährlich ist, wenn sie mit anderen Vorfällen gekoppelt auftritt. Deshalb wird hier nach der Modellierung des Epidemievorfalls an sich auch ein Ausblick dafür gegeben werden, welche weiteren Gefahren sich daraus für die Firma ergeben. Dieser Ausblick wird in der Beschreibung des Szenarioablaufs erfolgen.

5.5.2. Technischer Aufbau und Art des Vorfalls

Wie gewohnt folgen nun zunächst die Festlegung der Kenngrößen und danach die Ablaufbeschreibung.

- Systeme

Für den Epidemievorfall selbst sind die IT Systeme nicht relevant, da sie durch ihn nicht direkt betroffen werden. Wird allerdings durch den Mangel an Arbeitskraft die Beherrschbarkeit und Administrierbarkeit der Systeme bedroht, ist der Aufbau der Systeme dennoch von Belang.

Der Aufbau des Netzes im Hauptquartier stimmt im Wesentlichen mit dem Netzaufbau aus dem zweiten und dem dritten Szenario überein. Der größte Teil des Netzes wird von Workstations gebildet, von denen jeder Mitarbeiter eine eigene nutzt. Die Workstations verfügen über lokale Platten, auf denen die Arbeitsdaten gespeichert werden. Zudem haben sie Internetzugang über die beiden Firewalls. Auf allen Workstations läuft dasselbe Betriebssystem, und auch die Hardware ist gleich.

Der Personalserver und der Fileserver haben die gleiche Bauart wie die Workstations. Lediglich die Festplatte ist größer, um genug Platz für die gelagerten Daten zur Verfügung zu stellen. Beide Server verfügen je über einen CD Brenner zum Erstellen von Backups.

Die beiden Firewalls und das Fluttor befinden sich ebenfalls auf Rechnern der Workstation-Bauart, allerdings ist nur die minimal nötige Software installiert, um die Firewalls zu betreiben. Es wird dasselbe Betriebssystem wie im ganzen Netz verwendet.

- Backups

Die Daten auf den beiden Servern werden einmal pro Woche als Backups gesichert. Dies erfolgt am Freitag um 17.00 Uhr, wenn die normalen Arbeitszeiten beendet sind. Zum Erstellen der Backups werden die zu sichernden Daten auf eine CD gebrannt, die anschließend im Keller der Firma gelagert wird. Da die CDs nur wenig Platz wegnehmen, lagern im Keller der Firma Backups aus mehreren Jahren.

- Zugriffsrechte

Für das Erstellen der Backups ist grundsätzlich der Netzadministrator zuständig. Die Netzorganisation kennt nur eine Administratorrolle, die alle administrativen Aufgaben übernimmt: Installation, Konfiguration, Wartung, Problembehandlung, Sicherheitsadministration, Backups usw.

Auf den einzelnen Workstations kann die Anmeldung als Benutzer erfolgen, um mit den auf der Workstation gespeicherten Daten zu arbeiten, mit dem Internet zu kommunizieren oder mit den Daten auf dem Fileserver zu arbeiten. Der Personalserver bietet diese Workstationfunktionalität ebenfalls. Zudem hat jede Workstation ein Administratorkonto, das

im Gegensatz zum Benutzerkonto administrative Arbeit zulässt, aber nicht die eben geschilderten Benutzerarbeiten.
Auf dem Fileserver befinden sich für jeden Benutzer ein passwortgeschütztes Verzeichnis und ein öffentliches Verzeichnis. Auch hier gibt es ein Administratorkonto mit denselben Möglichkeiten wie bei den Workstations. Der Personalserver hat neben Benutzerkonto und Administratorkonto noch ein Sachbearbeiterkonto, das Zugriff auf die Daten und die Bearbeitungssoftware auf dem Personalserver erlaubt.
Die Firewalls und das Fluttor haben nur ein Administratorkonto, mit dem die Rechner selber und die Firewallsoftware administriert werden können.

- Mitarbeiterkompetenzen

Jeder Benutzer hat auf seiner Workstation Benutzerrechte. Zudem hat die Personalsachbearbeiterin sowohl Benutzerrechte als auch Sachbearbeiterrechte auf dem Personalserver. Im gesamten Hauptquartier gibt es nur einen Netzadministrator, der sich mit den Aufgaben der Administration wirklich auskennt und auf allen Rechnern Administratorrechte hat. Für den Fall seines Ausfalls übernimmt ein Mitarbeiter seine Stellvertretung. Dieser sammelt allerdings in der Regel nur eingehende Meldungen und legt die Backups an. Sobald der Administrator wieder da ist, arbeitet er dann die eingegangenen und katalogisierten Meldungen ab.

- Sicherheitspolitik

Da eine grassierende Krankheit unter den Mitarbeitern der Firmenleitung als äußerst abwegig erscheint, wird diese Gefahr in der Sicherheitspolitik nicht berücksichtigt. Für die IT Systeme gelten jedoch die in den Szenarien zwei und drei aufgestellten Richtlinien. Die Daten auf den Servern und Workstations sind verfügbar, integer und vertraulich zu halten. Diese Vorgaben sollen mit dem Passwortschutz und den Firewalls umgesetzt werden (vgl. Abschnitte 5.2.3. und 5.3.3. zur Sicherheitspolitik).
Ansonsten soll die Sicherheitspolitik für dieses Szenario nicht näher modelliert werden, da hier das Ziel verfolgt wird, die Bandbreite der möglichen Folgen einer Epidemie aufzuzeigen und nicht einen bestimmten Folgevorfall im Detail zu untersuchen.

- Konfiguration der Firewalls

Die Filtermechanismen der Firewalls arbeiten mit dem Prinzip des generellen Verbots und sind für den benötigten Netzverkehr prinzipiell korrekt konfiguriert. Allerdings ist die Firewallsoftware schon seit mehreren Jahren im Einsatz, weshalb es eine Fülle von inaktiven und optional zuschaltbaren Regeln gibt, die nur im Bedarfsfall aktiviert werden. Einige Regeln werden auch überhaupt nicht mehr gebraucht und sind lediglich noch nicht endgültig gelöscht worden. Nur der Administrator hat Überblick über die Funktionen der einzelnen Regeln, allerdings hat er dieses Wissen nicht dokumentiert.

- Konfiguration der Fluttore

Die Konfiguration der Fluttore ist für dieses Szenario nicht von Belang, da über das Fluttor kein kritischer Netzverkehr modelliert werden soll. Als Folgevorfall der Epidemie wäre ein Angriff aus einem Zweigstellennetz denkbar, diese Möglichkeit soll aber nicht weiter verfolgt werden.

- Weitere Kenngrößen

Der Erreger des Büroschlafs ist Hitzeresistent und überlebt somit auch in durchgegartem Fleisch. Er gelangt mit einer Portion Rindergulasch in die Firma, das von einem verseuchten Hof stammt. Unter den Weidetieren grassiert die Seuche schon eine ganze Weile unbemerkt, und zahlreiche Großküchen und Firmenkantinen haben verseuchtes Fleisch verarbeitet.
Die Inkubationszeit des Büroschlafs beträgt 3-4 Tage. Die ersten Symptome sind Erschöpfung und Schwindelgefühl, später kommen Fieber, Durchfall und Appetitlosigkeit hinzu. Die Krankheit dauert unbehandelt ein bis zwei Wochen an. Danach sind die meisten Patienten allerdings durch den Verlust von Nährstoffen und Mineralien so geschwächt, dass sie eine einwöchige Aufbaukur benötigen, um wieder arbeitsfähig zu sein. Manche Patienten mit einer besonders schwachen Konstitution müssen sogar künstlich ernährt werden.
Zur Behandlung des Büroschlafs gibt es noch kein zugelassenes Medikament, da die Krankheit ganz plötzlich aufgetreten ist. Neben der Infektion über das Fleisch der Weidetiere kann die Krankheit sich auch durch Körperkontakt ausbreiten. Dazu reicht es aus, einige Zeit auf engerem Raum zusammen zu sein, wie etwa in einem Großraumbüro oder im Fall der Weidetiere in einem Stall.
Die Firma verfügt über ein firmeneigenes IRT, das alle Aufgaben eines IRT übernimmt, allerdings nur im Auftrag der Firma.

Es folgt nun der Ablauf des Szenarios. Während des Sommers breitet sich der Büroschlaf über Wochen hinweg unbemerkt unter den Weidetieren aus. Woher die Krankheit ursprünglich kommt und wie sie auf einmal die Weidetiere und später den Menschen befallen hat, wird zu wilden Spekulationen führen, soll hier aber nicht modelliert werden.
Einige Bauern wundern sich über Tiere, die scheinbar etwas antriebslos und müde sind. Da der Sommer aber sehr schwülwarm ist, halten die meisten Bauern das Wetter für Schuld. Einige lassen dennoch ihre Tiere untersuchen. Da die Krankheit aber noch unbekannt ist, führt die Untersuchung zu keinem Ergebnis.
Unerkannt befällt die Seuche viele Höfe. Die ersten an Büroschlaf erkrankten Menschen sind einige Bauern. Aufgrund der Ähnlichkeit der Symptome mit einer einfachen Magen-Darm-Erkrankung nimmt aber niemand Notiz davon. Schließlich gelangen die erkrankten Tiere zum Schlachten. Ein Großteil des Fleisches wandert in die Großküchen der Firmen. Einige Wochen später treten gehäuft Erkrankungen von Büroschlaf auf. Zunächst in einigen großen Firmen, dann auch in Privathaushalten. Auch die Firma des Szenarios ist davon betroffen.

Zunächst erkranken dort einige einfache Mitarbeiter. Sie werden nach Hause geschickt, und ihre Arbeit kann zu Beginn problemlos von den Kollegen miterledigt werden. Als jedoch fast ein Drittel der Belegschaft erkrankt ist, kommen die Geschäftsprozesse ins Stocken. Schließlich fällt auch der Administrator aus. Dies führt zu einer gefährlichen Konstellation für das Firmennetz: Zum einen wird das Netz nicht mehr korrekt administriert. Zum anderen bleiben eventuelle Fehlerfunktionen, Angriffe oder Anomalien unentdeckt, da die Mitarbeiter fehlen, die diese Dinge entdecken könnten.
Einige Mitarbeiter mit guter Konstitution kehren nach einer raschen Auskurierung in die Firma zurück. Manche stecken sich an dem offenbar hartnäckigen Virus erneut an und fallen wieder aus. Der Administrator wurde besonders schwer getroffen. Sein Körper wurde durch den Büroschlaf dermaßen geschwächt, dass er auf eine einmonatige Erholungskur geschickt werden muss.
Die Zustände im Netz des Hauptquartiers werden nach zwei Wochen ohne den Administrator allmählich unhaltbar. Zwar sammelt sein Stellvertreter alle eingehenden Meldungen über ungewöhnliche Ereignisse und zieht weiterhin die Backups, aber der reibungslose Ablauf der Arbeit ist empfindlich gestört. Die Firmenleitung wendet sich an das firmeneigene IRT und bittet um Beratung und um die Bereitstellung eines Ersatzadministrators...

Soweit der Ablauf des eigentlichen Epidemievorfalls. Die Hauptgefahr geht bei diesem Szenario nicht von der Epidemie selber aus, sondern von den Ausfällen, die sie verursacht. Durch sie werden einerseits die Geschäftsprozesse gestört, andererseits kann die Firma weniger gut auf andere Vorfälle reagieren oder diese überhaupt entdecken. An dieser Stelle werden einige Beispiele für zusätzliche Gefahren gegeben, denen die Firma aufgrund der Epidemie ausgesetzt ist. Dabei soll das Augenmerk auf Gefahren für die IT Systeme liegen.
Die fehlende Administration und die geringere Präsenz der Mitarbeiter steigert die Gefahr, dass ein Angriff auf das Netz großen Schaden anrichten kann. Die Wahrscheinlichkeit für einen Angriff von außen muss nicht zwangläufig höher ausfallen als normal, solange die Epidemie in der Firma nicht nach außen bekannt gegeben wird. Die Wahrscheinlichkeit eines Angriffs von innen nimmt allerdings zu, da korrupte Mitarbeiter diesen Moment der Schwäche ausnutzen könnten.
Die Resultate eines Angriffs, egal ob von innen oder von außen, fallen schwerwiegender aus als ohne Epidemie. Durch die herabgesetzte Wachsamkeit können Angriffe wie etwa Würmer oder Trojaner schwerer entdeckt werden und über längere Zeit Schaden anrichten. Auch fehlt für die Durchführung des Notfallkonzepts und die Beseitigung des Angriffs und seiner Folgen das Personal. Dieser Effekt wird durch die Abwesenheit des Administrators noch erheblich verstärkt.
Besonders gefährdet ist das Netz an seiner Verbindung nach außen: An den Firewalls. Falls ein Angriff doch die Firewalls durchbrechen kann, wird er nicht entdeckt, da niemand die Logfiles der Firewalls auswertet. Aber selbst wenn gar kein Angriff vorliegt, können die Firewalls zu einem Problem werden. Falls ein neues Kommunikationsprotokoll frei geschaltet

werden muss oder sonst eine Änderung an der Konfiguration nötig ist, so kann sie wegen der Flut an teils inaktiven Regeln nur schwer umgesetzt werden.
Nicht nur Angriffe, auch Unfälle und Fehlfunktionen bedrohen das Netz stärker als ohne Epidemie. Falls beispielsweise der Fileserver ausfällt, könnte im Normalfall der Administrator den Schaden schnell beheben. Ob der Server ohne den Administrator und ohne einen Großteil der übrigen Mitarbeiter schnell wieder einsatzbereit gemacht werden kann, ist fraglich.
Bei der Behandlung des vorliegenden Vorfalls ist die eigentliche Vorfallsbekämpfung somit nur ein kleiner Teil der anstehenden Aufgaben. Die Firma und das von ihr beauftragte IRT müssen vor allem Schäden durch Folgevorfälle abwenden oder beheben.

5.5.3. Bestehendes Notfallkonzept

Ein Vorfall der Art, wie er hier modelliert wurde, wird in der Praxis wohl selten in einem Notfallkonzept Beachtung finden. Falls eine Epidemie grassiert, werden die Mitarbeiter einfach zum Arzt geschickt, der dann die Behandlung übernimmt. Ein Notfallkonzept für eine Epidemie macht für eine Firma keinen Sinn. Sinnvoller ist ein allgemeineres Notfallkonzept, das immer dann greift, wenn ein Großteil der Mitarbeiter ausfällt. Warum dies passiert, ist zunächst einmal unerheblich. Wichtig sind die Gewährleistung der Fortsetzung der Produktivität und das Aufrechterhalten des Sicherheitsniveaus. Für die Notfallbeseitigung können im Einzelfall Zusatzmaßnahmen im Notfallkonzept enthalten sein, bei der in diesem Szenario modellierten Epidemie ist dies jedoch nicht der Fall. Es wird also ein Notfallkonzept modelliert, das nur Maßnahmen zur Fortsetzung der Geschäftsprozesse und zur Wahrung des Sicherheitsniveaus hat. Um die Einflussmöglichkeiten eines IRT auf das Notfallkonzept zu zeigen, wird von einem wenig konkreten Notfallkonzept ausgegangen. Vielmehr hat die Firma nur eine ungefähre Vorstellung davon, was im Falle des Mitarbeiterausfalls im großen Stil zu tun ist.

Falls ein Großteil der Mitarbeiter ausfällt, stehen weniger Arbeitskräfte für dieselbe Arbeit zur Verfügung. Deshalb müssen die einzelnen Geschäftsprozesse priorisiert werden: Welche Prozesse sind auch im Notfall unentbehrlich, und auf welche kann bis zur Beendigung des Notfalls verzichtet werden? Die Priorisierung fällt in den Aufgabenbereich der Geschäftsleitung, eventuell mit beratender Unterstützung der jeweils beteiligten Mitarbeiter. Die Ergebnisse dieser Priorisierung sind relevant für das firmeneigene IRT, da eventuell Netzumstellungen u.ä. nötig sind. Der Wahrung des IT Sicherheitsniveaus kommt auf jeden Fall eine hohe Priorität zu, da die Firma stark von der IT abhängt. Die Entscheidungen darüber, welche Prozesse fortgesetzt werden müssen und welche nicht, müssen möglichst schnell getroffen werden, da es beim Umsetzen eines Notfallkonzeptes auf Geschwindigkeit ankommt. Deshalb sind einige Richtlinien bereits im Notfallkonzept selber verzeichnet: Die Administration des Netzes muss gewährleistet sein. Falls der Administrator länger als eine Woche ausfällt und kein anderer Mitarbeiter diese Rolle zufrieden stellend ausfüllen kann,

muss ein Ersatzadministrator angeheuert werden. An dieser Stelle sei angemerkt, dass es sich dabei um einen kritischen Punkt handelt. Es ist für eine Firma ein nicht unerhebliches Zusatzrisiko, wenn sie einer firmenfremden Person administrative Funktion und damit einen tiefen Einblick in die IT der Firma gewähren muss. Um dieses Risiko zu umgehen, wird der Ersatzadministrator von einem firmeneigenen IRT zur Verfügung gestellt. Dieses IRT ist nur für Vorfälle innerhalb der Firma zuständig und existiert neben der normalen Firmenhierarchie mit seinen eigenen Mitarbeitern.
Von den übrigen Geschäftsprozessen sind außerdem alle weiterzuführen, die für den täglichen Betrieb der Firma notwendig sind. So muss etwa die Personalsachbearbeiterin bei Ausfall vertreten werden. Ähnliches gilt für alle anderen internen Verwaltungsprozesse, die im Szenario nicht modelliert wurden. Die produktiven Prozesse, also die tägliche Arbeit der normalen Mitarbeiter, kann hingegen für die Dauer des Notfalls reduziert werden. Laufende Aufträge haben bei der Bearbeitung Vorrang. Falls viele Mitarbeiter ausfallen, werden keine weiteren Aufträge angenommen, bis die Lage sich entspannt hat. Dies kann allerdings zu Imageverlust führen, der hier jedoch in Kauf genommen wird.
Zur unmittelbaren Notfallbekämpfung sind, wie gesagt, keine konkreten Angaben im Notfallkonzept vorhanden. Allerdings soll nach Möglichkeit die Ursache des Vorfalls geklärt werden, um später vermeidende Maßnahmen erarbeiten zu können.

5.5.4. Arbeit und Ergebnisse des IRTs

Die Arbeit des IRTs, das hier als firmeneigen modelliert wurde, konzentriert sich auf Hilfestellung bei der Aufrechterhaltung der Arbeitsprozesse und der Wahrung des Sicherheitsniveaus. Die sonst übliche Aufklärungsarbeit kann weitgehend entfallen, da der Vorfall nicht aus dem Bereich der IT entstammt und diese auch nur indirekt beeinflusst.

- Incident Analysis

Die Analysearbeit, die das IRT beim Epidemievorfall leisten muss, umfasst hauptsächlich eine „Einschätzung der Lage". Die Aufgabe des IRTs besteht in der Abschätzung, inwieweit die Sicherheit der IT bedroht ist und was dagegen getan werden kann. Im Unterschied zu den bisherigen Szenarien muss also kein bereits eingetretener Sicherheitsvorfall untersucht werden, sondern es müssen durch die Epidemie entstandene oder verschärfte Risiken für mögliche Sicherheitsvorfälle entdeckt und beurteilt werden. Letztlich muss also eine Risikoanalyse vorgenommen werden. Einige mögliche Ergebnisse wurden bei der Szenariobeschreibung in Abschnitt 5.5.2. bereits genannt.
Eine zweite wichtige Aufgabe des IRTs im Bereich der Vorfallsanalyse besteht darin herauszufinden, inwieweit die anliegende Arbeit mit der IT ohne das erkrankte Personal noch durchgeführt werden kann. Teilweise überschneidet sich dieser Aufgabenbereich mit der oben genannten Risikoanalyse, allerdings müssen hier auch die IT bezogenen Arbeitsprozesse untersucht werden, die nichts mit der Sicherheit zu tun haben. Beispielsweise fällt die Beantwortung der Frage, ob die Backups noch regelmäßig und korrekt angelegt werden

können, in beide Bereiche, denn das Anlegen von Backups ist sowohl ein IT Arbeitsprozess als auch eine sicherheitsrelevante Tätigkeit. Hingegen fällt die Frage, ob die firmenweite Installation eines neuen Bildschirmschoners planmäßig durchgeführt werden kann, nur in den zweiten Aufgabenbereich und nicht in die Risikoanalyse, denn der Bildschirmschoner ist nicht sicherheitsrelevant.
Die Ergebnisse aus beiden Analysen dienen dazu, wie im Notfallkonzept verlangt die Arbeitsprozesse zu priorisieren. Da diese Priorisierung schnell erfolgen soll, muss auch die Analyse schnell vollzogen werden. Aus diesem Grund kann vor allem die naturgemäß aufwendige Risikoanalyse nur oberflächlich und in Teilen vorgenommen werden.

- Reinigung

Die Aufgaben der Reinigung, die im Epidemieszenario anfallen, entstammen nicht dem Vorfall selber, sondern eher der liegen gebliebenen Administrationsarbeit. Zu den normalen Aufgaben des Administrators gehört auch, defekte Systeme neu zu installieren oder zu reinigen. Da das IRT für die Dauer des Vorfalls einen Ersatzadministrator stellt, übernimmt es auch diese Aufgaben.
Reinigungsarbeiten, die von einem Vorfall direkt herrühren, treten nur dann auf, wenn ein Folgevorfall eintritt. Falls es sich dabei um einen Angriff handelt, müssen gängige Reinigungsmaßnahmen vom IRT ergriffen werden. Für Beispiele solcher Arbeiten sei auf die ersten beiden Szenarien verwiesen.

- Vermeidung

Maßnahmen der Vermeidung sind beim Epidemieszenario außerordentlich wichtig. Die Firma befindet sich während des gesamten Vorfalls in einer Situation erhöhter Verletzbarkeit, die das IRT vor allem mit Wachsamkeit beantworten muss. Das IRT muss zunächst die Aufgaben der Netzüberwachung vornehmen, die ansonsten der Administrator wahrnimmt. Damit ist nicht etwa die Überwachung der Mitarbeiter oder das Ausspionieren des Netzverkehrs gemeint, sondern beispielsweise das Durchsehen der Logfiles von Firewalls und Fluttoren sowie das Sammeln und Abarbeiten von Hinweisen auf Anomalien. Da wie in 5.5.2. ausgeführt die Gefahr eines Angriffs von innen während der Epidemie größer ist als normal, sind die internen Sicherheitsvorkehrungen nicht nur weiterhin zu betreiben (eventuell mit personeller Unterstützung durch das IRT), sondern sie sind eventuell sogar zu verschärfen. Beispielsweise könnten Serverzugriffe geloggt werden (vgl. das erste Szenario), oder es könnten physikalische Schutzmaßnahmen eingerichtet werden, ähnlich beispielsweise der im ersten Szenario beschriebenen Datenträgerkontrolle.
Die Vermeidungsmaßnahmen beim Epidemievorfall unterscheiden sich also von den üblichen Vermeidungsmaßnahmen, die ein IRT vornimmt. Normalerweise zielen Vermeidungsmaßnahmen darauf, weiteren durch den konkreten Vorfall eingetretenen Schaden zu verhindern oder den konkreten Vorfall als ganzes zu verhindern. In diesem

Szenario richtet der Vorfall selber gar keinen IT sicherheitsrelevanten Schaden an, sondern macht nur andere Vorfälle wahrscheinlicher und gefährlicher. Ähnlich wie schon bei der Vorfallsanalyse muss also nicht nur mit einem Vorfall gearbeitet werden, sondern mit einer Vielzahl noch nicht eingetretener Vorfälle.

- Gegenwehr

Das IRT kann gegen die Epidemie wenig Gegenwehr leisten. Auch an der IT gibt es wenig an Gegenwehr zu tun, außer die hochpriorisierten Prozesse fortzuführen und die beschriebenen Aufgaben der Analyse, Reinigung und Vermeidung wahrzunehmen. Das IRT muss sich jedoch bereithalten, um gegebenenfalls gegen Folgevorfälle Gegenwehr zu leisten.

- Rechtliche Schritte

Die rechtlichen Schritte, bei deren Ergreifung das IRT helfen kann, spielen in diesem Szenario kaum eine Rolle. Obwohl beispielsweise an eine Rechtsverfolgung der behandelnden Tierärzte zu denken ist, die den Büroschlaf nicht als Epidemie erkannt haben bevor das Fleisch in den Handel kam, ist dies nicht Aufgabe des IRTs.

5.5.5. Einfluss auf die Weiterentwicklung des Notfallkonzeptes

Die Möglichkeiten des IRTs, auf das Notfallkonzept einzuwirken, sind in diesem Szenario sehr groß. Das IRT nimmt sogar sehr direkten Einfluss auf das Notfallkonzept, denn durch seine Arbeit während des laufenden Vorfalls nimmt das Notfallkonzept erst seine genaue Gestalt an und wird noch während desselben Vorfalls verwendet.

Das bestehende Notfallkonzept umfasste hauptsächlich die Aufgabe der Priorisierung der Arbeitsprozesse im Notfall. Damit diese Aufgabe erfüllt werden konnte, waren die Ergebnisse der Vorfallsanalyse durch das IRT abzuwarten. Das Notfallkonzept wurde also durch die Arbeit des IRTs überhaupt erst konkretisiert. Dies entspricht dem üblichen Vorgehen, das bereits in Kapitel 1 dargestellt wurde: Am Anfang steht eine Risikoanalyse. Diese nimmt hier in der Analyse des Vorfalls Gestalt an. Aus der Risikoanalyse werden geeignete Gegenmaßnahmen abgeleitet, von denen dann einige in ein Notfallkonzept integriert werden.

Das in diesem Szenario vor dem Eintritt des Vorfalls erstellte Notfallkonzept war nur ein Rahmenwerk, welche Typen von Maßnahmen im Notfall getan werden sollen. Wie genau diese Aufgaben zu erfüllen sind, ergab sich erst aus der Analysearbeit des IRTs. Ohne sie kann selbst die Priorisierung nur unzureichend durchgeführt werden, da die Relevanz einzelner Prozesse eventuell nicht abgeschätzt werden kann. Wurden die hochpriorisierten Prozesse dann gefunden, kann die Methode, wie ihre Fortsetzung gewährleistet werden kann, ebenfalls aufgrund der Analyse durch das IRT ermittelt werden.

Letztlich ist die Arbeit, die das IRT während des Vorfalls wahrnimmt, nichts anderes als ein Risikomanagement im Kleinen. Die Erkenntnisse, die daraus gewonnen wurden, können für weitere Vorfälle der Klasse „Mitarbeiterausfall“ verwendet werden.

5.5.6. Fazit

Das Fazit aus diesem Szenario besteht in zwei Dingen: Zum einen wird die Wichtigkeit des Risikomanagements für ein erfolgreiches Notfallkonzept noch einmal deutlich. Zum anderen wurde gezeigt, dass die Arbeit des Risikomanagements sehr gut durch ein IRT übernommen werden kann.

Dennoch: Das Risikomanagement im Ganzen gehört nicht zum üblichen Aufgabenbereich eines IRT. Es erfordert einen tiefen Einblick in die Struktur und die Daten einer Firma, und wird deshalb nur selten von einem IRT vorgenommen, dass nicht zur Firma selbst gehört.

Wäre die Risikoanalyse vor Eintritt der Epidemie von der Firma sachgemäß durchgeführt worden, hätte es bereits ein ausformuliertes Notfallkonzept gegeben. Im Normalfall wäre diese Risikoanalyse für den Fall des Mitarbeiterausfalls von der Firma selber durchgeführt worden, und zwar vor dem Vorfall. Dann hätte die Priorisierung der Prozesse schon stattgefunden, und Konzepte für die Aufrechterhaltung von wichtigen Prozessen und Sicherheitsniveau hätten schon vorgelegen.

5.6. Unfall: Ausfall der Firewalls

Im sechsten und letzten Szenario soll ein Unfall modelliert werden, der durch menschliches Fehlverhalten ausgelöst wird. Die Firewalls des Hauptquartiers seien für dieses Szenario mit „intelligenten Bedienungshilfen“ versehen, die eine „besonders einfache Administration“ ermöglichen. Mit solchen Bedienelementen sind in der heutigen Zeit viele Programme ausgestattet. Sie sollen das Installieren und vor allem das Konfigurieren und Warten von Software einfacher gestalten. Auf eine bestimmte Handlung des Benutzers bzw. Administrators hin versucht ein spezieller Algorithmus zu ermitteln, was der Benutzer gerade vorhat. Anschließend wird der vermeintliche Benutzerwille umgesetzt, ohne dass der Benutzer alle normalerweise für diesen Schritt notwendigen Eingaben getätigt hat. Solche Mechanismen sind hilfreich, wenn die Ratealgorithmen den richtigen Benutzerwillen ermitteln. Andernfalls sind sie oft störend, oder bei Sicherheitssoftware sogar gefährlich.

5.6.1. Vorstellung des Szenarios

Die Firewallsoftware des Hauptquartiers ist mit einer der oben beschriebenen Eingabehilfen versehen, die dem Administrator ermöglichen soll, möglichst schnell neue Regeln zu aktivieren oder andere zu deaktivieren. Ein Teil dieser Funktionalität besteht darin, dass mit einem einzelnen Knopfdruck die Firewall von generellem Verbot auf generelle Erlaubnis umgestellt werden kann und umgekehrt. Alle früheren Erlaubnisregeln werden dann zu Verbotsregeln. Somit wird die Konfiguration der Firewall exakt umgedreht: Was früher geblockt wurde wird jetzt durchgelassen, und was früher erlaubt war, wird jetzt geblockt.

Das Szenario ist so gestaltet, dass der Administrator zum Zeitpunkt des Vorfalls im Urlaub ist. Sein Stellvertreter konnte sich bislang nur unzureichend in die Firewalladministration einarbeiten, weshalb er aus Versehen diesen Umschaltknopf betätigt.

Durch diese Fehlkonfiguration werden im Grunde zwei Vorfälle ausgelöst. Zum einen wird das Schutzniveau der Firewall gesenkt, da potentiell gefährlicher Netzverkehr nun nicht mehr gefiltert wird. Zum anderen wird die Produktivität der Firma gesenkt, da die gewollte Internetkommunikation nicht mehr verfügbar ist. Für beide Vorfälle müssen die bedrohten Werte getrennt voneinander ermittelt werden. Die Senkung des Schutzniveaus kann zudem zu Folgevorfällen führen, die wiederum andere Werte bedrohen. Einen genaueren Überblick gibt Abbildung 12

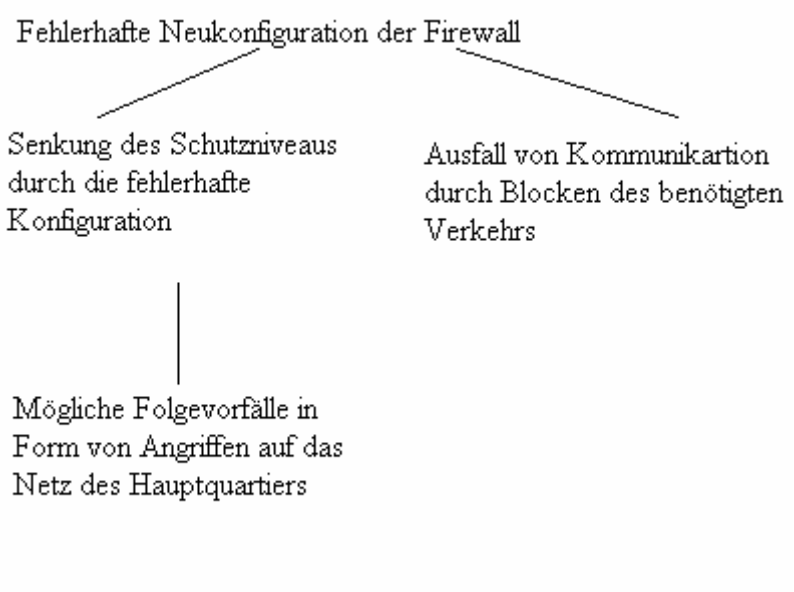


Abbildung 12: Konstellation beim Firewallausfall

Durch die Senkung des Schutzniveaus selber ohne Betrachtung möglicher Folgevorfälle wird eigentlich nur ein Wert bedroht: Der Schutz, den die Firewall bietet. Auch Schutz anderer Werte ist wiederum ein Wert, der durch einen Vorfall beeinträchtigt werden kann.
Die Senkung des Schutzniveaus macht sich zunächst nicht in einem konkreten Schaden an den durch die Firewall geschützten Werten bemerkbar, sondern nur in einer möglichen Beeinträchtigung von Vertraulichkeit, Verfügbarkeit und Integrität dieser Werte. Die Freischaltung der Firewall für ungewollten Netzverkehr schafft nur eine neue Schwachstelle, die zu neuen Risiken führt und damit in Folgevorfällen münden kann, aber nicht muss.
Die durch diese Risiken bedrohten Werte sind zunächst einmal die Daten, die im Rechnernetz gespeichert sind. Hinzukommen andere mit dem Netz verflochtene Werte wie etwa Rechenzeit, Verfügbarkeit von Diensten und Hardware usw. Auf welchen der drei Achsen des Sicherheitsniveaus sich ein Schaden an diesen Werten bewegt, hängt vom konkreten Folgevorfall ab. Die Daten beispielsweise können einen Vertraulichkeitsverlust erleiden, wenn der Folgevorfall in z.B. Datenspionage von außen besteht (vgl. das erste und dritte Szenario). Sie können auch einen Integritätsverlust erleiden, wenn ein Angreifer von außen die gespeicherten Daten modifiziert oder löscht, etwa mit einem so genannten „remote administration tool“. Genauso gut kann aber auch ein Verfügbarkeitsverlust eintreten, wenn

beispielsweise der Fileserver Opfer einer denial of service Attacke wird. Ähnliches gilt auch für die übrigen aufgezählten Werte.
Der zweite Vorfall, ausgelöst durch das Blocken des normalerweise erwünschten Verkehrs, bedroht andere Werte. Zunächst ist wiederum eine Funktion der Firewall als Wert betroffen. Allerdings handelt es sich dabei nicht um den Schutz, den sie bieten soll, sondern um die Funktionalität, den gewollten Netzverkehr ins Internet oder aus dem Internet ins Hauptquartier zu leiten (von konkreten Diensten wie etwa Gatewayfunktionalitäten soll hier abstrahiert werden). Auch diese Funktionalität der Firewall ist ein Wert, und durch den Vorfall wird an diesem Wert ein Verfügbarkeitsschaden verursacht.
Zusätzlich sind noch Werte auf indirekte Weise bedroht. Durch den Wegfall der Kommunikationsmöglichkeiten können Kunden wegfallen, was wiederum zu Gewinneinbußen führt. Auch sind wichtige Internetressourcen wie Suchmaschinen oder Patches eventuell nicht mehr verfügbar. Die Reihe der sekundär bedrohten Werte ließe sich noch weiter fortsetzen.

5.6.2. Technischer Aufbau und Art des Vorfalls

Auch hier folgen zunächst die Kenngrößen, danach der Ablauf des Vorfalls.

- Systeme

Das Netz des Hauptquartiers besteht wie in den vorangegangenen Szenarien aus hardwaretechnisch nahezu baugleichen Rechnern. Die Workstations haben absolut die gleiche Hardware, das gleiche Betriebssystem und eine identische Grundausstattung an Software, die der einzelne Mitarbeiter für seine Arbeit benötigt. Fileserver und Personalserver haben eine größere Festplatte und einen CD Brenner, sind ansonsten aber baugleich. Auch die Rechner der Firewalls und des Fluttors entsprechen der Bauweise der Workstations. Für die Funktionalität von Firewalls und Fluttor wird dieselbe Software verwendet. Alle Workstations und beide Server haben eine Benutzerverwaltung, die eine Anmeldung als Benutzer oder als Administrator zulässt (bei Kenntnis des jeweiligen Passworts). Die Benutzerverwaltung auf den Firewallrechnern und dem Fluttorrechner kennt nur die Administratorkennung.
Von allen Workstations aus sowie vom Personalserver aus besteht Internetzugang, der über die Firewalls ins Internet geleitet wird, und wieder zurück. Prinzipiell ist das Betriebssystem durch zahlreiche ungepatchte Schwachstellen für eine Vielzahl von netzbasierten Angriffen anfällig, deren Erfolg nur durch die Filtermechanismen der Firewall und eventuell den Malwarescanner vereitelt wird.
Auf dem Fileserver hat analog zu den anderen Szenarien jeder Benutzer ein passwortgeschütztes Verzeichnis, und es existiert zusätzlich ein öffentliches Verzeichnis. Der Personalserver wird von der Personalsachbearbeiterin nebenbei als Workstation genutzt. Er unterscheidet nicht zwischen einem normalen Benutzer und einem Personalsachbearbeiter, somit kann jede als Benutzer angemeldete Person sowohl die Workstationfunktionalität als

auch die Serverdienste nutzen. Die Serverdienste sind zudem nicht gesondert passwortgeschützt.

- Backups

Backups von den Daten auf dem Fileserver und dem Personalserver werden jeden Freitag um 17.00 gezogen und auf CD gebrannt. Diese Aufgabe fällt dem Administrator zu.

- Zugriffsrechte

Auf den Workstations kann ein Benutzer nur die Workstationfunktionalität nutzen, ein Administrator kann nur die administrativen Funktionen benutzen. Auf dem Fileserver hat ein Benutzer Zugriff auf sein eigenes Verzeichnis und das öffentliche Verzeichnis. Das öffentliche Verzeichnis hat keinerlei Passwortschutz.
Auf dem Personalserver kann ein Benutzer die Workstationfunktionalität und zusätzlich die Serverfunktionalität nutzen. Die Daten des Personalservers können über das Netz abgerufen, kopiert und geändert werden, wenn der Betreffende sich über das Netz auf dem Personalserver als Benutzer anmeldet. Ein Administrator kann auch hier nur die administrativen Funktionen nutzen.
Die Firewalls und das Fluttor kennen nur eine Anmeldung als Administrator und haben keinerlei Workstationfunktionalität.

- Mitarbeiterkompetenzen

Jeder Benutzer hat auf seiner Workstation Benutzerrechte. Es gibt einen Administrator, der das gesamte Netz administriert. Während seiner Abwesenheit übernimmt ein Mitarbeiter seine Aufgaben, der darin zumindest teilweise ausgebildet wurde. Allerdings kennt sich der Stellvertreter nicht mit der Handhabung der Firewallsoftware aus.
Die Personalsachbearbeiterin hat auf dem Personalserver Benutzerrechte. Außer ihr kennt nur der Firmenchef das Benutzerpasswort, und somit nutzt normalerweise niemand die Funktion, die Serverdaten über das Netz abzurufen.

- Sicherheitspolitik

Alle Daten im Netz sind vertraulich, verfügbar und integer zu halten. Auch die Hardware und die Dienste im Netz sind verfügbar zu halten, dies gilt insbesondere für die Firewalldienste und den Internetzugang.
Die Verfügbarkeit der Dienste hat der Administrator sicherzustellen. Falls einem Benutzer Probleme auffallen, hat er den Administrator darüber zu informieren. Die Sicherheit der Daten ist durch die Firewall und den Passwortschutz sicherzustellen. Die Sicherheitspolitik wurde in der Firma kommuniziert.

- Konfiguration der Firewalls

Die Firewalls sind nach dem generellen Verbot konfiguriert. Die Erlaubnisregeln folgen einer Standardkonfiguration, die vom Hersteller der Firewall empfohlen wurde und mit einem einfachen Knopfdruck aktiviert werden kann. Sie wurde vom Administrator überprüft und aktiviert. Durchgelassen werden die üblichen Internetprotokolle, die für einen normalen Internetverkehr nötig sind, etwa http und ftp. Zudem fungiert die Firewall unter anderem als Mailgateway, auf dem ein Malwarescanner läuft. Dieser ist mit den neuesten Signaturen ausgestattet, die vom Administrator jeden Tag herunter geladen und eingebunden werden.
Zur Konfiguration der Firewalls wird ein Konfigurationsprogramm verwendet, das die Konfiguration beider Firewallrechner steuert.

- Konfiguration der Fluttore

Das Fluttor wird in diesem Szenario nicht verwendet, und deshalb ist seine Konfiguratiuon nicht von Belang.

- Weitere Kenngrößen

Die Firewallsoftware verfügt über eine Reihe von „einfachen Administrationsmöglichkeiten“. Eine davon erlaubt es, per Knopfdruck die Firewall von generellem Verbot auf generelle Erlaubnis umzustellen und gleichzeitig alle Erlaubnisregeln in Verbotsregeln umzuwandeln. Wird diese Funktion aktiviert, so findet diese Neukonfiguration statt, ohne dass der Benutzer noch einmal gesondert die Aktion bestätigen muss oder auf die Änderung der Konfiguration hingewiesen wird.

An einem Montagmorgen reicht der Administrator einen längeren Urlaub ein. Dieser soll drei Wochen umfassen und in einer Woche beginnen. Da der Administrator seinen Urlaub auf einer Insel in einem weit entfernten Land verbringen möchte, wird er während des Urlaubs auch in Notfällen nicht erreichbar sein.
Damit auch während der Abwesenheit des Administrators der reibungslose Betrieb des Netzes gewährleistet ist, beauftragt die Firmenleitung den Administrator, seinen Stellvertreter vor Beginn des Urlaubs noch einmal in alle Aufgaben einzuweisen. Bislang hatte der Stellvertreter nur Meldungen gesammelt, die der eigentliche Administrator dann bei seiner Rückkehr abgearbeitet hatte.
Der Administrator führt den Stellvertreter in alle wichtigen Aufgaben ein und informiert auch die Mitarbeiter, wer der Stellvertreter sein wird. Nur in die Handhabung der Firewall wird der Stellvertreter nicht eingeführt, da die Konfiguration ohnehin eine Standardeinstellung sei und während des Urlaubs bestimmt nichts daran geändert werden müsse.
So tritt der Administrator seinen Urlaub an. Der Stellvertreter macht seine Arbeit sehr gut, beim normalen Administrationsalltag treten keinerlei Probleme auf. Am vierten Tag seiner Stellvertretertätigkeit überkommt ihn dann doch die Neugier. Er beschließt, sich die

Firewallkonfiguration einmal anzusehen. Unbewusst betätigt er beim Durchsehen der Regeln einen Knopf, der die Konfiguration wie oben beschrieben umkehrt.
Kurze Zeit später melden zahlreiche erboste Mitarbeiter, dass der Internetzugang nicht mehr funktioniere. Der Stellvertreter macht einige Untersuchungen am Netz und den Workstations der betroffenen Mitarbeiter, kann aber keinen Fehler finden. Da er nicht mit einer Konfigurationsänderung der Firewall rechnet, wird diese nicht untersucht. Da der Stellvertreter den Fehler nicht finden kann, wird schließlich ein IRT mit der Untersuchung beauftragt...

5.6.3. Bestehendes Notfallkonzept

Der Ausfall der Firewalls ist ein in der Realität nicht seltener Notfall, weshalb für ihn ein Notfallkonzept existieren muss. In diesem Szenario wird es allerdings für die beiden geschilderten Teilvorfälle getrennt modelliert werden, ein einheitliches Notfallkonzept für den Firewallausfall gibt es noch nicht. Die Untersuchung wird zeigen, warum ein einheitliches Notfallkonzept für den gesamten Firewallausfall geeigneter ist als zwei getrennte.

Der Wegfall der Filterfunktion der Firewall ist ein Vorfall, der außer an der Firewall selbst keinen messbaren Schaden anrichtet (siehe auch Abschnitt 5.6.1. zu den bedrohten Werten). Deshalb umfasst das Notfallkonzept hauptsächlich Präventivmassnahmen, um Folgevorfälle und die daraus resultierenden Schäden zu vermeiden.
Wurde der Wegfall der Filterfunktionalität entdeckt, soll das Hauptquartiernetz sofort physikalisch vom Internet getrennt werden (bzw. von den Zweigstellen, falls der Ausfall im Fluttor auftritt). Oberste Priorität hat dann das Ermitteln des Grundes, warum die Filterfunktionalität ausgefallen ist. Ziel der Ermittlung ist, die Filtermechanismen so schnell wie möglich wieder in Betrieb zu nehmen. Außerdem soll die Ursache des Ausfalls dauerhaft beseitigt werden. Falls er beispielsweise durch einen Angriff erfolgt ist, muss der Angriff vor dem Einleiten weiterer Maßnahmen beendet werden. Parallel dazu wird das Netz nach den Spuren eventuell bereits eingetretener Folgevorfälle abgesucht. Falls solche gefunden werden, beginnt eine Analyse dieser Folgevorfälle und danach die übliche Vorfallsbehandlung. Zusätzlich werden die für die jeweiligen Folgevorfälle vorhandenen Notfallkonzepte ebenfalls abgearbeitet.

Auch der zweite Vorfall, der Wegfall des Internetzugangs und der damit verbundene Produktivitätsausfall, erfordert eine rasche Bearbeitung durch ein Notfallkonzept. Hier sind im Gegensatz zum ersten Vorfall keine Präventivmaßnahmen gefordert, sondern Abstellungsmaßnahmen. Außerdem sind hier kaum Folgevorfälle zu befürchten.
Analog zum ersten Vorfall soll der Grund für den Ausfall der Verbindungen möglichst rasch geklärt werden. Auch hier besteht das Ziel darin, die Störung schnellstmöglich zu beseitigen, also den Zugang zum Internet wiederherzustellen.

Falls dies nicht innerhalb eines halben Tages möglich ist, soll der Administrator eine Ersatzverbindung etablieren. Dazu wird der betroffene Firewallrechner aus dem Netz entfernt und durch einen Ersatzrechner ersetzt, auf dem dann eine Firewall mit Notkonfiguration installiert wird. Zu beachten ist, dass für die Firewallkonfiguration kein Backup angelegt wurde und die Konfiguration deshalb tatsächlich neu vorgenommen werden muss. Die Notkonfiguration basiert auf generellem Verbot. In Erlaubnisregeln werden dann die am dringendsten benötigten Dienste und Protokolle zum Durchlassen festgelegt.

Der detaillierte Ablauf der beiden Notfallkonzepte, etwa die Reihenfolge, in der mögliche Gründe für die Ausfälle geprüft werden, soll hier nicht modelliert werden, da er für das Szenario keine Rolle spielt. Wichtig ist, dass es sich bei den beiden Teilvorfällen um häufig auftretende Vorfälle handelt, für die in der Regel bereits gute Notfallkonzepte existieren. Der Sonderfall, der in diesem Szenario zum Tragen kommt, besteht darin, dass beide Vorfälle gleichzeitig eintreten

5.6.4. Arbeit und Ergebnisse des IRTs

Das IRT hat in diesem Szenario zwei gleichzeitig auftretende Vorfälle zu bearbeiten, die dieselbe Ursache haben. Allerdings ist diese Tatsache zu Beginn der Vorfallsanalyse noch unbekannt, weshalb zunächst von zwei Vorfällen ohne Verbindung ausgegangen wird.

- Incident Analysis

Das IRT bekommt zunächst nur Mitteilungen aus der Firma wie etwa „wir kommen nicht mehr ins Internet“. Dass auch die Filterfunktionalität ausgefallen ist, wird in der Firma zunächst nicht auffallen, da sich der Netzverkehr und das Netzverhalten nicht ändern. Erst dann, wenn normalerweise verbotener Netzverkehr abgeschickt und plötzlich nicht mehr geblockt wird, kann das Fehlen der Filtermechanismen auffallen. Am deutlichsten wird dies, wenn ein Angriff von außen auf das Netz der Firma gestartet wird. Da dies jedoch nicht der Fall ist und auch ansonsten niemand anomalen Netzverkehr beobachtet, wird der Ausfall der Filtermechanismen zunächst nicht entdeckt.
Das IRT wird also die einzelnen Rechner und Netzleitungen untersuchen. Mögliche Ursachen für einen Wegfall der Internetverbindungen gibt es viele, etwa Fehler auf den Workstations, Kabelbrüche, lose Stecker bei den Netzkabeln usw. Auch ein Fehler bei der Firewall gehört zu den möglichen Ursachen, wird aber eventuell nicht als erstes abgeprüft.
Nachdem das IRT festgestellt hat, dass das gesamte Hauptquartier keinen Internetzugang mehr hat, können Fehler an den Workstations nahezu ausgeschlossen werden. Auch die Untersuchung der Kabel und Steckverbindungen bleibt ohne Befund. Schließlich wird das IRT dann auch die Firewall untersuchen.
Es wird eine Workstation direkt hinter den Firewalls ins interne Netz gestellt, sodass sie ohne weitere zwischengeschaltete Rechner direkt über die Firewalls mit dem Internet verbunden ist. Da auch hier kein Internetzugang möglich ist, muss der Fehler an den Firewalls oder

außerhalb des Firmennetzes liegen. Er wird dadurch auf die Firewalls festgelegt, indem die Workstation nun noch einmal ohne Firewalls direkt ans Internet angeschlossen wird und hier ein Internetzugang möglich ist.
Somit steht fest, dass die Firewallrechner den Internetzugang blockieren. Da die Analyse des Fehlers eventuell längere Zeit in Anspruch nehmen könnte, wird zunächst eine Ersatzfirewall aufgestellt. Nach einigen Untersuchungen zeigt sich, dass die Firewall falsch konfiguriert wurde und sich der Fehler relativ einfach beheben lässt. Der zweite Vorfall, der Wegfall der Filterfunktionen wird dabei ebenfalls entdeckt und gleich mitbeseitigt. Anschließend muss das Netz sicherheitshalber auf Folgevorfälle untersucht werden, was hier nicht näher beschrieben werden soll.
Findet jedoch gleichzeitig ein Angriff von außen auf das Netz statt wie etwa durch einen Wurm (vgl. das zweite Szenario), so wird die Analyse komplizierter. Die Analyse und Behandlung des Wurmvorfalls, exemplarisch in 5.2.4. dargestellt, hat dann Priorität. Mehrere Vorfallsanalysen laufen dann parallel ab und könnten sich gegenseitig behindern, sodass verwendbare Erkenntnisse über die Ursachen der Vorfälle erst später zur Verfügung stünden. Auch würde der Zusammenhang zwischen den Vorfällen erst später deutlich werden, was eventuell zu ungeeigneten Behandlungsmaßnahmen führen könnte.

- Reinigung

Die beiden durch die Fehlkonfiguration ausgelösten Vorfälle erfordern keine Reinigung. Allerdings können Folgevorfälle eine Reinigung eventuell des ganzen Netzes nötig machen (vgl. die Szenarien zwei und drei).

- Vermeidung

Präventivmaßnahmen sind vor allem im Zusammenhang mit dem Ausfall der Filterfunktion nötig. Falls dieser Vorfall wie im Hauptteil der Vorfallsanalyse beschrieben nicht bemerkt wird, bevor der Vorfall quasi schon zu Ende ist, sind keine Präventivmaßnahmen möglich. In dem Moment, in dem der Vorfall entdeckt wird, besteht auch schon die Möglichkeit, ihn komplett zu beenden. Dies macht weitere Vermeidungsmaßnahmen überflüssig.
Fällt der Wegfall der Filterfunktionalität aber schon vorher auf, sei es durch einen Angriff, anormalen Netzverkehr o.ä., so sind Vermeidungsmaßnahmen dringend angezeigt. Die wichtigste steht schon im Notfallkonzept: Das Hauptquartiernetz vom Internet trennen. Anschließend muss zunächst die Vorfallsanalyse angestoßen werden, die sich mit dem Ausfall der Filterfunktionen beschäftigt. Nebenher werden weitere Vermeidungsmaßnahmen gegen Folgevorfälle etabliert. Anomalien im Netz sind sofort zu melden. Das Netz muss auf eventuell schon eingetretene Folgevorfälle untersucht werden. Eventuell müssen Patches eingespielt oder die Rechner des Netzes auf eingedrungene Malware untersucht werden. Auf jeden Fall muss das Fluttor untersucht werden, ob die Filterfunktionen dort noch

funktionieren. Falls dies nicht der Fall ist, müssen die Zweigstellen benachrichtigt und eventuell die Netzverbindungen dorthin ebenfalls zeitweilig unterbrochen werden.

- Gegenwehr

Sobald beide Vorfälle aufgeklärt sind, liegt die wichtigste Gegenwehrmaßnahme auf der Hand: die Wiederherstellung einer korrekten Firewallkonfiguration. Dabei spielt es eine verhältnismäßig kleine Rolle, wie dies erfolgt. Nur sollte es schnell gehen, da der normale, abgesicherte Internetzugang so schnell wie möglich wieder verfügbar sein sollte.
Falls die Vorfallsanalyse genug Details zum Ablauf des Vorfalls erbracht hat, kann die Konfiguration durch einfache Umkehr der Fehlkonfiguration wiederhergestellt werden. Ist dies nicht der Fall, muss eine neue Konfiguration eingestellt werden. Dazu muss aber zunächst der Inhalt derselben ermittelt werden, etwa durch eine Anforderungsanalyse im Netz. Ohne Backups der Firewallkonfiguration kann die Wiederherstellung sehr lange dauern, zumal der kundige Administrator nicht verfügbar ist und keine Auskünfte geben kann.
Dauert die Wiederherstellung länger als einen halben Tag, so greift nach dem Notfallkonzept die Einstellung einer Ersatzfirewall. Diese birgt jedoch auch wieder das Risiko der Fehlkonfiguration, sodass benötigter Verkehr eventuell trotzdem teilweise geblockt wird, während gefährlicher Verkehr eventuell teilweise durchgelassen wird. Auf jeden Fall ist die Ersatzfirewall eine suboptimale Lösung.

- Rechtliche Schritte

Rechtliche Schritte wären gegen den Administrator und seinen Stellvertreter anzudenken. Bei der Ermittlung können die Ergebnisse der Vorfallsanalyse verwendet werden. Ansonsten ist die rechtliche Aufklärung des Vorfallsablaufs hier wegen der simplen Ursache kein Problem.

5.6.5. Einfluss auf die Weiterentwicklung des Notfallkonzepts

Das Szenario hat gezeigt, dass es große Schwierigkeiten mit sich bringen kann, wenn zwei Vorfälle mit derselben Ursache gleichzeitig auftreten, und die Ursache unbekannt ist. Durch die Analysen des IRTs hat sich gezeigt, dass die in der Firma verwendete Firewall Schwächen in der Konfigurierbarkeit hat. Soll diese Firewall weiterhin verwendet werden, bietet sich die Erstellung eines neuen Notfallkonzeptes zum Notfall „Firewallausfall“ an. Dieses Notfallkonzept behandelt dann einheitlich alle Folgen des Firewallausfalls, anstatt die beiden durch ihn ausgelösten Vorfälle getrennt zu behandeln. Dies hat mehrere Vorteile: Zum einen wird in Zukunft die Firewall als erstes Objekt im Netz untersucht werden, wenn der Internetzugang ausfällt. Weiterhin wird der Ausfall der Filtermechanismen grundsätzlich mituntersucht anstatt nur zufällig entdeckt zu werden. Schließlich kann auch Zeit gespart werden, denn die Behandlung des Firewallausfalls hat Möglichkeiten gezeigt, wie der Vorfall schneller behandelt werden kann. Eine davon wäre das Anlegen von Firewallbackups, um die Konfiguration schnell wiederherstellen zu können. Diese sind bei einer exakten Wiederholung

des Vorfalls zwar nicht nötig (der Knopf, um alles wieder richtig zu stellen, ist jetzt ja bekannt), aber bei lediglich ähnlichen Vorfällen kann das Backup wichtig sein. Die Firewallkonfiguration kann nicht nur durch Bedienungsfehler, sondern beispielsweise auch durch einen Festplattenfehler verändert werden.

5.6.6. Fazit

Bei der Erstellung eines Notfallkonzeptes kommt es sehr darauf an, für welchen Notfall das Notfallkonzept anwendbar sein soll. Etwa nur für einen ganz bestimmten Notfall oder für eine größere Klasse ähnlicher Notfälle? Bei der Beantwortung dieser Frage gibt es grundsätzlich kein Richtig oder Falsch, es hängt von der Situation und der Struktur der Organisation ab. In diesem Szenario waren die beiden Notfallkonzepte für je einen speziellen Notfall eindeutig weniger gut geeignet als ein Notfallkonzept für eine größere Notfallklasse. Die Arbeit des IRTs hat dies aufgezeigt, und die Firma kann nun ein neues Notfallkonzept entwickeln.
Allerdings heißt das nicht, dass die getrennten Notfallkonzepte nicht auch von Bedeutung wären. Wird beispielsweise der Internetzugang durch ein defektes Kabel unterbrochen und es gibt nur das Notfallkonzept „Firewallausfall“, so wird die Behandlung des Notfalls unnötig länger dauern.
Für jeden möglichen Notfall sollte es ein angemessen detailliertes Notfallkonzept geben. Deshalb darf die Betrachtung des Raumes möglicher Notfälle nicht zu groß gewählt werden. Ein Notfallkonzept der Form „Wenn irgend etwas nicht stimmt, rufe Deinen Vorgesetzten an und informiere ihn darüber, dass irgend ein Fehler vorliegt“ ist eindeutig zu grobmaschig und berücksichtigt die Eigenschaften des konkreten Notfalls zu wenig. Dagegen steht die Empfehlung, zusammenhängende Teilnotfälle auch zusammenhängend zu betrachten, bzw. ähnliche Notfälle in Gruppen mit einem einheitlichen Notfallkonzept zusammenzufassen. Ein Konzept der Form „Wenn die linke Tür zum Büro sich nicht öffnen lässt, weil dahinter eine Kiste mit 42kg Gewicht steht, tue folgendes...“ ist zu feinmaschig und betrachtet unnötige Details. Deshalb ist es wichtig, einen Mittelweg zu finden. Im Szenario könnte er beispielsweise daraus bestehen, bei einer Anomalie mit dem Internetzugang oder ungewöhnlichem Netzverkehr oder anderen Anzeichen für Angriffe zunächst die Firewall und ihre Konfiguration zu überprüfen (grobes Notfallkonzept). Falls hier etwas gefunden wird, werden die Maßnahmen des groben Notfallkonzepts angestoßen. Andernfalls wird für das beobachtete Symptom das entsprechende feine Notfallkonzept abgearbeitet.

Fazit und Ausblick

Schon lange vor der Zeit des Computers gab es ein Wechselspiel von Notfall, Notfallkonzept und der Bearbeitung des Notfalls. Seit jeher wurden für Notfälle aller Art Konzepte für ihre Bekämpfung erstellt, die dann durch Erfahrungswerte mit dem konkreten Notfall verbessert wurden.
Unter anderem brachte das Computerzeitalter den IT Vorfall oder IT Notfall als Neuerung mit sich. Während Organisationen herkömmliche, nicht IT bezogene Vorfälle weitgehend selber bearbeiteten und bearbeiten, da hier das Prozedere eingeübt und bekannt war, wurden sie vom rasanten Fortschritt der IT nahezu überrollt. Innerhalb kurzer Zeit wurde es für die meisten Organisationen unumgänglich, eine IT Komponente in die eigene Struktur zu integrieren. Die Möglichkeiten und der Nutzungsumfang der IT wuchsen jedoch schneller als das IT Sicherheitsbewusstsein, weshalb IT Vorfälle bis heute für viele Organisationen Existenz bedrohend sein können.
Um Organisationen hierfür eine Stütze zu geben, wurden die IRTs geschaffen. Sie sollen Organisationen helfen, mit IT Vorfällen fertig zu werden, wenn in der Organisation selber dazu nicht die Möglichkeit besteht. Dies ist vergleichbar mit der Feuerwehr, die im Brandfall der Organisation zur Seite steht, die das Feuer nicht selber löschen kann. Nur sind IT Vorfälle so viel komplexer als ein einfaches Feuer, dass ein einheitliches IRT nach dem Vorbild der Feuerwache zur flächendeckenden und umfangreichen Vorfallsbekämpfung nicht ausreicht. Also spezialistisierten sich die IRTs, und viele Organisationen bildeten ihre eigenen IRTs, die im Notfall Hilfe leisten sollten.

Das Phänomen des IT Notfalls ist noch relativ neu. Besteht für ihn ebenfalls der Zyklus von Notfall, Notfallkonzept und tatsächlicher Vorfallsbearbeitung? Kann auch hier die Bearbeitung des Notfalls oder Vorfalls, der im IT Bereich der Name Incident Response gegeben wurde, Verbesserungen für das Notfallkonzept aufzeigen? Ein solcher Zyklus der Beeinflussung ist selbstverständlich vorhanden, denn das Grundprinzip hat sich nicht geändert, nur weil der Vorfall jetzt das IT System betrifft. Da Erfahrungswerte mit IT Vorfällen oftmals erst noch gesammelt werden müssen und durch die technische Entwicklung andauernd neue Möglichkeiten für IT Vorfälle entstehen, ist der Rahmen der Beeinflussbarkeit sogar sehr groß.

Wenn vom Einfluss von Incident Response auf Notfallkonzepte (und andere Bekämpfungsmaßnahmen) gesprochen wird, so ist damit der Einfluss der tatsächlichen, durchgeführten Incident Response auf die geplante, noch nicht durchgeführte Incident Response gemeint. Denn die in Notfallkonzepten und anderen Maßnahmenkatalogen vorgeplanten Schritte sind nichts anderes als geplante Incident Response. Es geht also letztlich darum, wie praktizierte Incident Response sich selber verbessern kann.

Diese Arbeit hat anhand von Szenarien einige Facetten möglicher Einflussnahme aufgezeigt. Zunächst einmal ist klar geworden, dass kaum ein Vorfall mit einem Notfallkonzept alleine angemessen bekämpft werden kann. Vielmehr ist ein Zusammenspiel von Präventivmaßnahmen, Notfallkonzept und langfristigen Maßnahmen erforderlich (siehe Abbildung 8). Bei einigen Vorfällen hat das Notfallkonzept sogar nur einen sehr geringen Anteil an der Summe der nötigen Maßnahmen. Ein Beispiel hierfür lieferte das erste Szenario mit einem Vorfall der Datenspionage. Um der Tragweite von Incident Response für Verbesserungsmöglichkeiten an Maßnahmenkatalogen gerecht zu werden, dürfen Notfallkonzepte also auf keinen Fall alleine betrachtet werden. Es ist nötig, alle Maßnahmen in ihrer zeitlichen Staffelung zu betrachten.

Die Szenarien haben gezeigt, dass Incident Response auf alle drei zeitlichen Kategorien von Maßnahmen verbessernd einwirken kann. In welchem Umfang dies tatsächlich geschieht, hängt von mehreren Faktoren ab. Zunächst sind je nach Vorfall die drei Arten von Maßnahmen unterschiedlich bedeutsam. Beispielsweise liegt bei Datenspionage der Schwerpunkt auf der Prävention, bei der Epidemie war das Notfallkonzept besonders bedeutsam, und beim Brandvorfall waren alle drei Arten etwa gleichbedeutsam.
Außerdem ist der Grad der Einflussnahme abhängig davon, wie gut die Maßnahmen vor dem Vorfall bereits geplant waren. Wenn die ergriffenen Maßnahmen den Vorfall optimal bekämpft haben, brauchen sie nicht weiter verbessert zu werden. Ein weiterer wichtiger Faktor liegt in der Person oder Organisation, die die Maßnahmen der Incident Response tatsächlich ausführt. In den Szenarien dieser Arbeit war stets ein spezielles IRT damit betraut. Grundsätzlich ist es aber nicht erforderlich, dass eine Organisation für einen Vorfall ein IRT zu Rate zieht. Ohne IRT könnten die gesammelten Erkenntnisse und damit die Verbesserungsmöglichkeiten anders ausfallen.

Somit kann abschließend gesagt werden, dass praktizierte Incident Response einen großen Einfluss auf die Erstellung und Weiterentwicklung von Notfallkonzepten und anderen Vorfallsbekämpfungsmaßnahmen hat. Dies gilt insbesondere dann, wenn die Arbeiten der Incident Response von einem IRT durchgeführt werden, wie die Szenarien dieser Arbeit gezeigt haben.
Wie der Einfluss jedoch im Einzelnen aussieht, hängt sehr stark vom jeweiligen Vorfall, von der bestehenden Vorausplanung, von den Gegebenheiten im Umfeld des Betroffenen und zahlreichen weiteren Faktoren ab.

Literaturverzeichnis

[BDSG]	Bundesdatenschutzgesetz, präsentiert auf „Bundesdatenschutzgesetz (BDSG)“, URL http://www.datenschutz-berlin.de/recht/de/bdsg/bdsg1.htm, Stand 8.5.2003
[Boran]	S. Boran “The IT security Cookbook – Security organisation” vom 16.10.2002, präsentiert auf „The IT security Cookbook – Security organisation“, URL http://www.windowsecurity.com/whitepapers/ The_IT_Security_Cookbook__Security_organisation_.html#Heading32, Stand 17.04.2003
[Brunnstein 99]	K. Brunnstein „From AntiVirus to AntiMalware Software and Beyond: Another Approach to the protection of Customers from Dysfunctional System Behaviour” Paper presented at 22. National Information Systems Security Conference Arlington/Washington, USA, 18-21. Oktober 1999.
[Brunnstein 02]	K. Brunnstein „Risikoanalyse, Risikomanagement und Forensische Informatik“ Vorlesungsunterlagen, Universität Hamburg, Fachbereich Informatik, 2002
[BSI]	Bundesamt für Sicherheit in der Informationstechnik „IT Grundschutzhandbuch“, präsentiert auf „IT Grundschutzhandbuch“, URL http://www.bsi.bund.de/gshb/deutsch/menue.htm, Stand 17.4.2003
[CERT/CC]	Homepage des Computer emergency response team coordination center, “CERT Coordination Center”, URL http://www.cert.org/, Stand 20.7.2003
[DFN CERT]	Homepage des Computer emergency response teams des Deutschen Forschungsnetzes, „DFN-CERT: Homepage“, URL http://www.cert.dfn.de/, Stand 20.7.2003
[FIRST]	Homepage des Forum of incident response ans security teams, “Forum of Incident Response and Security Teams”, URL http://www.first.org/, Stand 20.7.2003

[Forcht]	K. A. Forcht „Computer Security Management“ Boyd & Fraser 1994
[Freitag]	S. Freitag, „Webbasiertes Auffinden maliziöser Software mit fortschrittlichen heuristischen Verfahren“, Diplomarbeit an der Universität Hamburg, Fachbereich Informatik, Juli 2000
[Gruber]	A. Gruber „Erstellung und Einführung eines Notfallkonzeptes im IT Bereich eines Mittel- bis Großunternehmens“, präsentiert auf „D I P L O M A R B E I T“, URL www.google.de/search?q=cache:qi1ta49bsmMC:members.mcnon.com/agruber/Daten/DA_AntonGruber_free.pdf+notfallkonzept+computer&hl=de&ie=UTF-8 Stand 3.4.2003
[IRT]	Incident Response Team des Fachbereichs Informatik, „Sitzungsprotokoll vom 29.4.2003“, Universität Hamburg, Fachbereich Informatik 2003
[Jackson, Hruska]	R. M. Jackson; J. Hruska “Computer Security Reference Book” Butterworth Heinemann 1992
[Knaur]	Lexikografisches Institut München „Der Knaur Universal Lexikon in 15 Bänden“ Band 12, 1990
[Kossakowski 00]	K. P. Kossakowski „Information Technology Incident Response Capabilities“ Libri Books on Demand, 2000
[Kossakowski 03]	Homepage von K. P. Kossakowski, „Klaus-Peter Kossakowski“, URL http://www.kossakowski.de/index.htm, Stand 24.7.2003
[Krallmann]	H. Krallmann „EDV-Sicherheitsmanagement“ Erich Schmidt 1989, präsentiert in [Brunnstein 02]
[Mampu]	Malaysian Administrative Modernasation and Management planning unit “Glossary” präsentiert auf Mampu, URL http://www.mampu.gov.my/ICT/MyMIS/Glossary.pdf., Stand 17.04.2003
[MDSTV]	Mediendienste Staatsvertrag, präsentiert auf „Mediendienstestaatsvertrag“ URL http://www.datenschutz-berlin.de/recht/de/stv/mdstv.htm, Stand 8.5.2003

[Menne]	J. Menne, „Methoden der Vorfallserkennung und –analyse“, Diplomarbeit an der Universität Hamburg, Fachbereich Informatik, September 2003
[Moses]	R. Moses „Risk Analysis and Management“ präsentiert in [Jackson, Hruska]
[Mück, RRZ]	H. J. Mück, „RZ Memo, Jahrgang 9, Nummer 3-4 Sicherheit im Doppelpack, Aufbau eines DFN-Kompetenzzentrums im Bereich Netzwerksicherheit“, herausgegeben vom Regionalen Rechenzentrum der Universität Hamburg, ISSN 0939-0197, 1996
[Nedon]	J. Nedon „Ein IT Sicherheitskonzept für eine wissenschaftliche Einrichtung am Beispiel des Fachbereichs Informatik der Universität Hamburg“, Diplomarbeit an der Universität Hamburg, Fachbereich Informatik, 1999
[Pfleeger]	C. P. Pfleeger „Security in Computing“ Prentice Hall 1989
[RFC 2828]	R. Shirey, “Internet Security Glossary”, Mai 2000 präsentiert auf „RFC 2828 (rfc2828) – Internet Security Glossary” URL http://www.faqs.org/rfcs/rfc2828.html Stand 16.4.2003
[RFC 3227]	D. Brezinski, T. Killallea, “Guidelinies for Evidence Collection and Archiving”, Februar 2002, URL http://www.ietf.org/rfc/rfc3227.txt?number=3227, Stand 7.5.2003
[Stelzer]	D. Stelzer „Risikoanalyse Konzepte, Methoden und Werkzeuge“, präsentiert bei den Proceedings der Fachtagung SIS 1994, Universität Zürich-Irchel vom 10.-11.3.1994 URL www.wirtschaft.tu-ilmenau.de/im/infothek/documents/ Stelzer_Risikoanalyse_Konzepte_Methoden_Werkzeuge_1994.pdf, Stand 3.4.2003
[StGB]	Strafgesetzbuch, präsentiert auf „UB Mannheim: BB Rechtswissenschaft – Strafgesetzbuch“, URL http://www.bib.uni-mannheim.de/bib/jura/gesetze/stgb-inh.shtml, Stand 8.5.2003
[Ulrich]	C. Ulrich, „Computerbetrug (§ 263a StGB)JurPC Web-Dok. 189/1999, Abs. 1 - 45“, erschienen in „UR Internet Zeitschrift für Rechtsinformatik“, präsentiert auf http://www.jurpc.de/aufsatz/19990189.htm#ue11, Stand 17.7.2003

[West-Brown et al.]	M. J. West-Brown; K. P. Kossakowski; D. Stikvoort “Handbook for Computer security incident response teams” Pittsburgh, PA: Carnegie Mellon University 1998
[Wilbert]	P. Wilbert „Getting serious about security“, präsentiert auf “Kingsley IT Security Devision”, URL http://security.kingsley.co.za/articles/article16.htm, Stand 17.4.2003

Abbildungsverzeichnis

Ich versichere, dass ich die vorstehende Arbeit selbständig und ohne fremde Hilfe angefertigt und mich anderer als der im beigefügten Verzeichnis angegebener Hilfsmittel nicht bedient habe. Alle Stellen, die wörtlich oder sinngemäß aus Veröffentlichungen entnommen wurden, sind als solche kenntlich gemacht.

Benjamin Hoherz