ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

TIK Institut für Technische Informatik und Kommunikationsnetze

Kostenanalyse von präventiven IT-Sicherheitsmassnahmen

Semesterarbeit SA-2005-25
April bis Juli 2005

Professor: Bernhard Plattner
Betreuer: Thomas Dübendorfer
Verfasser: Markus Häcki

Einführung

IT-Sicherheit ist kein Neologismus der 90er Jahre. Schon vor dem Internetzeitalter war die IT diversen Bedrohungen ausgesetzt. Früher konnte der Verbreitung von Viren mittels Diskette noch mit relativ einfachen organisatorischen Mitteln entgegnet werden. Bedrohungen die von den eigenen Mitarbeitern ausgehen, stellen nach wie vor ein grosses Problem dar. Das ungewollte Löschen von Dateien kann verheerende Folgen nach sich tragen, wenn nicht ein regelmässiges Backup durchgeführt wird. Datenverlust kann aber auch durch technische Defekte der Hard- und Software entstehen. Damit bei solchen technischen Defekten die Kapazität des Systems nicht verkleinert wird, müssen Sie redundant konzipiert werden. Auch die physische Einbruchssicherheit ist ein relevantes Thema der IT-Sicherheit.

Mit der Integration des Internets in die Unternehmens-IT hat sich das Sicherheitsbedürfnis aber verändert. Der schnelle Austausch von Informationen über das Netz birgt die Gefahr in sich, dass sich Viren und Würmer installieren können, und Schaden anrichten. Ohne zusätzliche Massnahmen wäre das IT-System eines Unternehmens nicht lange online. Komponenten wie Firewall, Antivirenprogram, Antispamprogram usw. sind nötig, um ein funktionsfähiges Netzwerk zu betreiben. Wegen des schnellen Wandels in diesem Business werden zusätzliche IT-Arbeitskräfte benötigt. Alle diese neu anfallenden Arbeiten und Kosten sind in der letzten Zeit stetig gewachsen, ohne dass man ihnen ein spezielles Augenmerk gerichtet hätte. Der mit dem Internet hinzugewonnene Nutzen übertrifft diese Kosten aber immer noch bei weitem![1]

Aus diesen Gründen widmet sich die vorliegende Arbeit den neuen Aufgaben der IT-Sicherheit. Sie untersucht worin die Neuerungen bestehen und was schon immer nötig war. In einem weiteren Schritt wird der Versuch gestartet die neu auftretenden Kosten zu strukturieren und Grössenordnungen zu beschreiben.

Dazu wurden insgesammt 13 Interviews geführt. Sieben davon mit IT nutzenden Unternehmen und die übrigen sechs mit IT-Sicherheitsfirmen, die den umfassenden Schutz von Hard- und Software zu ihrer Kernkompetenz ernannt haben. An den sieben IT nutzenden Unternehmen wurde das zuvor erarbeitete Massnahmen-Kosten Modell getestet. Die Kosten der von ihnen unternommenen Massnahmen wurden evaluiert. Die ürsprüngliche Idee, zwei der sieben Kostenbeispiele den IT-Sicherheitsfirmen zu unterbreiten, damit sie eine unverbindliche Offerte erstellen könnten, hat sich als ein nicht umsetzbares Projekt erwiesen. Die ungenauen Angaben wurden damit begründet, dass sich die Kosten je nach Sicherheitsbedürfnis des Unternehmens bis zu einem Faktor fünf unterscheiden können. Daher resultierten aus den Interviews mit den IT-Sicherheitsunternehmen lediglich qualitative Ergebnisse.

[1] Diese Aussage stützt sich auf das Resultat aus den Befragungen, dass 99.95% aller Clients der befragten Firmen die ganze Zeit mit dem Internet verbunden sind.

Aufgabenstellung

Basierend auf einer früheren Semesterarbeit von Bodo Hechelmann am TIK zu einem “Kostenmodell zu präventiven IT-Sicherheitsmassnahmen” [SA04], soll eine umfassende Kostenanalyse durch Erweiterung des Kostenmodells und durch Erhebungen der Präventionskosten in Schweizer Grossunternehmen durchgeführt werden. Daraus soll ersichtlich sein, wie stark präventive Massnahmen das IT-Budget von Unternehmen belastet. Soweit wie möglich sollen Potentiale und Weisungen bezüglich dem Vorgehen aufgespürt und unterbreitet werden.

Erwartete Resultate

Die folgenden Resultate werden erwartet:

1. *Erweitertes Systemmodell* Zur Abgrenzung der Arbeit soll das bestehende Systemmodell erweitert werden, um die von präventiven IT-Sicherheitsmassnahmen betroffenen Objekte und zu identifizieren.

2. *Aufstellung zu Präventionskosten* Eine umfassende kategorisierte Liste soll möglichst umfassend die Präventionskosten aufzeigen. Diese Liste soll als Grundlage für die Bemessung der totalen Präventionskosten in Unternehmen eingesetzt werden können.

3. *Interviewplanung* Da ein grosser Teil der Informationen durch Interviews gesammelt wird, soll möglichst frühzeitig in einem Interviewplan festgelegt werden, welche Institutionen und Personen befragt werden. Zudem wird ein Fragenkatalog erstellt, der die Antworten-Konsolidierung für das zu entwickelnde Kostenmodell unterstützt.

4. *Fallbeispiele* Zur Validierung der Nützlichkeit und Vollständigkeit des Modells sollen zumindest zwei verschiedene konkrete Fallstudien gerechnet werden und in Follow-Ups zu den Interviews den beteiligten Personen präsentiert und mit ihnen diskutiert werden. Sofern eine auskunftsbereite Firma, die einen grösseren Virenbefall hatte, gefunden werden kann, sollen die Kosten der Virenbeseitigung abgeschätzt werden und in Relation zu den Präventionskosten gesetzt werden.

5. *Dokumentation* Die schriftliche Dokumentation soll die durchgeführten Arbeiten und erhaltenen Resultate im Rahmen dieser Arbeit anschaulich und prägnant beschreiben. Der Inhalt soll u.a. die Aufgabenstellung, Bezug zu bestehenden Arbeiten, das Systemmodell, die Aufstellung der Präventionskosten, die Interviewergebnisse, das Kostenmodell, die Fallbeispiele, Schlussfolgerungen und einen Ausblick für mögliche Folgearbeiten oder Erweiterungen enthalten.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1 Situationsanalyse und Systemabgrenzung

Dieses Kapitel gibt einen groben Überblick zu den verschiedenen Facetten der IT-Sicherheit und zeigt auf, worauf sich diese Arbeit konzentriert. Besonderen Wert wird darauf gelegt, zunächst alle möglichen Aspekte zu berücksichtigen. Zeitliche, räumliche und organisatorische Dimensionen kommen hier zur Sprache. Den Begriff Sicherheit an sich und die dazu notwendigen Massnahmen werden erläutert und auf Neuheit geprüft. Die Abgrenzung des betrachteten Systems ist ebenso Inhalt dieses Kapitels, wie der Vergleich mit bisherigen Arbeiten ähnlicher Thematik.

1.1 Situationsanalyse von verschiedenen Sicherheitsaspekten

1.1.1 Definition der Grundziele

Der Zustand der Sicherheit wird in verschiedenen Definitionen als subjektiv beschrieben, und kann nur zu einem Teil in absolute Zahlen gefasst werden. Verschiedene nachfolgende Definitionen sollen einen Überblick geben, was man unter dem Begriff Sicherheit im Allgemeinen und im Speziellen (in der IT-Sicherheit) versteht. Im Risikomanagement wird die Sicherheit nach der Norm ISO 14971 [BA05] folgendermassen beschrieben:

> Sicherheit ist die Freiheit von nicht akzeptablen Risiken.

Aus dieser Definition lässt sich schlussfolgern, dass man unterscheiden kann zwischen akzeptablen und nicht akzeptablen Risiken. Was akzeptabel genau bedeutet ist individuell definierbar. Hier kommt das Element der Empfindung deutlich zum Ausdruck. Etwas aussagekräftiger ist die Definition der Fachhochschule Heilbronn [FH05]:

> Im Zustand der Sicherheit liegen keine oder nur geringe Gefahren vor. Gefahren gehen von Bedrohungen aus und können durch Schutzmaßnahmen vermindert werden. Das Risiko einer Gefahr ist im Zustand der Sicherheit minimal. Das verbleibende Restrisiko wird akzeptiert oder kann an Versicherungsgesellschaften überwälzt werden.

Hier wird der Zustand der Sicherheit erst mal mit keiner bis geringer Gefahr beschrieben. Aus der Sicht der IT-Sicherheit ist der Zustand ohne Gefahr sicherlich eine unerreichbare Idealvorstellung. Dennoch, so die Definition, können die Risiken mittels Massnahmen vermindert werden. Auf diese Weise kann ein Zustand im Verhältnis sicherer gemacht werden. Das Abwälzen des Restrisikos ist auch in der IT-Branche eine mögliche Methode. Die Universität Mannheim [UN05] nimmt einen spezifischeren Bezug auf die Informationstechnologie und gibt folgende Definition der Sicherheit:

> Schutz von Informationsquellen vor unberechtigten Änderungen, Zerstörungen oder Preisgabe, unabhängig davon, ob sie absichtlich oder unabsichtlich erfolgten. IT-Sicherheit wird angestrebt durch die Einhaltung bestimmter Sicherheitsstandards, die die Verfügbarkeit, Unversehrtheit und Vertraulichkeit von Informationen erhalten sollen. Sicherheit in der IT wird durch direkte Sicherheitsvorkehrungen in informationstechnischen Systemen (oder Komponenten) und indirekt durch die Anwendung von Regelungen und informationstechnischen Systemen (oder Komponenten) erreicht.

Diese Definition entspricht am ehesten den gängigen Sicherheitsvorstellungen in der IT-Praxis. Doch lässt sich die IT-Sicherheit nicht nur auf die drei Gebiete Verfügbarkeit, Vertraulichkeit und Unversehrtheit (Integrität) beschränken. Vielmehr sind mit den wachsenden Möglichkeiten auch neue Anforderungen an die Sicherheit gestellt worden. Die Authentizität und die Zurechenbarkeit sind mitunter Anforderungen des e-commerce, die miteinbezogen werden müssen. Zur Veranschaulichung illustriert nachfolgende Liste die Aufgaben der IT-Sicherheit (siehe dazu [MM04] und [FD05]):

Autorisierung: Die Arbeitenden im LAN sind die autorisierten Personen

Authentizität: Die Information stammt vom angegebenen Absender

Unversehrtheit: Die Information erreicht den Empfänger unverändert (auch Integrität genannt)

Vertraulichkeit: Die Information kann nur der vorgesehene Empfänger lesen

Verfügbarkeit: Die Kommunikation zwischen Absender und Empfänger ist jeder Zeit möglich

Zurechenbarkeit: Das Absenden bzw. Empfangen einer Nachricht kann unabstreitbar nachgewiesen werden

Damit sind die Grundziele der IT-Sicherheit festgelegt.

1.1.2 Sicherheitsmassnahmen

Die verschiedenen Massnahmen welche die zuvor definierten Ziele erreichen sollen, lassen sich aus den Sicherheitshandbüchen von Deutschland [GS05] und Österreich [GS05] ableiten. In diesen sehr umfassenden Dokumenten werden verschiedene Massnahmen bzw. Kriterien festgelegt, um das Sicherheitszertifikat des jeweiligen Landes zu erhalten. In der Schweiz kennt man bisher noch kein solches Zertifikat. Aufgrund dieser Quellen definieren wir sieben Bereiche, die Einfluss auf die Risikominimierung haben.

IT-Sicherheitsmanagement Hierzu gehört das Erstellen einer Sicherheitspolitik aufgrund der vorliegenden Anforderungen, Gefahren und Möglichkeiten. Die Vorgehensweisen und die Prozessabläufe werden richtlinienartig festgehalten und die Verantwortlichen bestimmt. Es ist das wichtigste Gebiet der IT-Sicherheit, da hier die grundlegenden Entscheidungen gemacht werden.

Bauliche und infrastrukturelle Massnahmen Dieser Bereich behandelt alle Gefahren, die nicht virtueller Natur sind. D.h. jegliche physisch negativ einwirkenden Kräfte auf das System müssen mit diesen Massnahmen behoben werden können. Diese Massnahmen umfassen bauliche Aspekte, um sich vor Einbrüchen, Bränden, Stromausfällen, Leitungsschäden und Abhörmanövern zu schützen. Die geeignete Einrichtung von Clients, Servern und Netzwerkkomponenten sind weitere Massnahmen in dieser Reihe. Die Umsetzung solcher Massnahmen hängt ganz davon ab, wie vertraulich das System sein soll.

Personelle Massnahmen In diesen Bereich gehören Regelungen für das Personal. Laut einer Aussage in einem Interview (siehe Seite 32) gehen die grössten Gefahren von den eigenen Mitarbeitern aus. Gewollt oder nicht komme es sehr oft vor, dass wichtige Daten gelöscht werden. Gerade deshalb ist ein darauf ausgerichtetes Konzept im Bereich Personal von grosser Bedeutung. Schulungen, bei denen die Mitarbeiter auf die Gefahren sensibilisiert werden, gehören ebenfalls in dieses Gebiet hinein.

Systementwicklung Um den gesamten Lebenszyklus des IT-Systems sicher managen zu können braucht es zusätzliche Massnahmen wie die Dokumentation von jeglichen Veränderungen. Es braucht vordefinierte Abläufe, z.B. wie neue Software aufgespielt wird.

Systemsicherheit Diesen Bereich umfasst das, was man im klassischen Sinn unter der IT-Sicherheit versteht. Dazu gehört der Schutz vor Viren, unerlaubten Zugriff, Spammails sowie der sichere Remote Access bzw VPN Zugang. Auch die ganze Netzwerkarchtitektur mit Redundanzen und DMZ-Anordnungen gehören zu diesem Themengebiet.

Sicherheit im laufenden Betrieb Die Wartung der Systeme wird hier eingeordnet. Das einspielen von Sicherheitspatches und von neuen Virensignaturen sowie die Reaktion auf sich neu abzeichnende Trends. Zu letzterem gehört auch die Selbstschulung der Administratoren.

Disaster Recovery Um sich gegen den „worst-case“ zu wappnen, braucht es Datensicherungen, die eine Wiederherstellung von verlorenen Daten erlauben. In dieses Kapitel gehört auch die Anfertigung eines Notfallplanes. Darin wird festgehalten, welche Kapazitäten redundant benötigt werden, damit trotz Ausfall noch weitergearbeitet werden kann. Ein Notfallplan beinhaltet auch die Überlegung wer in einem konkreten Angriffsfall was zu erledigen hat.

Diese sieben Bereiche können durch ihrer gegenseitigen Abhängigkeiten wie in Abbildung 1 dargestellt werden.

Wegweisend ist das IT-Sicherheitsmanagement, das den ganzen Rahmen und die nötigen Ressourcen bereitstellt. Auf der nächsten Stufe erkennt man zwei Ebenen. Auf der einen die Mitarbeiter, die durch die personellen Massnahmen auf die individuellen Sicherheitsaspekte geschult werden und auf der anderen die Infrastruktur, die bauliche und systembezogene Massnahmen aufweist. Das Disaster Recovery gehört durch die Datensicherung und die Notfallplanung sowohl zur infrastrukturellen Ebene als auch zum Kern des Sicherheitsmanagements.

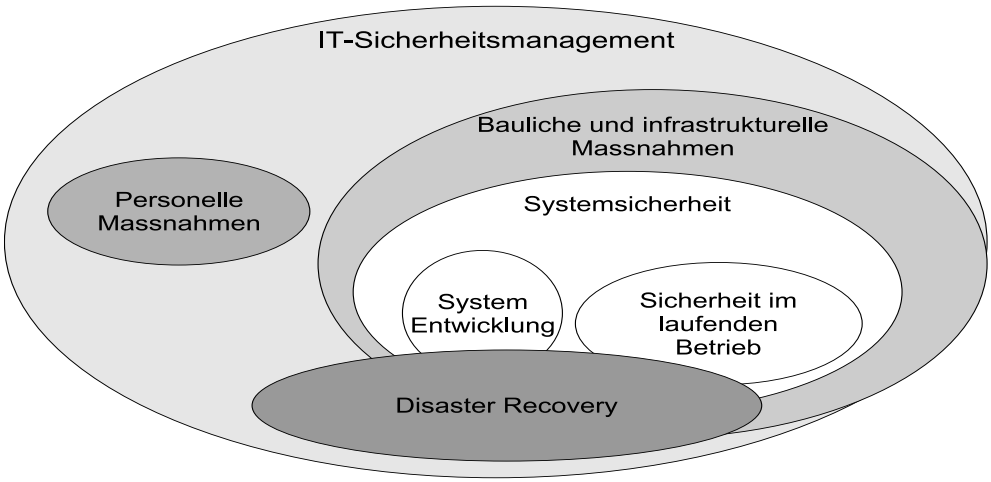


Abbildung 1: IT-Massnahmenbereiche

1.1.3 Sicherheitsphasen

Alle im Unterkapitel 1.1.2 dargestellten Massnahmen gehören zur pre Incident Phase (siehe Abbildung 2)[2]. Das heisst, dass sie **vor** einem möglichen Angriff (Ereignis) stattfinden müssen, damit sie ihre Wirkung haben. In der post Incident Phase (Phase 2) sind diejenigen Massnahmen enthalten, die **nach** einem Angriff anfallen. Ihr Ziel ist es, den ursprünglichen Zustand so schnell wie möglich wiederherzustellen. Je nach Vorgehensweise dauert diese Angelegenheit mehr oder weniger lang. Die Kosten steigen mit jedem Tag, bei dem die Systeme nicht laufen.

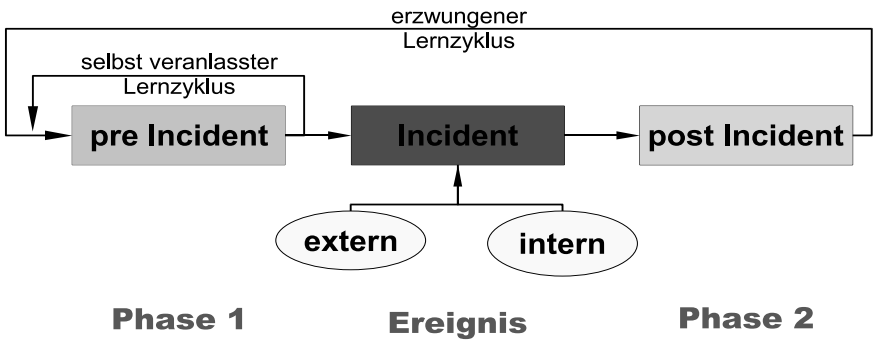


Abbildung 2: Phasenmodell

In der Idealvorstellung würde man nun abwägen, welche Kosten höher sind: pre Incident Kosten im Vergleich zu post Incident Kosten. Die post Incident Kosten müssen mit einem Wahrscheinlichkeitskoeffizient multipliziert werden, damit sie mit den pre Incident Kosten verglichen werden können. Im Allgemeinen ist es sinnvoller, den Lern- bzw. Fortschrittszyklus selbstständig zu ver-

[2]Die Präsentation [NM04] hat diese Abbildung inspiriert.

anlassen, als nach einem Incident sich erzwungenermassen an neue Entwicklungen anpassen zu müssen.

1.2 Systemabgrenzung

An dieser Stelle wird das im Kapitel 1.1 beschriebene System von Zielen, Massnahmen und Phasen im Sinne des Problemlösungszykluses der Systems Engineering Lehre [ZR99] abgegrenzt. Damit das Thema dieser Arbeit vertieft werden kann und es nicht bei einer oberflächlichen Beschreibung des Systems bleibt, werden lediglich die seit Beginn des globalen Internets (ab ca. 1995) neu aufgetauchten Bedrohungen untersucht. Das zu analysierende System umfasst die Prävention vor Angriffen, welche durch die Internetleitung in die Systeme eindringen und Schaden anrichten.

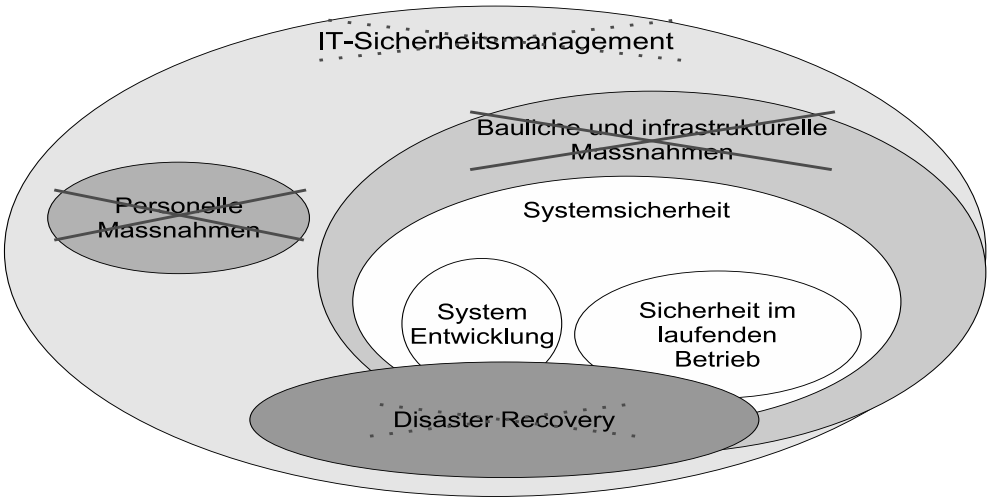


Abbildung 3: Eingrenzung der zu betrachtenden IT-Massnahmenbereiche

Zur alten IT-Sicherheit gehören die baulichen und infrastrukturellen Massnahmen, sowie die personellen Massnahmen. Die Gefahr des Einbruchs bzw. Diebstahls oder des internen Angriffs haben seit der Einführung der IT bestanden und haben sich durch das Internet auch nicht verändert (anschaulich zu betrachten in der Abbildung 3). Diese Massnahmen fallen daher nicht in das Betrachtungsfeld dieser Kostenanalyse. Das IT-Sicherheitsmanagement ist ebenfalls kein neues Element in der Handhabung eines IT-Systems. Dennoch lässt sich sagen, dass der Arbeitsaufwand in diesem Bereich mit dem Internet zugenommen hat. Es müsste also eruiert werden, wieviele der Kosten, die das IT-Sicherheitsmanagement verursacht, von alten resp. neuen Gefahren ausgehen, um eine genaue Abgrenzung vornehmen zu können. Auch das Disaster Recovery besteht nur aus alten Massnahmen. Doch hat sich auch der Umfang dieser Massnahme in den letzten Jahren vergrössert. Die nötigen Massnahmenpläne müssen ausgeklügelter sein, da ein Hackerangriff das ganze System lahm legen kann. Im Vergleich dazu sind die Gefahren, die früher schon bestanden haben, wie z.B der zufällige Ausfall einer einzelnen Hardwarekomponente, nicht weiter bedenklich. Realistisch betrachtet wird es nicht möglich sein, diese Differenzierung exakt vorzunehmen. Einfacher siehts mit der Systemsicherheit aus. Wie im Unterkapitel 1.1.2 beschrieben, sind die wirklich neuen Elemente der IT-Sicherheit darin enthalten.

In der zeitlichen Dimension wird das betrachtete System auf die Phase vor dem Incident beschränkt:

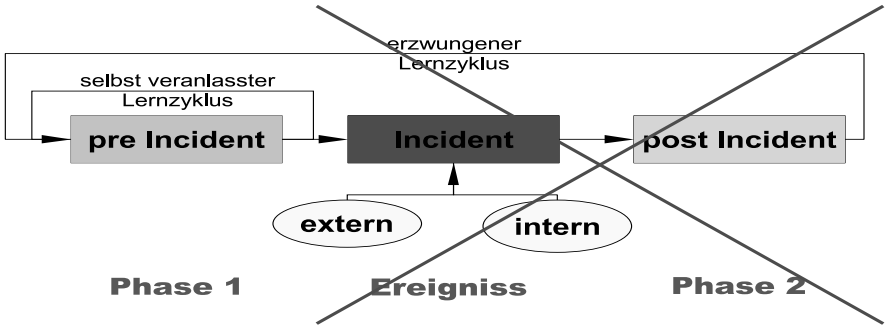


Abbildung 4: Eingrenzung der zu betrachtenden Phasen

1.3 Parallelen zu früheren Arbeiten

Diese Arbeit steht im Zusammenhang mit dem ETH Forschungsprojekt DDoSVax [DD05]. Eine ebenfalls von diesem Forschungsprojekt vorangegangene Studie von Bodo Hechelmann [SA04] hat das gleiche Betrachtungssystem von der Theorie aus analysiert. Deshalb beschäftigt sich diese Studie überwiegend mit konkreten Beispielen unterschiedlicher Unternehen. Diese Studie basiert auf der Arbeit von Herrn Hechelmann. Im Unterschied dazu wird aber bei der vorliegenden Studie ein stärkeres Gewicht auf die neuen Sicherheitselemente gelegt. So werden z.B. Datenbackups in dieser Arbeit ausser Betracht gelassen.
Eine weitere Kostenstudie, die sich jedoch auf die post Incident Kosten konzentriert, ist die Arbeit von Jürg Schmid und Peter Weigel [SA03]. Diese Arbeit weist dementsprechend nur wenig Parallelen auf.

2 Methodik

In diesem Kapitel wird die methodische Vorgehensweise beschrieben. Vom theoretischen Modell ausgehend über die Interviews bis hin zu den Auswertungsmethoden wird ein Überblick über die Entstehung der Resultate geliefert. Dabei wird auch beschrieben inwiefern die Resultate verlässlich sind oder noch relativiert werden müssen.

2.1 Erstellung eines theoretischen Modells

Das theoretische Modell wurde teils aus der vorgängigen Arbeit von Bodo Hechelmann und teils aus den Sicherheitsanweisungen der Sicherheitshandbücher von Deutschland und Österreich aufgestellt. Alle Kostenpunkte, die in das oben beschriebene Betrachtungssystem gehören, wurden evaluiert. Nach diversen Interviews mit Sicherheitsverantwortlichen und Sicherheitsexperten musste das Kostenmodell ein bisschen ausgeweitet werden. Die Details zu dem Modell finden sich im Kapitel 3.

2.2 Interviews mit Unternehmen

Damit das theoretische Modell verifiziert und ausgebaut werden kann, wurden verschiedene Unternehmen befragt. Insgesamt haben 7 Firmen mit zwischen 5 und 80’000 Mitarbeitern an der Befragung mitgemacht (Die Kosten der einzelnen Firmen sind im Anhang zu finden). Ein Interview dauerte ca. 1.5 Stunden und umfasste zwei Teile. Im ersten Teil ging es darum das Unternehmen zu charakterisieren, damit die anfallenden Kosten später verglichen werden können. Im zweiten Teil wurden die Kosten anhand der Kostenanalysematrix (siehe Seite 17) ermittelt. Da die Unternehmen unterschiedliche Lohnansätze haben und dies eine Verzerrung des Kostenvergleiches verursacht, wurden die durchschnittlichen Lohnkosten vom Bundesamt für Statistik [BU05] eingesetzt. Ein Informatiker verdiente 2004 in Zürich bei der Verrichtung von höchst anspruchsvoller und qualifizierter Arbeit 8667.- im Monat. In dieser Studie wurden Jahreslohnkosten von 130’000 eingerechnet. Für die Lohnkosten von Nicht-Informatikern wurden die in Zürich durchschnittlichen 4282.- Franken im Monat resp. die jährlichen 56’000.- angenommen.
Der Versuch die Kosten zu detektieren ist formell gelungen. Obwohl die Resultate teils auf Schätzungen der Sicherheitsverantwortlichen basieren, dürfen sie als gegeben betrachtet werden. Dennoch ist es sehr schwer diese Kosten mit denen anderer Firmen in ein Verhältnis zu setzen. Damit das Sicherheitsniveau eines Firmensystems analysiert, und verglichen werden kann, bräuchte es eine genaue Untersuchung des gesamten IT-Systems. Dies würde ein Vielfaches der Zeit einer Semesterarbeit erfordern. Deshalb ist es wichtig an dieser Stelle zu betonen, dass die aufgezeigten Kostenstrukturen Beispiele sind, und deshalb lediglich die Grössenordnungen verglichen werden können.

2.3 Interviews mit IT-Sicherheitsunternehmen

Zur Vertiefung in die Materie wurden spezialisierte IT-Sicherheitsunternehmen gesucht, welche bereit waren, die Sicherheit von zwei der befragten Unternehmen (siehe S.39) zu analysieren. Wenn möglich sollte eine unverbindliche Offerte Klarheit über die Sicherheitskosten der beiden Beispielfirmen verschaffen.
Das angestrebte Ziel, einen angemessenen Vergleich machen zu können, musste jedoch schon sehr bald korrigiert werden. In den Interviews mit den Sicherheitsexperten kam deutlich zum Vorschein,

dass das Sicherheitsdispositiv einer Firma sehr unterschiedlich ausgestaltet werden kann und dass die Kosten je nach Wunsch gut fünf mal höher sein können. Dennoch soll es möglich sein, eine Vorstellung zu vermitteln, welches die kostentreibenden Elemente in der IT-Sicherheit sind, und worauf allenfalls verzichtet werden kann. Diese Interviewreihe ergab einen Einblick in die neu entstandene IT-Sicherheitsbranche.

2.4 Auswertungsmethode

Bei der geringen Anzahl von Befragungen sind die Resultate einer statistischen Auswertung fragwürdig. Dies wird gestützt durch die Aussage des Interviews [INTa], wonach die IT-Sicherheit ein Investitionsgut sei. Dies ist ein komplexes Produkt, welches nur grobe statistische Vergleiche zulässt.
Der Auswertungsmechnanismus ist eine Art Delphimethode [TA05]. Mit dieser Methode werden Interviews geführt und die Gesamtresultate den interviewten Experten zur Überprüfung nochmals vorgelegt. Sie können dann Änderungen vornehmen, die ebenfalls in die Schlussarbeit aufgenommen werden. Die Delphimethode wird angewendet, damit sich die verschiedenen Meinungen angleichen, und Extrempositionen ausgemerzt werden. In dieser Arbeit dient sie als Kontrolle von Resultaten und Zitaten.

3 Das Massnahmen-Kosten Modell

In diesem Modell werden alle Massnahmen den dadurch entstehenden Kosten in einer Matrix gegenübergestellt. Mit einer solchen Kostenanalysematrix können die IT-Sicherheitsausgaben buchhalterisch erfasst werden. Dieses Modell beinhaltet jedoch keine Bewertung der Kosten wie es eine Total Cost of Ownership (TCO) oder eine Return On Security Investment (ROSI) Methode macht. In jedem Sicherheitsdispositiv gibt es eine Reihe von Massnahmen, die der Risikominimierung dienen. Gewisse Massnahmen wurden erst im Laufe der Interviews entdeckt und kommen in den Kostenmodellen der interviewten Unternehmen nicht vor. Diese Auflistung hat nicht den Anspruch auf Vollständigkeit.

3.1 Sicherheitsmassnahmen

In nachfolgender Abbildung sind die verschiedenen Bereiche dargestellt, in welche sich die Massnahmen eingliedern lassen. Mittels umfassender Analyse wird das Sicherheitskonzept erstellt, welches festlegt, welche weiteren Massnahmen nötig sind, damit das Risiko bis auf ein akzeptables Restrisiko reduziert werden kann.

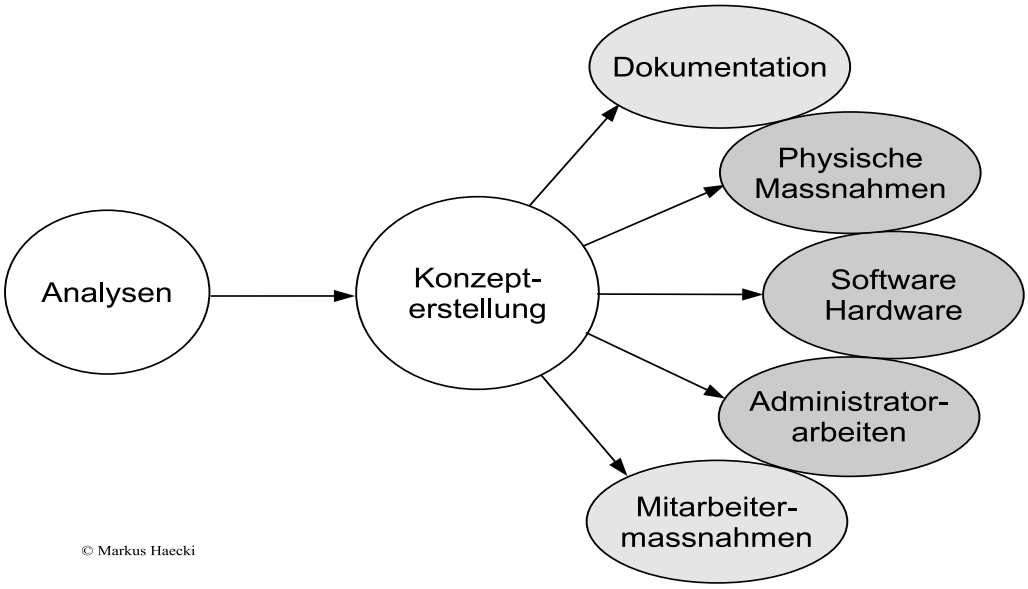


Abbildung 5: Massnahmenschild

3.1.1 Analysen

Eine wichtige Voraussetzung für einen erfolgreichen Schutz des IT-Systems ist das Analysieren der Gegebenheiten und Notwendigkeiten. Es gibt verschiedenste Faktoren, die mit dieser Massnahme betrachtet werden müssen, damit die Konzeptuierung auf möglichst genauen Fakten aufgebaut werden kann. Folgende Analyseformen sind bekannt:

Mit einer *Analyse durch Externe* wird verhindert, dass Betriebsblindheit die Analyse verunschärft. Zudem hat diese Analysemethode einen positiven Nebeneffekt. So können externe Experten oft als Zugangskanal zu bisher verschlossenem Wissen genutzt werden.

Eine *Self-Attack* auf ein IT-System ist mit einer Impfung vergleichbar. Die Antikörperbildung entsteht jedoch nicht automatisch. Bei dieser Analyse enstehen lediglich Hinweise, wo noch Löcher im System zu finden sind. Laut der Aussage des Sicherheitsverantwortlichen eines Unternehmens (siehe Kostenbeispiel auf Seite 32) führen die Mitarbeiter meist ohne Aufforderung Self-Attacks durch.

Die *Risikoanalyse* dient dem Abschätzen der Wahrscheinlichkeit eines Schadenereignisses, sowie dem Ermessen des wirtschaftlichen Schadens im Falle eines solchen Ereignisses. Eine gute Risikoanalyse ist wegweisend für ein erfolgreiches Risikomanagement. Dieses im nächsten Unterkapitel Konzepterstellung weiter besprochen wird.

3.1.2 Konzepterstellung

Das Erstellen eines *Sicherheitskonzeptes* ist grundlegend für die gesamte IT-Sicherheit. Sie wird auf den zuvor getätigten Analysen aufgebaut und muss in regelmässigen Abständen überarbeitet werden.

Ein häufiger Ansatz des Sicherheitskonzeptes stammt aus dem Risikomanagement. Ziel ist es, das Risiko stufenmässig zu minimieren. In einer ersten Stufe müssen alle unnötigen Risiken vermieden werden. Dazu zählen z.B. das Öffnen von bizarren Emails sowie alle anderen unnötigen Aktivitäten im Internet. In einem zweiten Schritt werden risikoreiche Dienste des Internets verhindert. Mit Firewall, Antiviren- und Antispamsoftware kann das Gesamtrisiko um einen weiteren Grad verringert werden.

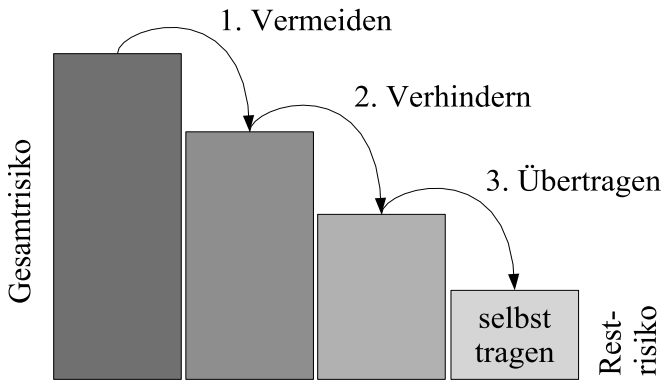


Abbildung 6: Risikomanagement

In einer dritten Stufe übergibt man die verbleibenden unakzeptablen Risiken externen Firmen (siehe Kapitel 4.2). Das verbleibende Risiko wird mit diesen drei Stufen klein gehalten, damit ein Schadenfall für die Firma verkraftbar wäre. Dieses Restrisiko muss selbst getragen werden.

Eine ebenso wirksame Methode ist die *Notfallplanung*, die schon vor einem eventuellen Incident erstellt werden muss. Damit kann das Risiko zwar nicht verkleinert werden, doch das Ausmass des Schadens kann mit einem geplanten Vorgehen entscheidend dezimiert werden. Jede Stunde, bei der die Systeme nicht arbeiten können, kostet riesige Summen. Laut der Semesterarbeit [SA03] steigen die Kosten nicht linear an, weil Forderungen von Dritten und Imageschaden erst später dazukommen.

3.1.3 Software und Hardware Produkte

Diese Massnahmenpakete umfassen den Einsatz von jeglichen Soft- und Hardware Tools die zu IT-Sicherheitszwecken verwendet werden. Dazu gehören auch solche Produkte, die lediglich als positiver Nebeneffekt eine gewisse Sicherheit gewährleisten wie z.B. ein Reverse Proxy, welcher verschiedene Funktionen übernimmt. Da es subjektiv ist, welcher Kostenanteil eines Reverse Proxys der Sicherheit angerechnet werden kann, wurden solche multifunktionale Produkte der Einfachheit halber in den Interviews nicht berücksichtigt.

	reine Sicherheitsprodukte	**Internet-Sicherheit als positiver Nebeneffekt**
Hardware	Firewall	Reverse Proxy Datenbackupsystem
Software	Firewall Antivirenprogramm Antispamprogramm Antispyware Intrusion Detection Systeme	Softwareverteilsystem Monitoring Software

Tabelle 1: Sicherheitsprodukte

Die sieben interviewten Unternehmen wurden zu den nachfolgenden Massnahmen befragt, ob und wie sie die Massnahmen einsetzen. Ebenso wurden deren Aufwände registirert (siehe dazu Anhang A.1)

Die *Firewall* grenzt das lokale Netzwerk vom Zugang nach aussen ab. Sie regelt sowohl den Zugriff von aussen nach innen, wie auch denjenigen von innen nach aussen. Dazu benötigt sie Regeln, wer worauf zugreifen darf. Diese Regeln sind dynamisch zu verwalten, so dass neue Gefahrenherde identifiziert und schnellst möglich von der Firewall boykottiert werden können. Eine Firewall kann sowohl auf den Clients als Software wie auch als Hardware dem Netzwerk im Stil eines Proxys vorgeschaltet werden. Sie registiert im Normalfall alle Ereignisse, damit Rückschlüsse gemacht werden können.

Das *Antivirenprogramm* schützt den Computer vor schädlichem Programmcode. Diese können in einem Dokument, oder als Trojaner in einem nützlichen Programm versteckt sein. Der Antivirenscanner überprüft den ganzen Datenstrom auf die ihm bekannten Virensignaturen. Dieses Programm erfordert ein regelmässiges Update auf die neusten Virensignaturen. Es ist dabei von

entscheidender Bedeutung, wie schnell nach dem ersten Auftreten eines Virus die entsprechende Signatur verfügbar ist.

Das *Antispamprogramm* schützt den Mailaccount (Mailserver) vor unerwünschten Mails. Es ist die Aufgabe dieses Programmes zu realisieren, welche Mails unerwünscht sind und welche nicht. Auch diese Art von Programmen bedarf oft eines regelmässigen Updates. Grey listing nützt hingegen die Tatsache aus, dass 97% der Spammails bei Nicht-ankommen kein zweites Mal verschickt werden [DS05]. Deshalb werden bei grey listing sämtliche Mails ein zweites Mal angefordert.

Intrusion Detection Systeme versuchen Angreifer möglichst früh zu erkennen, und zu alarmieren. Bekannt sind drei Varianten wie dies erreicht werden kann [HD05]. In einer ersten Kategorie werden ähnlich wie bei den Antivirenprogrammen bekannte Angriffsmuster detektiert und an die Zentrale gemeldet. Eine zweite Kategorie macht sich den Umstand zu Nutze, dass meist gewisse wichtige Systemdateien geändert werden. Die Kontrolle dieser Dateien hat dieselbe Wirkung die Angriffe zu detektieren. Die dritte Variante merkt sich das Verhalten von Benutzern und Systemen. Sobald sich eine Anomalie bemerkbar macht schlägt das System Alarm. IP-Systeme sind den ID-Systemen verwandte Programme. Sie leiten jedoch im Gegensatz Sofortmassnahmen ein.

Nachfolgende Massnahmen wurden in der Interviewreihe nicht berücksichtigt. Sie bestehen nur zu einem Teil aus Sicherheitsüberlegungen. Ausserdem ist ihr Kostenanteil an der IT-Sicherheit nicht exakt bestimmbar.

Der *Reverse Proxy* ist dem Webserver vorgelagert. Er entlastet den Webserver und bietet oft mittels eingebautem Content Filter zusätzliche Sicherheit (siehe dazu [SI05]).

Das *Datenbackupsystem* speichert in regelmässigen Abständen alle wichtigen Daten und Dokumente.
Mit einem *Softwareverteilsystem* können Softwareupdates von einer Konsole aus direkt auf allen Clients installiert werden. Es reduziert unter anderem die Sicherheitskosten in der Administration. Dies kann jedoch einen erhöhten Sicherheitsbedarf für den betreffenden Arbeitsplatz zur Folge haben.

Antispyware ist eine weitere Spezialisierung der Antivirensoftware. Sie konzentriert sich auf unbekannten Programmcode, der den Computer ausspioniert. In der Studie wurde diese Unterteilung zwischen Antispyware und Antivirensoftware nicht vorgenommen.

Damit die Mitarbeiter einer gewissen Kontrolle ausgesetzt sind, wird *Monitoring Software* eingesetzt. Sie hat unter anderem die Eigenschaft, das System vor Computerviren und Spam-Mails zu schützen (siehe dazu [EC05]).

3.1.4 Administratorarbeiten

Dieses Massnahmenpaket beinhaltet alle alltäglichen Arbeiten eines Administrators. Sie können in analysierende und agierende Arbeiten unterteilt werden:

Analysierende Arbeiten	Agierende Arbeiten
Überprüfung der Logfiles	Neue Sicherheitssoftware installieren
Updates überprüfen	Patchen
Internetrecherche	Rechtevergabe der Internetnutzung
Kontrollsoftware überprüfen	

Tabelle 2: Administratorarbeiten

Diese Massnahmen werden alle aus Sicherheitsgründen zum Schutz vor Hackerattacken unternommen. Die in dieser Studie befragten Unternehmen wurden deshalb auf alle diese Massnahmen angesprochen.

Das *Überprüfen der Logfiles* kann vor oder nach einem Incident gemacht werden. Durch dieses Prüfen erhoft man sich, unerwünschte Aktionen oder Eindringlinge feststellen zu können. Mit der richtigen Software kann das Prüfen bedeutend erleichtet werden.

Kontrollsoftware überprüfen müssen natürlich nur diejenigen Administratoren die diese Art von Software (wie z.B. ID/IP-Systeme) implementiert haben. Meistens gibt solche Software eine Unmenge von false positive Alarmen aus (siehe dazu [SA05]).

Internetrecherchen werden meist unregelmässig gemacht. Häufig beschränken sich die Administratoren auf das Prüfen von bestimmten Newsseiten. Bei einer potentiell neuen Gefahr vertiefen sie ihr Wissen mit zusätzlichen Recherchen.

Neue Sicherheitssoftware braucht genau dann installiert zu werden, wenn ein neuer Securityservice zum System hinzugefügt wird. Es handelt sich dabei um eine einmalige Arbeit.

Das *Überprüfen von Updates* ist zum grössten Teil voll automatisiert. Je nach Sicherheitsrichtlinie müssen die Administratoren die Updates erst kontrollieren bevor sie ins System gelangen. Nach Aussage des Sicherheitsverantwortlichen der Firma von S.36 ist ein zu langes Abwarten mit z.B. Sicherheitspatches von Microsoft schlimmer, als die Auswirkungen, welche fehlerhafte Patches haben können.

Unter *patchen* versteht man im Allgemeinen das Einspielen von Sicherheitsupdates auf die Betriebssysteme oder Applikationen. Ein Patch ist eine Korrektur eines Programmes. Solche gibt es für alle möglichen Programme. In dieser Studie sind ausschliesslich Sicherheitsupdates gemeint. Das Patchen folgt auf das Überprüfen von Updates.

Die *Rechtevergabe der Internetnutzung* dient der Kontrolle der Mitarbeiter. Mitarbeiter haben häufig unterschiedliche Arbeiten und benötigen deswegen unterschiedliche Dienstleistungen. Die Frage, die sich eine Firma deshalb zu stellen hat, ist diejenige nach der Notwendikeit einer sochlen

[2]False positive Alarme sind Fehlarme von ID-Systemen

Regelung. Oft verursacht sie einen grossen administrativen Aufwand, wobei mit harten Richtlinien und Sanktionen derselbe Effekt viel kostengünstiger erreicht werden kann.

3.1.5 Physische Massnahmen

Alle Massnahmen, die physisch in dem System vorgenommen werden, und dem Schutz vor Übergriffen aus dem Internet dienen, werden dieser Kategorie zugeordnet. Folgende Massnahmen wurden identifiziert:

Mit dem *Abtrennen von Teilsystemen* möchte man die wichtigsten Systembereiche dem Internet gar nicht erst aussetzen. Dies setzt aber voraus, dass in diesem Teilsystem die Anbindung ans Internet gar nicht notwendig ist. Updates können nicht automatisiert werden und müssen von einem centralen Computer ausgehen. Dies kann entweder bei höchst sensitiven Daten der Fall sein oder aber bei Teilen die vollkommen ohne Internet auskommen.

Redundante Kapazitäten werden in allen Bereichen des IT-Systems integriert. Dabei wird die Tatsache ausgenutzt, dass die Wahrscheinlichkeit, dass 2 Kapazitäten gleichzeitig ausfallen viel kleiner ist, als diejenige, wenn nur eine Kapazität eingesetzt wird. Redundant gehaltene Firewalls zur Absicherung vor einem Hardwareausfall und redundante Antivirenprogramme von verschiedenen Anbietern[3] sind bekannte Massnahmen zur Verminderung des Risikos. Häufig werden auch redundante Clients eingesetzt. Nur selten sind alle Clients betroffen[4]. Eine bei grossen Unternehmen übliche Massnahme ist die redundante Nutzung der Standleitung mittels einem 2. Internetanbieter.

Damit das interne Firmennetz vom Internet möglichst unangreifbar bleibt, wird eine *Demilitarisierte Zone (DMZ)* eingebaut (siehe [EK05]). Diese schaltet die Server vor das LAN, wobei zwischen Internet und Server und zwischen Server und LAN je eine Firewall[5] eingebaut ist. Der Datenverkehr Internet-LAN ist damit nur über eine Zwischenstation möglich. Leider war dieser Punkt zu Beginn der Interviewreihe noch nicht ins Modell miteinbezogen, sodass er in den Resultaten ausser Betracht fällt.

3.1.6 Dokumentation

Aus verschiedensten Gründen werden Dokumentationen angefertigt. Bei einem grossen Netzwerk müssen Dokumentationen zur Überschaubarkeit des Netzwerkes erstellt werden. Sie erleichtern zudem die Durchführung einer Sicherheitsanalyse und das Fehlerfinden nach einem Incident. Ebenso verschieden sind die Objekte, welche dokumentiert werden. Eine Aufstellung ist in der Tabelle 3 zu finden.

Obwohl die Dokumentationsmassnahme nicht vollständig dem Schutz vor Internetangriffen zuzuordnen ist, wurde auch hier eine Vereinfachung gemacht und die Kosten der Dokumentation vollumfänglich miteingerechnet.

[3] Aussage des Sicherheitsverantwortlichen der Firma siehe S.38: Der eine Anbieter updatet schneller als der andere!

[4] Diese Aussagen basieren auf den 7 Interviews. Die Verallgemeinerung, dass selten alle Clients redundant bereitgestellt werden, wurde lediglich mit dem gesunden Menschenverstand gefolgert

[5] kann auch nur eine logische Firewall sein

Aktuelle Netzwerksituation
Benutzerrechte
Datenbackups
Software
Logfiles

Tabelle 3: Dokumentationsobjekte

3.1.7 Mitarbeitermassnahmen

Bei dieser Massnahme wird entschieden wie fest die Mitarbeiter durch Sicherheitsmassnahmen in ihrer Arbeit behindert werden sollen. Es kann sein, dass Mitarbeiter regelmässig *Sicherheitsanfragen des Computers* bearbeiten müssen, oder dass gewisse Arbeitsschritte *verlangsamt* werden, weil der Computer zeitraubende Sicherheitschecks mit den zu verarbeitenden Daten vornimmt. Dies war zum Beispiel bei der Firma von S.33 der Fall. Die genauen Kosteneinbussen zu bestimmen war in diesem Fall leider nicht möglich.

Bei einer restriktiven Handhabung der Zugriffsrechte auf das Internet kommt es vermehrt zu Anfragen nach *benötigten Zugriffsrechten.* Dieser Punkt wird oft unterschätzt. Nach Aussage des Sicherheitsverantwortlichen der Firma von S.38 vergessen 40% der Mitarbeiter nach den Ferien ihr Passwort. Mit einer restriktiven Handhabung wird diesen Effekt zusätzlich gefördert.

Eine weitere Massnahme, um die erste Phase im Risikominimierungsprozess (siehe Abbildung 6) voranzubringen, ist die *Schulung* der Mitarbeiter. Sowohl für Administratoren wie auch für sonstige Mitarbeiter kann diese Massnahme sinnvoll sein.

3.2 Kostenarten

Damit die verschiedenen Massnahmenarten nicht mit den verschiedenen auftretenden Kostenarten verwechselt werden, sind in diesem Unterkapitel die verschiedenen Kostenfaktoren kurz erklärt. Es wird hier unterschieden zwischen einmalig anfallenden Kosten sowie regelmässig wiederkehrenden Kosten. Dies ist für die Bewertung der Kosten von grosser Bedeutung, denn je nach Sicherheitsbedarf erneuert man die Produkte schneller oder langsamer, bzw. muss man die Kosten schneller abschreiben oder langsamer. Folgende Kostenarten wurden unterschieden:

Erstehungskosten Alles wofür nur einmal ein Betrag bezahlt werden muss ist hier unter Erstehungskosten zusammengefasst. Jedes Produkt hat eine gewisse Lebensdauer, und muss ersetzt werden. Für die Statistiken (siehe Kapitel 4.1) wurde eine Abschreibung der Erstehungskosten von 3 Jahren angenommen.

Wartungskosten Damit die oben beschriebenen Massnahmen ausgeführt werden können braucht es Angestellte, die einen Lohn erhalten. Die Lohnkosten wurden wie im Kapitel 2.2 beschrieben als Zeitaufwand erfasst und dann mit den Durchschnittswerten des Bundesamtes für Statistik vereinheitlicht.

Lizenzkosten Ein Softwareprodukt enthält oft eine jährliche Lizenzgebühr. So können Updates unverzüglich bezogen werden, vorausgesetzt die letzten Lizenzgebühren wurden bezahlt.

Schulungskosten Die Kosten von Schulungen gehen gleich doppelt zu Buche. Zum einen fallen Kurskosten an, und zum anderen muss dem teilnehmenden Mitarbeiter ein Lohn ausbezahlt werden. Vielleicht ist dies die Ursache dafür, dass vier der sieben interviewten Unternehmen angegeben haben keine Schulungen durchzuführen (siehe Kapitel 4.1).

Produktivitätseinbussen Immer dann, wenn das IT-System aus Sicherheitsgründen nicht zur Verügung steht, oder wenn es verlangsamt wird, entstehen Produktivitätseinbussen. Dieser Verlust schlägt sich in den Lohnkosten nieder. Da diese Kosten Fixkosten sind, werden sie häufig unterschätzt.

Diese Kosten unterscheiden sich auch in der zeitlichen Dimension. Es kommen einmalige, regelmässige und unregelmässig auftretende Kosten vor. Die unregelmässig auftretenden Ausgaben wurden in der Befragung als Kosten pro Jahr abgeschätzt.

Einmalig	Regelmässig	Unregelmässig
Erstehungskosten	Wartungskosten	Schulungskosten
	Lizenzkosten	Produktivitätseinbussen

Tabelle 4: Zeitliche Gliederung der Kosten

3.3 Kostenanalysematrix

Damit die Gesamtkosten buchhalterisch erfasst werden können, werden die Massnahmen den Kostenarten in einer Matrix gegenübergestellt. Nachfolgend ist die Matrix, mit welcher die Kosten der sieben Unternehmen ermittelt wurde:

Kosten: / **IT-Sicherheitsmassnahmen:**	Grundkosten	Wartungskosten	Schulungskosten	Produktivitäts-einbussen
Software / Hardware				
Firewall (Soft- und Hardware)				
Antivirenprogramm				
Antispamprogramm				
Intrusion Prevention Systeme				
Administratorarbeiten				
Überprüfen der Logfiles				
Kontrollsoftware überprüfen				
Internetrecherche				
Neue IT-Sicherheissoftware installieren				
Überprüfen von Updates				
patchen				
Rechtevergabe der Internetnutzung				
Physische Massnahmen				
Abtrennung von Teilsystemen				
Redundante Kapazitäten				
Dokumentation				
Netzwerksituation und Modifikation				
Benutzerrechte				
Datenbackups				
Software				
Aufruf von Administrationstools				
Analysen				
durch Externe				
Self-Attack				
Risikoanalyse				
Konzepterstellung				
Sicherheitskonzept				
Notfallplanung				
Mitarbeiterkonsequenzen				
Sicherheitsanfragen des Computers				
Verlangsamung				
Erlangen von benötigten Zugriffsrechten				
Schulungen				

Abbildung 7: Kostenanalysematrix

Die Lizenzkosten waren zu Beginn der Interviews noch als Wartungskosten verstanden worden, und wurden erst nach der Interviewreihe separat aufgeführt. Deswegen konnte in den Resultaten leider kein Verhältnis der Produktkosten zu den Gesamtkosten angegeben werden.

4 Resultate

Dieses Kapitel widmet sich den insgesamt 13 Interviews. Sieben verschiedene Unternehmen haben sich bereit erklärt, ihre IT-Sicherheitskosten darzulegen und sechs auf IT-Sicherheit spezialisierte Unternehmen haben sich Zeit genommen, um ihre Erfahrung in Bezug auf die Sicherheitskosten darzulegen. Das Kapitel ist deswegen in drei Teile gegliedert. Im ersten werden die Kostenmodelle der sieben Nicht-IT-Unternehmen betrachtet. Im zweiten die werden die qualitativen Äusserungen von IT-Sicherheitsdienstleistern festgehalten. Der letzte Teil widmet sich interessanten Äusserungen, die in den Interviews gemacht wurden.

4.1 Kostenanalyse der interviewten Unternehmen

4.1.1 Übersicht

Vergleiche zwischen den sieben Kostenbeispielen zeigen trotz der kleinen Stichprobe gewisse Tendenzen auf. Dafür ist es notwendig, die Gesamtkosten bestimmen zu können. Da die Erstehungskosten einmalig und die restlichen Kosten jährlich einbezogen wurden, ist eine lineare Abschreibung über 3 Jahre eingerechnet worden. Die gemeinsam mit den IT-Sicherheitsverantwortlichen der jeweiligen Unternemen erhobenen Daten finden sie ab Seite 32. Folgende fünf Verhältnise sind interessant:

$$\frac{Jährliche\ Kosten}{Erstehungskosten} \tag{1}$$

Dieses Verhältnis illustriert, ob mehr Gewicht auf die Erstehungskosten, oder auf die jährliche Kosten gelegt wird.

$$\frac{Gesamtkosten}{Anzahl\ Mitarbeiter} \tag{2}$$

Diese Kennzahl macht nur innerhalb der gleichen Branche Sinn, denn es arbeiten nicht immer alle Mitarbeiter an einem Client.

$$\frac{Gesamtkosten}{Anzahl\ Clients} \tag{3}$$

Die genaueste Angabe zum Sicherheitsbedürfnis illustriert dieses Verhältnis. Es vergleicht die Ausgaben mit der Systemgrösse.

$$\frac{Analyse-\ und\ Konzepterstellungskosten}{Gesamtkosten} \tag{4}$$

Damit wird gezeigt, welcher Teil der Gesamtkosten für die Auseinandersetzung mit dem eigenen

IT-System aufgewendet wird.

$$\frac{Schulungskosten}{Gesamtkosten} \tag{5}$$

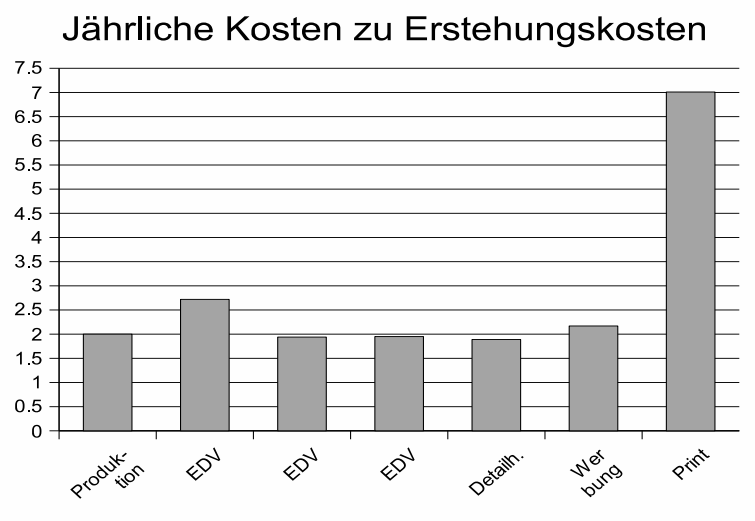
Diese Verhältnis gibt die Gewichtung der Mitarbeiterschulung an.

(Verhältnis), [Einheit]	(1), [1]	(2), [CHF]	(3), [CHF]	(4), [%]	(5), [%]
Mittelgross, Produktion	2	186	224	20	0
Mittelgross, EDV	2.72	1105	655	12	11
Klein, EDV	1.94	1129	941	0	0
Klein bis mittel, EDV	1.95	990	907	4	0
Gross, Detailhandel	1.89	34	1099	3	1
Klein, Werbung	2.17	355	254	7	0
Gross, Print	7.01	351	398	15	6
Durchschnitt	**2.81**	**593**	**640**	**8.7**	**2.6**
Standardabweichung	1.74	431	328	6.7	4.0

Abbildung 8: Kostenverhältnisse aus den Interviews mit nicht IT-Sicherheitsunternehmen

4.1.2 Kostenbeurteilung

Jährliche Kosten / Erstehungskosten An diesem Verhältnis erkennt man, wie wichtig die Erstehungskosten sind. Bei einem Verhältnis > 1 wird in einem Jahr mehr für die Sicherheitsbetreuung des Systems ausgegeben als die spezifischen Produkte gekostet haben.

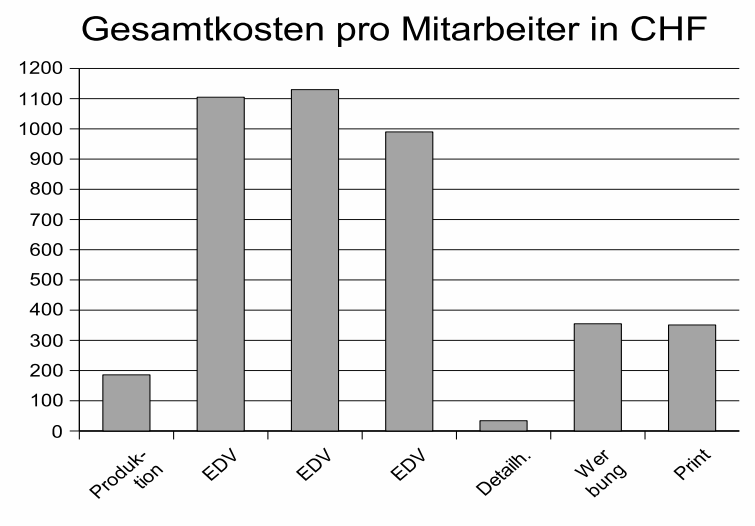


In dieser Grafik erkennt man, dass mit Ausnahme von einem Ausreisser alle Firmen etwa doppelt so hohe jährliche Kosten haben wie Erstehungskosten. Der Ausreisser könnte aufgrund von Messungenauigkeiten entstanden sein. Da die übrigen Messwerte ziemlich nahe beieinander liegen, wird vermutet, dass dieses Verhältnis von 2:1 über diverse Branchen hinweg gilt.

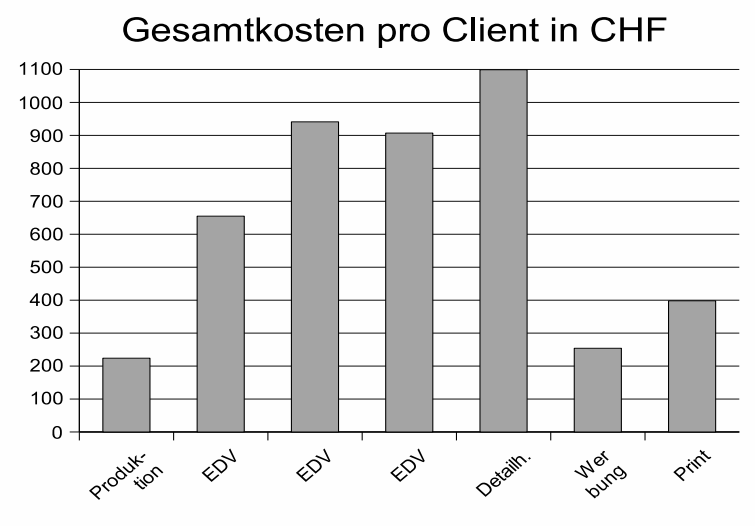
Angenommen, das Verhältnis von doppelt so hohen jährliche Kosten wie Erstehungskosten sei über alle Branchen hinweg gegeben, dann muss beim Kauf von IT-Sicherheitsprodukten dem entstehenden Aufwand vermehrt Beachtung geschenkt werden. Dieser Aufwand muss dann über alle Faktoren wie z.B. Schulungen, Konzepterstellung und Wartung der Produkte aufgerechnet werden. Der daraus folgende Hinweis ist dann: Ein teures Produkt, welches dafür weniger wartungsaufwändig ist, kann gesamthaft bedeutend kostengünstiger sein.

Gesamtkosten / Anzahl Mitarbeiter Bei diesem Verhältnis gibt es zwei Einflussfaktoren. Zum einen sind dies die Sicherheitskosten, die pro Arbeitsplatz ausgegeben werden, und zum anderen die Anzahl Mitarbeiter, die das IT-System benutzen. Deshalb geben Unternehmen, die ihren Umsatz mit Daten generieren viel mehr pro Mitarbeiter aus, als Firmen welche physisch greifbare Produkte herstellen.

Diesen Trend erkennt man auch an den sieben untersuchten Unternehmen. Die drei Firmen, bei denen die Wertschöpfung in der Datenaufbereitung besteht, haben drei mal höhere Kosten, als die anderen Unternehmen. Die Schlussfolgerung, dass diese Unternehmen einen hohen Sicherheitsstand haben, kann aus dieser Statistik nicht gezogen werden. Dazu werden im nachfolgenden Verhältnis die Kosten pro Client genauer angeschaut.

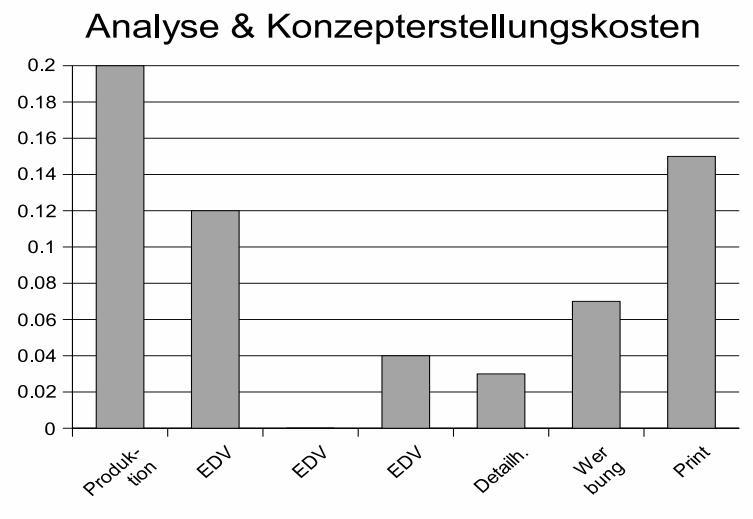


Gesamtkosten / Anzahl Clients Die Anzahl Mitarbeiter ist in der Regel nicht deckungsgleich mit der Anzahl Clients. Daher wird mit diesem Verhältnis versucht, die Dimension der betrachteten IT-Systeme in die Kostenrechnung miteinzubeziehen. Die Gesamtkosten pro Client sagen aus, wie wichtig einem Unternehmen die Sicherheit ist. Es wird mit Absicht nicht vom Sicherheitsniveau gesprochen, weil die Effizienz der Ausgaben nicht konstant ist.



Die Vermutung, dass Unternehmen mit Kernkompetenz in der Datenaufbereitung, einen grösseren Sicherheitsbedarf haben, erhärtet sich in dieser Grafik. Alle drei Unternehmen im Datenerhebungssektor geben mit 650.- CHF und mehr pro Client und Jahr etwa doppelt soviel aus wie die übrigen Unternehmen. Eine Ausnahme bildet das Grossunternehmen im Detailhandel. Dazu ist aber einzuwenden, dass diese Firma vor nicht all zu langer Zeit als Einziges der befragten Unternehmen einen erfolgreichen Angriff erlitten hatte. Möglicherweise hat dieser Incident den Sicherheitsbedarf erhöht, was die überhohen Kosten erklären würde.

Analyse- und Konzepterstellungskosten / Gesamtkosten Das grundlegende Element der IT-Sicherheit ist die Auseinandersetzung mit dem eigenen System. Gründliche Analysen bilden das Fundament eines Sicherheitskonzepts, welches dann umso besser vor bösen Überraschungen schützen kann. Aus diesem Grund betrachtet dieses Verhältnis den Anteil solcher Konzeptenwicklungskosten an den Gesamtausgaben. Von besonderem Interesse ist dabei, welche Unternehmen diesem Aspekt viel und welche wenig Bedeutung beimessen.



Die verschieden hohen Analyse- und Konzepterstellungsausgaben lassen weder Schlüsse auf Branchenzugehörigkeit noch auf Unternehmensgrössen zu. Die Gewichtung dieser Auseinandersetzung mit dem eigenen System reicht bei den befragten Unternehmen von 0% bis 20%. Diese Zahlen lassen zwei mögliche Schlüsse zu. Erstens ist es möglich, dass in den Interviews unter der Analyse und Konzepterstellung nicht bei allen Firmen dasselbe verstanden wurde, und dass die Sicherheitsverantwortlichen zuviel, bzw. zu wenig von ihren Analysen und Konzepterstellungskosten angerechnet haben.

Die andere Interpretation geht von der Korrektheit der Angaben aus und führt zum Schluss, dass die Unternehmen die Auseinandersetzung mit dem eigenen IT-System sehr unterschiedlich bewerten. Dies wirft die Frage auf, in wie fern die Firmen mit einer starken Gewichtung besser vor den Gefahren aus dem Internet geschützt sind.

Schulungskosten / Gesamtkosten Die Schulung als IT-Sicherheitsmassnahme wird generell wenig genutzt. Lediglich drei der sieben Unternehmen gaben an Schulungen durchzuführen.

4.2 Auf IT-Sicherheit spezialisierte Unternehmen

Es gibt verschiedene Gründe, weshalb ein Unternehmen exteren IT-Sicherheitsfirmen anstellen. Zum Einen erhält man dadurch Zugang zu neuem Wissen, und zum Anderen kann Betriebsblindheit verhindert werden.

Damit in dieser Arbeit ein vollständiges Bild der bestehenden Kostenstrukturen gezeigt werden kann, wurden sechs Interviews mit Mitarbeitern von fünf IT-Sicherheitsfirmen durchgeführt. Das Ziel, unverbindliche Kostenvoranschläge zu zwei der interviewten Unternehmen zu bekommen, wurde nicht erreicht. Zwei IT-Sicherheitsunternehmen haben während der mit ihnen geführten Interviews innerhalb von zwei Minuten einen möglichen Kostenvoranschlag angegeben. Die anderen Sicherheitsunternehmen haben gar keine Offerte unterbreitet. Der Grund für dieses Verhalten (wie im Interview [INTd] erklärt wurde) liegt darin, dass aufgrund der in diesen Beispielen (siehe Anhang A.2) dargelegten knappen Datenlage für IT-Sicherheit sowohl 100'000.- wie auch 500'000.- CHF pro Jahr eingerechnet werden könne. Beide Kostengrössen können aufgrund von nötigen Interpretationen gerechtfertigt sein.
Deshalb versucht dieses Kapitel zunächst den Markt der professionellen IT-Sicherheitsfirmen zu veranschaulichen. Wenn schon das Ziel eines Kostenvoranschlages nicht erreicht wurde, so sollen immerhin die kostentreibenden Faktoren an dieser Stelle genauer betrachtet werden.

4.2.1 Einteilung der IT-Sicherheitsdienstleister

Unter den sicherheitsanbietenden Unternehmen lassen sich zwei verschiedene Arten von Angeboten erkennen.

Managed-Security-Anbieter	Lösungsanbieter
Ein Service Level Agreement (SLA) bestimmt den Verantwortungsbereich, welchen die professionelle Sicherheitsfirma abzudecken hat.	Produkte werden durch die Lösungsanbieter vertrieben und installiert. Die Wartung wird lediglich bei Bedarf übernommen.
Oft wird ein 24h Fernüberwachungsservice angeboten.	Der Support wird als Zusatz, jedoch vor Ort getätigt.
Ein Remotezugriff ermöglicht es dem Managed-Security-Anbieter, Kunden in der ganzen Welt zu betreuen.	Die Kunden sind Firmen mit Hauptsitz in der erweiterten Region. Internationale Vertretungen werden höchstens durch Remotezugriff betreut.
Die Sicherheitsprodukte bleiben im Besitz des Anbieters, der sie bei einem Defekt sogleich kostenlos ersetzt.	Der Kunde kauft die Produkte und kommt im Schadenfall selbst dafür auf.

Es sind dies die Lösungsanbieter sowie die Managed-Security-Anbieter. Verallgemeinert verkauft der Lösungsanbieter einzelne Lösungen, die der Kunde auch mit Produkten von anderen Anbietern kombinieren kann. Der Managed-Security-Anbieter übernimmt hingegen den Betrieb und die Verantwortung zu einem gewissen Teil.

Zusätzlich kann die Unterscheidung gemacht werden, wie viele Mitarbeiter eines Kunden betreut werden. Es gibt Sicherheitsfirmen, die nur kleine und mittlere Unternehmen betreuen, aber auch solche, die sich auf grosse und mittelgrosse Kunden mit hohen Sicherheitsanforderungen (wie zum Beispiel eine Kleinbank) spezialisiert haben.

4.2.2 Interviewte Sicherheitsunternehmen

Die Auflistung der interviewten Sicherheitsfirmen wurde alphabetisch vorgenommen:

Lösungsanbieter:

Avantec: Ihre Kunden haben Unternehmensgrössen von > 200 Mitarbeitern, wobei die kleineren Unternehmen für ihre Grösse eher speziell hohe Sicherheitsanforderungen haben. Die Kundschaft stammt zu 90% aus der Schweiz und aus Liechtenstein.

Softlab: Mittel bis grosse Unternehmen im Finanzbereich, in der Telekomunikation, im Transport und dem Bund gehören zu ihrem Kundenkreis. Situiert sind ihre Kunden hauptsächlich in der Schweiz, Deutschland, Österreich und in Großbritannien.

System Support: Diese Firma bedient vor allem kleine Unternehmen mit zwischen 20 bis 300 Mitarbeitern. Sie kommen hauptsächlich aus der Deutschschweiz.

Managed-Security-Anbieter:

Celeris: Als Vertreter von Managed-Security, haben sie Kunden in 30 verschiedenen Ländern. Ihre Kundengrösse reicht von 200 Mitarbeitern an aufwärts. Als Ausnahme unter den Managed-Security-Anbietern verkaufen sie ihre Produkte, und bieten bei einem Schadensfall keinen kostenlosen Ersatz an.

Open Systems: Ihre Kunden sind in 70 verschiedenen Ländern und auf allen Kontinenten zu finden. Unter den Kleinkunden sind höchstens Kleinbanken vertreten. Ansonsten haben sie Kunden mit bis zu 10’000 Mitarbeitern.

4.2.3 Kostenfaktoren für spezialisierte Unternehmen

In diesem Unterkapitel wird der Frage nachgegangen, welche Faktoren die Kosten von Sicherheitsdienstleistungen beeinflussen. Folgende Faktoren haben einen Einfluss:

-*Netzdurchsatz*
Dies spiegelt sich meist in der Anzahl Mitarbeiter oder der Anzahl Clients wieder.

-*Verfügbarkeitsanforderungen*
Hier geht es um die Relevanz der Verfügbarkeit des jeweiligen Dienstes.

-*Erlaubte Ausfallzeit*
Ein Managed-Security-Anbieter definiert mit seinem Kunden eine maximale erlaubte Ausfallzeit. Je kürzer die ist, desto teurer kommt das Service Level Agreement zu stehen.

-*Komplexität bzw. Dynamik des Systems*
Unter Komplexität wird beispielsweise die Anzahl zu betreuender Standorte verstanden, da jeder einen eigenen VPN-Anschluss benötigt.

-*Zukünftige Anforderungen*
Wenn ein Ausbau der Firma absehbar ist, dimensioniert man die Syseme so, dass sie bei Bedarf beliebig ausgebaut werden können

-*Notwendigkeit des Supports vor Ort*
Je nach Fall ist das Erscheinen vor Ort nötig. Je nach Firmenstandort entstehen hier verschieden hohe Kosten.

-*Produktvorlieben (Marke)*
Siehe dazu das nachfolgende Kapitel.

Aus der Erfahrung von Herrn Bosshardt der Firma Open Systems [INTd] liegt die Kunst im richtigen Dimensionieren des Systems:

„Um ein Dispositiv richtig zu dimensionieren, sollten die Betriebs-Kosten in Relation zum Risiko-Potential, sprich der potentiellen Schadenhöhe im Falle eines Systemausfalls, gestellt werden.“ Es könne sich möglicherweise lohnen, ein Sicherheitsrisiko in Kauf zu nehmen, wenn der daraus resultierende potentielle Schaden gering wäre. „Beispielsweise ist der Ausfall oder das Defacement eines Corporate Auftritts im Normalfall mit recht geringem Schaden verbunden. Ein komplexes Schutzdispositiv ist in diesem Fall kaum gerechtfertigt. Handelt es sich jedoch um die WebSite einer grossen Zeitung, kann ein Defacement von grosser Bedeutung sein und falsch publizierte Information mit einem grossen Schaden verbunden sein. Risiken auszuschalten ist in diesem Fall entscheidend.“

4.2.4 Lösungsbewertung aus Sicht des Verkäufers

Im Interview [INTa] wurde erklärt, dass in der IT-Sicherheit die Kosten nicht als einziges Kriterium für den Entscheid zu einem Produkt bzw. einer Dienstleistung ausschlaggebend sind. Aus der Erfahrung von Herrn von Känel der Firma Avantec kommen neben den bekannten Erstehungs-, Wartungs- und Lizenzkosten zusätzlich der Investitionsschutz, die Securityfunktionalität und die Bekanntheit eines Produktes eine bedeutende Rolle zu.

Beim Investitionsschutz spricht man das Problem an, dass Investitionen, die sich nur auf den heutigen Bedarf beschränken, das Wachstum hemmen. Wenn die Lösung hingegen zu gross dimensioniert wird, erhöht man das Risiko die Investitionen nicht zu benötigen.

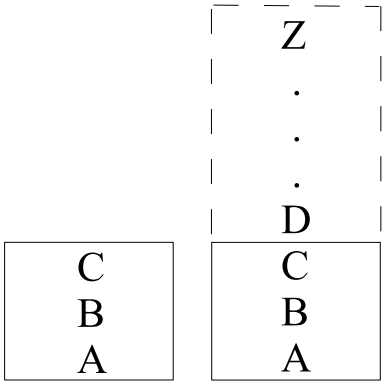


Abbildung 9: Produkterweiterungsfähigkeit

Eine Lösung mit einem guten Investitionsschutz erfüllt die heutigen Anforderungen, und lässt sich zudem beliebig weiter ausbauen (wie die Abbildung 9 rechte Spalte darstellt).

Die Securityfunktionalität drückt aus, wie weit und wie gut das Produkt Sicherheit bietet. Dieser Faktor fällt umso mehr ins Gewicht, je grösser der Sicherheitsbedarf des Käufers ist. Es ist zu beachten, dass bei einem Kauf gewisse Securitystandarts oft eine Bedingung darstellen. Falls diese nicht erfüllt sind, fällt das Produkt erst gar nicht in Betrachtung.

Der in der IT bekannte Spruch „Nobody ever got fired for buying IBM“ spricht die Thematik des Vertrauens an. Der Ruf und die Bekanntheit eines Produktes tragen entscheidend zum Erfolg bei. Je grösser der Sicherheitsbedarf des Kunden ist, desto wichtiger wird das Vertrauen.

Nachfolgende Formel könnte die Bewertung eines Produktes in etwa modellieren. Es ist dabei zu beachten, dass die Einheiten der Variablen in dieser Gleichung Gefühle sein müssten. Da dies keine physikalisch anerkannte Einheit ist, soll diese Formel lediglich die psychologischen Einflussgrössen an der Lösungsbewertung beschreiben.

$$bew = erst + betr + inv + (funk + vertr) * s$$

bew:	Lösungs**bew**ertung [positiv, negativ]
erst:	Bewertung der **Erst**ehungskosten
betr:	Bewertung der nachträglich anfallenden **Betr**iebskosten
inv:	Bewertung des **Inv**estitionsschutzes
funk:	Bewertung der **Funk**tionalität
vertr:	**Vertr**auen in das Produkt
s:	**S**icherheitsbedürfnis des Käufers [0 .. 1]

Diese Formel drückt unter anderem aus, dass bei Firmen mit einem hohen Sicherheitsbedürfnis der Vertrauensfaktor und die Funktionalität einen zunehmenden Einfluss hat. Der Faktor s reguliert dazu mit Werten zwischen 0 und 1 die Variablen funk und vertr.

Damit wie oben erwähnt Mindestanforderungen an die Funktionalität erfüllt sind, müsste die Formel mit der Sprungfunktion multipliziert werden, welche die Funktionalität als Argument hat. Dies würde bedeuten, dass eine negative Bewertung der Funktionalität die gesamte Lösungsbewertung auf 0 setzt. Dies wurde jedoch zu gunsten der Anschaulichkeit weg gelassen.

Es fällt auf, dass die betrachteten IT-Sicherheitsfirmen ihre Strategie nach dieser Formel ausrichten. Da je nach Grösse des Unternehmens das Sicherheitsbedürfnis variert, haben sich alle IT-Sicherheitsunternehmen auf entweder kleine Firmen oder grosse Firmen fokussiert (siehe Kapitel 4.2.2).

4.3 Interessante Aussagen

In den Interviews wurden diverse interessante Aussagen gemacht, die dem Leser dieser Studie nicht vorenthalten werden sollen. Auch wenn sie zum Teil im Text schon zitiert wurden, sind nachfolgend alle spannenden Aussagen aufgelistet:

Erkenntnisse nach einem erzwungene Lernzyklus (siehe Abbildung 2):

„Sofortiges patchen auf dem richtigen System (kein Testdurchlauf). Heikle Funktionen des Netzwerkes dürfen kein Windows Betriebssystem übernehmen“

„Der I-love-you Virus hatte alle MP3 Sammlungen gelöscht“

Woher die wirklichen Gefahren kommen:

„Die Gefahren durch Mitarbeiter innerhalb der Firma sind viel grösser als diejenigen, die von Hackern ausserhalb der Firma ausgehen“

„Produktivitätseinbussen wegen privatem Internetsurfen ist freitags am grössten“

„Backups werden vor allem bei intern verlorenen Daten benötigt“

„40% der Mitarbeiter haben nach den Sommerferien ihr Passwort vergessen“

Alternativen in der Systemhandhabung:

„Bei bekannt werden einer neuen Attacke lohnt es sich, den Emailserver für die Zeit abzustellen, bis ein Antivirus- bzw ein Antispamupdate erhältlich ist. Keine Emails zu erhalten verursacht, falls nur eine kleine Zeitperiode betroffen ist, minime Produktivitätseinbussen“

„Gewisse Computer sind nicht mit dem Internet verbunden. Dadurch entfallen die sonst nötigen Sicherheitsmassnahmen für diese Arbeitsplaetze. Die benötigte Zusatzzeit um diese Computer auf den neusten Stand zu bringen laesst sich einfach mit einer portablen Festplatte, oder dem kurzzeitigen Zuschalten des Internets bewerkstelligen. Diese Massnahme schützt auch vor privatem Surfen der Mitarbeiter“

„Wegen 5min Unterbruch durch das Patchen während der Arbeitszeit gibt es nur minime Produktivitätseinbussen, da in dieser Zeit andere Arbeiten erledigt werden können oder eine Pause vorgeholt werden kann“

Sonstige Aussagen:

„Die Jährlichen Wartungskosten entsprechen rund 15% des Nettopreises des jeweiligen Produktes“

„Redundantes Antivirenprogramm ist sinnvoll, da immer eines der beiden die neuen Virensignaturen schneller bereitstellen kann“

„Es kann auch wirtschaftliche Schaeden trotz einem perfekt funktionierenden System geben: IP- oder Mailadress-Spoofing verursachen enormen Imageschaden“

5 Zusammenfassung und Ausblick

Die IT-Sicherheit ist ein oft schwer messbares Gut. Dementsprechend unterliegen die Ausgaben, welche man für die Sicherheit vor Attacken aus dem Internet investiert, einer zu einem Teil unbekannten Effizienz. Die Ausgaben pro Mitarbeiter bzw. pro Client können deswegen nur eine Aussage zum Sicherheitsbedürfnis der Firma machen. Eine Folgerung daraus, wie hoch das Sicherheitsniveau der Firma ist, wäre verfehlt. Unsere Resultate zeigen, dass Unternehmen, welche in der EDV-Branche tätig sind, einen höheren Sicherheitsbedarf haben als andere. In dieser Studie zeigt sich, dass die Ausgaben pro Client bei EDV-Unternehmen etwa doppelt so hoch sind, wie bei produzierenden Unternehmen.

Die jährlichen Ausgaben sind in allen sieben interviewten Firmen mindestens doppelt so hoch wie die Erstehungskosten. Dies lässt einen Hinweis zur Kosteneffizienz zu. Beim Kauf eines Produktes soll vermehrt auf die entstehenden Betriebskosten geachtet werden. Sie fallen im Zeitraum von mehreren Jahren um ein Vielfaches mehr ins Gewicht als die einmaligen Erstehungskosten.

Aus Sicht von IT-Sicherheitsexperten wird der Kaufentscheid aus folgenden Faktoren beeinflusst. Der Preis, die entstehenden Aufwände im laufenden Betrieb, der Investitionsschutz und das Vertrauen gegenüber dem Produkt respektive der Firma. Ein Produkt hat einen guten Investitionsschutz, wenn es nach mehreren Jahren immer noch brauchbar ist, und wenn der zukünftige Bedarf trotz Wachstum durch dieses Produkt gedeckt werden kann. Der Faktor des Vertrauens hat aus Sicht von IT-Sicherheitsexperten einen umso grösseren Einfluss, je höher der Sicherheitsbedarf einer Firma ist.

Deshalb sind die Firmen, welche IT-Sicherheit anbieten, spezialisiert auf eine bestimmte Zielkundschaft, die entweder ein kleines oder ein grosses Sicherheitsbedürfnis hat. Vier der fünf interviewten Firmen haben Kunden mit mehr als 200 Mitarbeitern und lediglich ein Unternehmen sucht sich Kunden, welche weniger als 300 Mitarbeiter haben. Zudem kann eine Unterscheidung gemacht werden in der Art des Services, den das IT-Sicherheitsunternehmen anbietet. Managed Security bietet das Outsourcen von bestimmten Bereichen an, soweit wie in einem Service Level Agreement vereinbart. Lösungsanbieter hingegen verkaufen und installieren die Produkte, bieten aber oft keinen oder nur als Zusatz einen 24h Überwachungsservice an.

Ausblick

Wie in einem Interview mitgeteilt wurde, laufen auf den Systemen der interviewten Firma gewisse Arbeitsabläufe bis zu zehn mal langsamer. Dies und die Tatsache, dass die Produktivitätseinbussen in dieser Studie sehr klein eingestuft wurden, lässt vermuten, dass viele Systemadministratoren diese Kostenart vernachlässigen. Aufbauend auf folgenden Resultaten dieser Studie:

Abbildung 10: Produktivitätseinbussen

könnten Mitarbeiterbefragungen in ein bis zwei Unternehmen zu Produktivitätsverlusten gemacht werden. Durch den Vergleich dieser Produktivitätsverluste mit den zuvor vom Administrator abgeschätzten Kosten, könnte eine Aussage über den Umgang mit dieser Kostenart gemacht werden. Die Forschungsfrage würde sodann lauten:

> Werden die Produktivitätseinbussen von den IT-Sicherheitsverantwortlichen im Allgemeinen unterschätzt?

Im Vergleich mit dieser Studie, in der die beiden grossen der befragten Unternehmen praktisch keine Produktivitätseinbussen aufweisen, könnten möglicherweise Mängel von der hier angewandten Befragungsmethode aufgezeigt werden.

A Anhang

A.1 Kosten der intervieweten Unternehmen

Branche	Lüftung und Klima
Umschreibung	Herstellung von Hauseinbauteilen
Mitarbeiter	600
Sicherheitsverantwortliche	5
Rechner	500
Davon portabel	100
Mit Internet verbunden	alle

Firewall	4(DMZ,Mail,VPN,Strong Authentication)
Software-Firewalls	100 Auf allen portablen Rechnern
Antispamprogramm	Auf Mail-Firewall
Antivirenprogramm	Auf allen Systemen
VPN	Verbindung von 15 Standorten
Strong Authentication	für 70 User

Massnahmen-Pakete:	Grund-kosten (G)	Wartungs-kosten (W)	Schulungs-kosten (S)	Produktivitäts-einbussen (P)	Bemerkungen
Firewall	40’000	26’200			W= 2Tag/Monat + 15’000 für Prod.
Antispamprogramm	8’000	4’800			W= 1Std/Woche + 2’000 für Prod.
Antivirenprogramm		21’200			W= 2Tag/Monat + 10’000 für Prod.
Admin. Arbeiten: *Patchen*		5700		15’000	W= 1Tag/Monat P= 5’*500MA/Monat
Dokumentation: *des Netzwerks*		950			W= 2Tag/Jahr
Analysen: *durch Externe*		2’500			alle 2 Jahre für 5’000.-
Risikoanalyse		10’000			alle 2 Jahre
Konzepterstellung:		9’500			W= 20 Tag/Jahr
Gesamt	**48’000**	**80’850**		**15’000**	

Tabelle 5: Interview mit mittelgrossem Unternehmen im industriellen Sektor

Branche	Datenerhebung
Umschreibung	Informationsdienstleistung über das Internet
Mitarbeiter	80
Sicherheitsverantwortliche	2
Rechner	135
Davon portabel	20
Mit Internet verbunden	alle

Firewall	2 redundant
Antispamprogramm	grey listing
Antivirenprogramm	auf Mailserver und auf Clients
VPN	für Heimarbeiten

Massnahmen-Pakete:	Grund-kosten (G)	Wartungs-kosten (W)	Schulungs-kosten (S)	Produktivitäts-einbussen (P)	Bemerkungen
Firewall		12’500			W= durch Externe
Antispamprogramm		minimal			
Antivirenprogramm	9’000	22’750			W= durch Externe + 1 Std/Tag
Admin. Arbeiten: *Logfiles prüfen*		10’000			W= durch Externe
Updates		2’500			W= durch Externe
Physische Massnahmen: *redundante Clients*	20’000				4 zusätzliche Arbeitsstationen
Dokumentation: *des Netzwerks*		5600			W= 2 Std/Woche
Analysen: *durch Externe*		5000			jährlich
Konzepterstellung:		5600			W= 2 Std/Woche
Konsequenzen auf die Mitarbeiter: *Verlangsamung*				...	gewisse Arbeiten dauern bis zu 10 mal langsamer
Schulungen			10’000	4’800	S= 10’000.- Kurs P= 2 * 1 Woche
Gesamt	**29’000**	**63’950**	**10’000**	**4’800 + ...**	

Tabelle 6: Interview mit kleinem bis mittleren Unternehmen im Datenerhebungssektor

Branche	Datenerhebung
Umschreibung	Informationsdienstleistung über das Internet
Mitarbeiter	25
Sicherheitsverantwortliche	1
Rechner	35
Davon portabel	8
Mit Internet verbunden	alle

Firewall	4 an drei Standorten (eine redundant)
Antispamprogramm	auf Mailserver
Antivirenprogramm	auf Mailserver & auf Clients

Massnahmen-Pakete:	Grund-kosten (G)	Wartungs-kosten (W)	Schulungs-kosten (S)	Produktivitäts-einbussen (P)	Bemerkungen
Firewall	6'000	2'200			W= 3 Std/Monat
Antispamprogramm		1'100			W= 1.5 Std/Monat
Antivirenprogramm		1'100		5200	MA sind für Updates selbst verantwortlich W= 1.5 Std/Monat P=15'/Woche*15MA
Admin. Arbeiten:					ist automatisiert
Logfiles prüfen	2'400	5'700			G= 1 Woche W= 1 Tag/Monat
SW installieren		7'000			W= 3 Std/Woche
Patchen				1800	MA sind selbst verantwortlich P= 5'/Woche*15MA
Physische Massnahmen: *redundante Clients*	4'000				4 zusätzliche Arbeitsstationen
Gesamt	**12'400**	**17'100**		**7'000**	

Tabelle 7: Interview mit kleinem Unternehmen im Datenerhebungssektor

Branche	Verlag, Medien
Umschreibung	Informationsdienstleistung über das Internet
Mitarbeiter	55
Sicherheitsverantwortliche	1
Rechner	60
Davon portabel	10
Mit Internet verbunden	alle

Firewall	2 einfache Redundanz
Antispamprogramm	vorhanden
Antivirenprogramm	vorhanden
VPN	für Heimarbeiten

Massnahmen-Pakete:	Grund-kosten (G)	Wartungs-kosten (W)	Schulungs-kosten (S)	Produktivitäts-einbussen (P)	Bemerkungen
Firewall	6'000	5'000			W= externe Wartung + 0.5 Tag/Monat
Antispamprogramm	4'200	9'500			G= 3'000 +0.5Woche W= Supportvertrag
Antivirenprogramm	6'200	9'700			G= 5'000 +0.5Woche W= Supportvertrag
Admin. Arbeiten: *Logfiles prüfen*		7'000			W= 0.5 Std/Tag
Patchen		5'700			W= 1 Tag/Monat
Dokumentation: *des Netzwerks*	2'400				G= 1 Woche
von Modifikationen		5'700			W= 1 Tag/Monat
Analysen: *durch Externe*	5'000				einmalig
Konzepterstellung: *Sicherheitspolitik*		2'400			W= 1 Woche/Jahr
Schulungen				1'500	P= 3 Tag/Jahr
Gesamt	**23'800**	**45'000**		**1'500**	

Tabelle 8: Interview mit kleinem bis mittlerem Unternehmen im Datenerhebungssektor

Branche	Lebensmittel und Detailhandel
Umschreibung	von Produktion bis Verkauf im Detailhandel
Mitarbeiter	80’000
Sicherheitsverantwortliche	ca. 60
Rechner	3’020
Davon portabel	450
Mit Internet verbunden	alle

Firewall	12
Intrusion Prevention Systeme	5 Proben
Software-Firewalls	auf allen portablen Computern
Antispamprogramm	Opensource seriell AND-verknüpft mit einem Lizenzprodukt
Antivirenprogrmam	auf Servern und Clients
VPN	Verbindung verschiedener Standorte
Strong Authentication	für externe Arbeiten

Massnahmen-Pakete:	Grund-kosten (G)	Wartungs-kosten (W)	Schulungs-kosten (S)	Produktivitäts-einbussen (P)	Bemerkungen
IDS/IPS	60’000	9’000			W 15% der G
Firewall	950’000	142’500			W 15% der G
Antispamprogramm / Antivirenprogramm	200’000	30’000			W 15% der G
Admin. Arbeiten:		1’017’000			15% von 60 MA
Dokumentation:					
der Software		339’000			5% von 60 MA
des Netzwerks		22’600			10% von 60 MA
von Modifikationen		565’000			30% von 4 MA
Analysen:					
durch Externe		25’000			1 mal im Jahr
Self-Attack		5’700			5% von 1 MA
Risikoanalyse		22’600			10% von 2 MA
Konzepterstellung:					
Sicherheitspolitik		5’700			5% von 1 MA
Notfallplanung		28’200			10% von 25 MA
Mitarbeiter-konsequenzen:					
Sicherheitsanfragen		60’000			20’ pro Jahr und MA
Schulungen			12’000	5’700	4 MA 3 Tage/Jahr S= 1000.- pro Tag
Gesamt	**1’210’000**	**2’272’300**	**12 ’000**	**5’700**	

Tabelle 9: Interview mit Grossunternehmen im Detailhandelssektor

Branche	Reklame, Werbung
Umschreibung	Drucken von Werbung und Reklame
Mitarbeiter	5
Sicherheitsverantwortliche	1
Rechner	7
Davon portabel	1
Mit Internet verbunden	4

Software-Firewalls	Zonelab und XP-Firewall
Antivirenprogramm	Norton mit automatischem Update

Massnahmen-packete:	Grund-kosten (G)	Wartungs-kosten (W)	Schulungs-kosten (S)	Produktivitäts-einbussen (P)	Bemerkungen
Firewall	80	60			G= 50 + 0.5 Std W= 1 Std/Jahr

Antivierenprogramm	630	340			G= #Comp. * 90.-
					W= #Comp. * 40.-

Admin. Arbeiten: *Patchen*		780			15' pro Woche
Physische Massnahmen: *Abtrennung*				120	P= 120'/Jahr
Konzeptuierung:		120			60' Besprechung mit externer Arbeitskraft
Mitarbeiter-konsequenzen: *Zugriffsrechte*		120			W= 2 Std/Jahr
Gesamt	**710**	**1'420**		**120**	

Tabelle 10: Interview mit Kleinunternehmen im Werbesektor

Branche	Verlag, Printmedien
Umschreibung	Herstellung von Tages- und Wochenzeitungen
Mitarbeiter	2’300
Sicherheitsverantwortliche	1
Rechner	2031
Davon portabel	520
Mit Internet verbunden	alle

Firewall	1
Software-Firewalls	bei portablen Computern, die über VPN mit dem LAN verbunden sind
Antispamprogramm	Ausgelagert
Antivirenprogramm	2 verschiedene
VPN	für externe Arbeiten

Massnahmen-packete:	Grund-kosten (G)	Wartungs-kosten (W)	Schulungs-kosten (S)	Produktivitäts-einbussen (P)	Bemerkungen
Firewall	50’000	12’500			W= 25% von G
Antispamprogramm		85’000			(Ausgelagert)
Antivierenprogramm		120’000			W= 10’000/Monat + 160 Std/Monat
Admin. Arbeiten:		240’000			W= 20’000/Monat
Physische Massnahmen:					1% redundante
redundante Clients	60’000				Clients a 3’000.-
redundante Standleitung		144’000			12’000 pro Monat
Analysen:		100’000			2 Audit’s pro Jahr a 50’000.-
Konzepterstellung:		20’000			
Schulungen			50’000		gesamtes Personal
Gesamt	**110’000**	**721’500**	**50’000**		

Tabelle 11: Interview mit Grossunternehmen im Printverlagssektor

A.2 Unterbreitete Beispielfälle

Beispielfall Nr. 1:

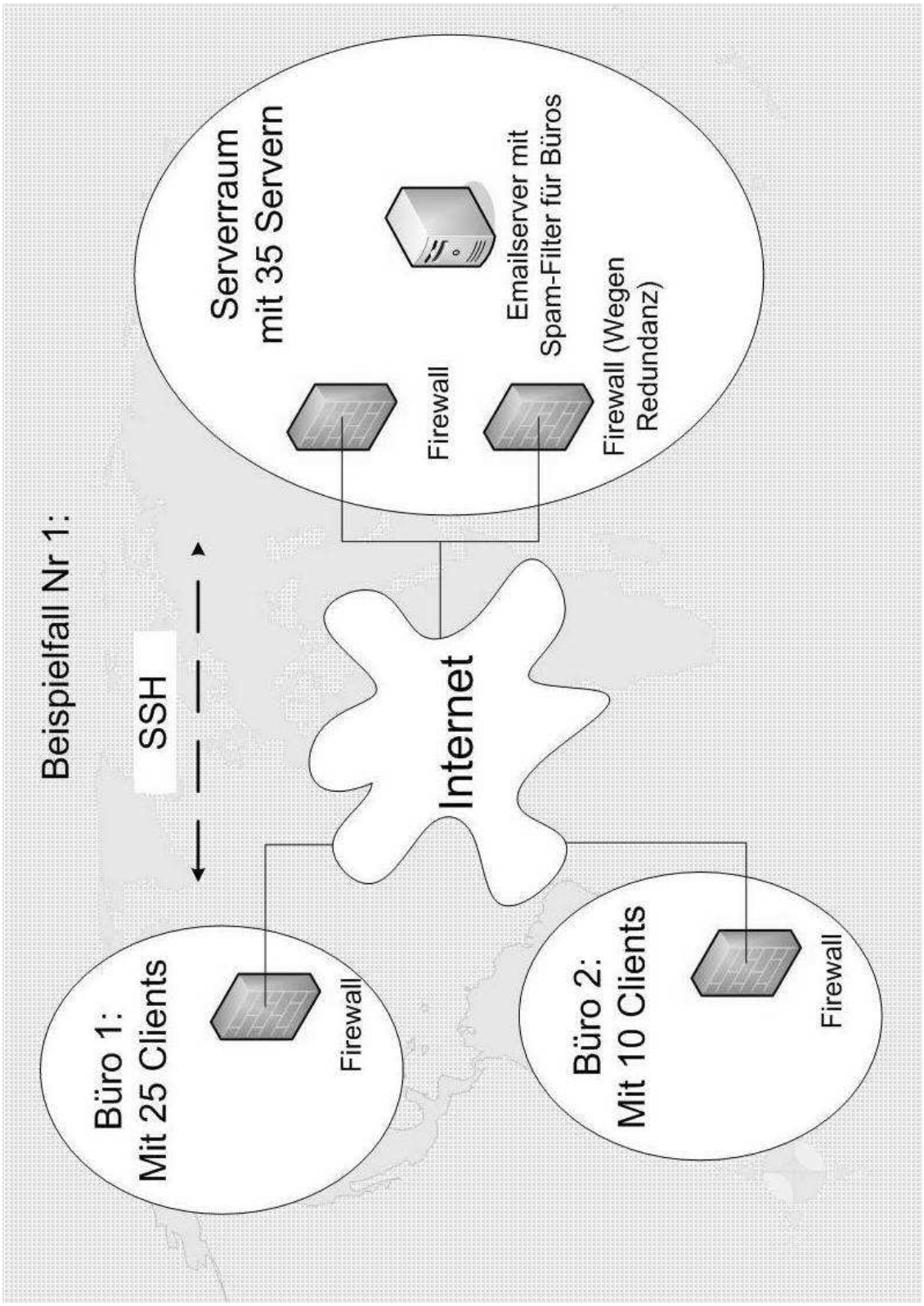
Kleinunternehmen im Internetbusiness:

Umsatz	4 Mio
Anzahl Mitarbeiter	25
Anzahl Computer	35
Firewall	2 für Server 2 in Büros
Emailserver	1
Antispamprogram	1 auf Emailserver
Antivirenprogram	auf Emailserver und auf allen Clients

Der Serverraum muss vom Internet her erreichbar sein.

Alle Standorte befinden sich in der Schweiz

Schutzbedarf:
Alle Rechner müssen dauerhaft zur Verfügung stehen und dazu vor Hackerangriffen geschützt werden. Sie sind stets mit dem Internet verbunden. Die Rechner sind Windowsclients für Officeanwendungen.

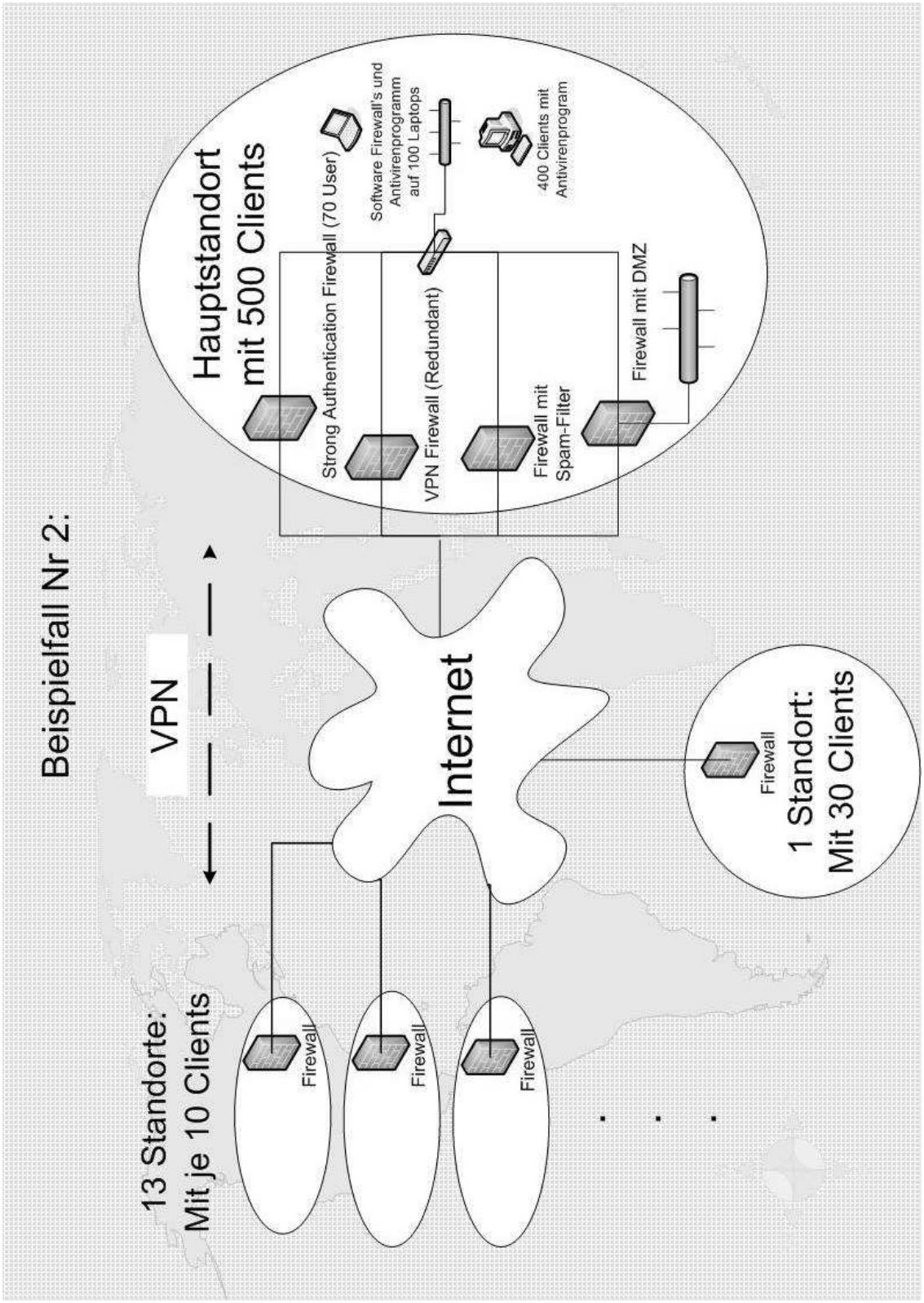

Beispielfall Nr 1:
SSH
Büro 1:
Mit 25 Clients
Firewall
Internet
Büro 2:
Mit 10 Clients
Firewall
Serverraum
mit 35 Servern
Firewall
Emailserver mit
Spam-Filter für Büros
Firewall (Wegen
Redundanz)

Beispielfall Nr. 2:

Mittelgrosses Unternehmen im Herstellungssektor:

Umsatz	250 Mio
Anzahl Mitarbeiter	600
Anzahl Computer	500
Standorte	15 weltweit
Firewalls	18
Emailserver	1
Personal Firewall	auf 100 Laptops
Antispamprogram	integriert in Firewall
Antivirenprogram	auf allen Systemen
Strong Authentication	für 70 User
VPN	Vernetzung aller 15 Standorte

Schutzbedarf:
Alle Rechner müssen dauerhaft zur Verfügung stehen und dazu vor Hackerangriffen geschützt werden. Sie sind stets mit dem Internet verbunden. Die Rechner sind Windowsclients für Officeanwendungen.


Beispielfall Nr 2:
VPN
13 Standorte:
Mit je 10 Clients
Firewall
Firewall
Firewall
Internet
Firewall
1 Standort:
Mit 30 Clients
Hauptstandort
mit 500 Clients
Strong Authentication Firewall (70 User)
Software Firewall's und
Antivirenprogramm
auf 100 Laptops
400 Clients mit
Antivirenprogram
VPN Firewall (Redundant)
Firewall mit
Spam-Filter
Firewall mit DMZ

Literatur

[SA03] TIK Studentenarbeiten. Semesterarbeit von Jürg Schmid und Peter Weigel: Wirtschaftliche Auswirkungen von DDoS Attacken auf Backbone Provider.
ftp://www.tik.ee.ethz.ch/pub/students/2003-So/SA-2003-27.pdf (April 2005)

[SA04] TIK Studentenarbeiten. Semesterarbeit von Bodo Hechelmann: Kostenmodell zu präventiven IT-Sicherheitsmassnahmen.
ftp://www.tik.ee.ethz.ch/pub/students/2004-So/SA-2004-28.pdf (April 2005)

[BA05] Bayoonet AG. Definitionen und Begriffe im Risikomanagementprozeß nach der Norm ISO 14971.
www.iso-14971.de/risikomanagementprozessdefinitionen.htm (Mai 2005)

[BU05] Bundesamt für Statistik. Siehe unter Arbeit, Löhne und Erwerbseinkommen.
www.bfs.admin.ch/bfs/portal/de/index/themen/arbeit_und_e/loehne__erwerbseinkommen/blank/kennzahlen0/lohnstruktur/nach_branche.html (Juni 2005)

[DD05] TIK DDOSVAX. A. Wagner, T. Dübendorfer Projekt zur Untersuchung von Wurmausbrüchen und Distributed Denial of Service (DDoS) Attacken.
www.tik.ee.ethz.ch/∼ddosvax/ (März 2005)

[DS05] Data Systems Austria. Eine Beschreibung von Greylisting.
www.datasystems.at/Internet/spamgreylist.asp (Juni 2005)

[EC05] ECIN. Eine Beschreibung zu Software Monitoring.
www.ecin.de/sicherheit/monitoring (Juni 2005)

[EK05] Elektronik Kompendium. Eine Beschreibung der Demilitarisierten Zone.
www.elektronik-kompendium.de/sites/net/0907241.htm (Juni 2005)

[FD05] Fachhochschule Deggendorf. Aufgaben der IT-Sicherheit.
www.biw.fh-deggendorf.de/partsch/dipl/it-sicherheit/kapitel/05.html (Juni 2005)

[FH05] Fachhochschule Heilbronn. Definition von Sicherheit (siehe Glossar).
sicherheit.i3g.fh-heilbronn.de (Mai 2005)

[GS05] Bundesamt für Sicherheit in der Informationstechnik. IT-Grundschutzhandbuch.
www.bsi.bund.de/gshb/deutsch/index.htm (April 2005)

[GS05] Zentrum für sichere Infromationstechnologie Austria (A-SIT). IT-Grundschutzhandbuch. www.a-sit.at/unterstuetzung/sicherheitshdb/sicherheitshdb.html (April 2005)

[HD05] Hessischer Datenschutzbeauftragter. Eine Beschreibung von Intrusion Detection Systemen.
www.datenschutz.hessen.de/tb28/K10p3.htm (Juni 2005)

[INTa] Interview mit Herrn von Känel der IT-Sicherheitsfirma *Avantec* vom 10.06.05 in Zürich

[INTb] Interview mit Herrn Guidon der IT-Sicherheitsfirma *Celeris* vom 27.05.05 an der Orbit-iEX in Basel

[INTc] Interview mit Herrn Lampart der IT-Sicherheitsfirma *Open Systems* vom 25.05.05 in Zürich

[INTd] Interview mit Herrn Bosshardt der IT-Sicherheitsfirma *Open Systems* vom 13.06.05 in Zürich

[INTe] Interview mit Herrn Zimmermann der IT-Firma *Softlab* vom 27.05.05 an der Orbit-iEX in Basel

[INTf] Interview mit Herrn Wermuth der IT-Firma *System Support* vom 27.05.05 an der Orbit-iEX in Basel

[MM04] Michael Mörike, *IT-Sicherheit* Seite 52, Grundwerte der IT-Sicherheit, dpunkt.verlag, Heidelberg, 2004.

[NM04] IT-SecurityArea. Rechtsfragen der IT-Security Slide NR. 39: Phasenmodell.
www.it-security-area.de/handout/ 2004/RO_DO_13_15_Niedermeier.ppt (Juli 2005)

[SA05] SAP Info. Ein Bericht zu Intrusion-Detection-Systemen.
www.sap.info/index.php4?ACTION=noframe&url=http://www.sap.info/public/de/article.php4/Article-206743f3b51321a821/de (Juni 2005)

[SI05] Auszüge aus den Lehrunterlagen zur SIZ-Prüfung in Zürich. Eine Beschreibung des Reverse Proxys.
www.redmill.ch/digicomp/glossar/glossar.htm# (Juni 2005)

[TA05] TA-NET-NRW. Beschreibung der Delphimethode durch eine Homepage mit dem Ziel der Technikfolgen Abschätzung.

www.ta-net-nrw.de/61.98.html (Juli 2005)

[UN05] Universität Mannheim. Definition von Sicherheit.
ncc.uni-mannheim.de/bsi-webkurs/gsschul/gskurs/seiten/glossar/gloss_pz.htm (Mai 2005)

[ZR99] Rainer Züst, *Systems Engineering - kurz und bündig*, Verlag Industrielle Organisation, Zürich, 1999.