ETH Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Semesterarbeit SA-2004-28
Sommersemester 2004

zum Thema

Kostenmodell zu präventiven IT-Sicherheitsmassnahmen

bei Prof. B. Plattner

Zürich, 18.07.2004

Tutor: **Thomas Dübendorfer**

Verfasst von: **Bodo Hechelmann**
(bodoh@student.ethz.ch)

TIK Institut für Technische Informatik und Kommunikationsnetze
Computer Engineering and Networks Laboratory

Inhaltsverzeichnis

Aufgabenstellung

Kostenmodell zu präventiven IT-Sicherheitsmassnahmen

Ausgangslage: “Always online - always under attack”

Immer mehr Computer sind ununterbrochen mit dem Internet verbunden und somit den Gefahren aus dem Internet wie z.B. einer Infektion mit Viren und Internet-Würmern oder einem Einbruchsversuch aus dem Internet ausgesetzt.

Intransparenz bei Präventionskosten

Durch laufende präventive IT-Sicherheitsmassnahmen versuchen sich Internet-Nutzer vor Angriffen zu schützen und mögliche Folgen eines Angriffs so klein wie möglich zu halten. Da viele dieser Kosten verdeckt anfallen und kaum separat ausgewiesen werden, ist es schwierig, eine exakte Kostenrechnung für solche Massnahmen aufzustellen.

Aufgabe

Diese Studienarbeit untersucht, mit welchen verschiedenen Kostenfaktoren die Internet-Nutzer wie Grossbetriebe, KMUs oder Heimanwender rechnen müssen für einen optimalen präventiven Schutz. Je nach Art der Internet-Nutzung variiert die Gewichtung der Kostenfaktoren erheblich. Nach der Erstellung eines Kostenmodells basierend auf den Grundsätzen des Systems Engineering und mittels Interviews und Literaturrecherche, sollen einige konkrete Fallbeispiele aufgestellt werden und die Resultate mit den Betroffenen diskutiert werden, um das Kostenmodell zu validieren.

Diese Arbeit steht im Zusammenhang mit dem ETH Forschungsprojekt DDoSVax (http://www.tik.ee.ethz.ch/~ddosvax/).

Erwartete Resultate

Die folgenden Resultate werden erwartet:

1. *Systemmodell* Zur Abgrenzung der Arbeit soll ein Systemmodell entworfen werden, um die von präventiven IT-Sicherheitsmassnahmen betroffenen Objekte zu identifizieren.
2. *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.
3. *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.
4. *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 Interviewergebnisse, das Kostenmodell, die Fallbeispiele, Schlussfolgerungen und einen Ausblick für mögliche Folgearbeiten oder Erweiterungen enthalten.

Weitere optionale Arbeiten sind die Validierung anhand weiterer konkreter Fallbeispiele, die Zusammenfassung des Modells und der Resultate als Konferenzpaper in Englisch, oder Erweiterungen zum vorgeschlagenen Kostenmodell.

Zürich, 2. April 2004

Thomas Dübendorfer
Prof. Bernhard Plattner

Zusammenfassung

Das Internet ist mit seinen mehreren hundert Millionen Benutzern und seiner weltweiten Verfügbarkeit eine grosse Quelle für mögliche Angriffe auf die Vertraulichkeit, Verfügbarkeit und Integrität der angeschlossenen Rechner. Um sich vor diesen Bedrohungen und Angriffen zu schützen, gibt es eine Vielzahl von IT-Sicherheitsmassnahmen. Eine wichtige Vorkehrung gegen Angriffe ist die umfassende Information über Gefährdungen und die Umsetzung von diesen IT-Sicherheitsmassnahmen.
Viele Kosten für IT-Sicherheitsmassnahmen fallen verdeckt an und werden kaum separat ausgewiesen werden. Darum ist es äusserst schwierig, eine exakte Kostenrechnung für diese Massnahmen aufzustellen.

Diese Semesterarbeit befasst sich mit dieser Problematik und versucht, die Kosten und den Zeitaufwand für die IT-Sicherheit mit Fokus auf Grossbetriebe und KMUs in einem Kostenmodell transparenter zu gestalten.

Mittels mehreren Interviews mit IT-Experten aus einer Anzahl verschiedener Unternehmen wurden die Kosten- und Zeitaufwandfaktoren der verschiedenen Arbeiten, die in einem Unternehmen wegen der IT-Sicherheit anfallen, evaluiert und diskutiert. Es wurde eine einfache Delphi-Methode angewendet, sprich mit den ersten Ergebnissen wurden einige Interviewpartner nochmals kontaktiert, um dann die Resultate zu analysieren und zu diskutieren.
Aus diesen Interviews wurde schnell ersichtlich, dass allgemeingültige Formeln mit einfach zu evaluierenden Parametern nicht in einem Kostenmodell zusammengetragen werden können. Die Unternehmen sind zu unterschiedlich und individuell, als dass dies möglich wäre. Daher sind in den Formeln weniger einfach zu evaluierende Parameter, wie zum Beispiel Anzahl Arbeitsrechner oder IT-User enthalten, als viel mehr eine Auflistung verschiedener Arbeitsschritte und deren Zeitaufwand, die für gewisse IT-Sicherheitsmassnahmen nötig sind.

Hier ergibt sich aber sogleich ein weiteres Problem. Da der Zeitaufwand, zum Beispiel ein Patchpaket zusammenzustellen, nun ein Parameter in der Gesamtformel ist (zum Beispiel fürs Patching), entsteht für das Unternehmen die Schwierigkeit, diesen Zeitaufwand zu erfassen. Jeder Mitarbeiter müsste seine Arbeiten zeitlich genauestens protokollieren, damit der Zeitaufwand und schliesslich die effektiven Kosten ersichtlich werden könnten. Da dies bei keiner interviewten Firma gemacht wird, konnte der Zeitaufwand für verschiedene Arbeiten nur geschätzt werden. Ein anderes Problem ergibt sich, wie die IT-sicherheitsrelevanten Arbeiten von den anderen Arbeiten abzugrenzen sind. Zum Beispiel die Kosten für die Kontrolle der IT-Infrastruktur, gehören diese nun vollumfänglich zum IT-Sicherheitsbudget, nur teilweise, oder gar nicht.

Daher wird in dieser Semesterarbeit die Gewichtung mehr auf die Evaluierung der verschiedenen Arbeiten und deren Zeitaufwand gelegt.

Es wird ersichtlich, dass neben den Kosten für die IT-sicherheitsrelevanten Produkte noch einige weitere ins IT-Sicherheitsbudget einfliessen sollten.
So werden die Kosten in vier verschiedene Teilbereicht gegliedert, die in einem Systemmodell vorgestellt werden. Es handelt sich um die Bereiche IT-Produkte, IT-Abteilung, Management / Organisation und IT-User.
Neben den Kosten für die IT-sicherheitsrelevanten Produkte fällt als erstes der Mehraufwand in den IT-Abteilungen, die sich um die IT-Sicherheitsmassnahmen kümmern

müssen, auf. Dabei sind folgende Arbeiten mit grossem Zeitaufwand verbunden: Patching, Logfiles-/Kontrollsoftwareüberprüfungen, Wartungsarbeiten und Internetrecherchen.

Aber durch die Internetanbindung des Unternehmens und durch die vermehrten Gefahren, denen das Unternehmen dadurch ausgesetzt ist, muss auch das Management handeln, indem es zum Beispiel IT-Sicherheitsgutachten in Auftrag gibt oder IT-Risikoanalysen im Unternehmen durchführen lässt. Diese Kosten werden eher selten zum Budget der IT-Sicherheitsmassnahmen gezählt.

Zum Schluss wird noch beobachtet, wie stark die Mitarbeiter, die an ihren Arbeitsstationen ihrer täglichen Arbeit nachgehen, von den IT-Sicherheitsmassnahmen beeinträchtigt werden. Wird ihre Arbeitsstation durch eine IT-Sicherheitsmassnahme blockiert, so können sie mit ihrer Arbeit nicht fortfahren, das bedeutet, dass dem Unternehmen Kosten in Form eines Produktivitätsverlustes entstehen. Gut ist das beim Patching zu beobachten. Werden zum Beispiel bei jedem Patching etwa 500 Mitarbeiter für 15 Minuten blockiert, so kann sich der Produktivitätsverlust bei 26 Patchings pro Jahr über eine halbe Million Schweizer Franken belaufen. Aber auch zum Beispiel beim Patching gehen die Unternehmen verschiedene Wege, was dann wiederum verlangt, dass sich jedes Unternehmen mit der im Bericht vorgestellten Formel individuell auseinandersetzt. Ebenso wird die Ablenkung durch Spammails als einen Produktivitätsverlust angesehen, der auch sehr gross ausfallen kann.

Am Beispiel einer fiktiven Firma werden Schätzwerte angenommen und die Formeln berechnet. Eine Übersicht der anfallenden Kosten ist im Bericht in Kapitel 5 ersichtlich, sie sind aber nur bedingt mit den Kosten anderer Firmen vergleichbar.

Könnten die Kosten für IT-Sicherheitsmassnahmen und das Gefährdungspotential einer Attacke genau berechnet werden, so wäre es möglich, einen „Return on Security Investment“ (ROSI) zu berechnen, welcher dann schön aufzeigen könnte, ob sich eine Investition in eine IT-Sicherheitsmassnahme lohnt oder eben nicht. Denn fallen die Kosten zur Umsetzung der wirkungsvollen Massnahmen kostengünstiger aus, als die Schäden, die durch Eintreten entstehen würden, ist eine Realisierungsplanung grundsätzlich empfehlenswert (Regelfall). Fallen die Kosten der Umsetzung jedoch höher aus, bedeutet dies, dass einerseits keine wirtschaftlich vertretbaren Massnahmen zur Verfügung stehen und andererseits, dass die Unterlassung der Risikominimierung auf absehbare Zeit zu einem existenzbedrohenden „Gau“ führen wird.

Mit dieser Semesterarbeit wird versucht, mehr Transparenz in die Kosten der IT-Sicherheitsmassnahmen zu bringen.

Schaffhausen, 18.07.2004

Bodo Hechelmann

1 Einleitung

1.1 Wieso diese Arbeit?

Immer mehr Unternehmen sind ständig online und daher auch ununterbrochen den Internet-Angriffen auf die Vertraulichkeit, Verfügbarkeit und Integrität ihres Systems ausgesetzt. Um sich vor diesen Bedrohungen zu schützen, gibt es eine Vielzahl von IT-Sicherheitsmassnahmen.
Über welche IT-Sicherheitsmassnahmen ein Unternehmen verfügen muss, um gegen Gefahren aus dem Internet gerüstet zu sein, gibt es haufenweise Literatur und Anweisungen (BITKOM 2003, BSI 1997, BSI 2001, Ernst & Young 2003, Harris 2002, Pohlmann/Blumberg 2004, Sadowsky 2004 u.a.). Somit wird in dieser Semesterarbeit auf dies nur in Ansätzen, um diese Arbeit abzurunden, eingegangen. Ebenso werden mögliche wirtschaftliche Schäden bei einem erfolgreichen Angriff nur leicht berührt (Dübendorfer u.a 2004, Schmid/Weigel 2003).
In dieser Semesterarbeit geht es vielmehr um die Kosten und den Zeitaufwand der IT-Abteilung, die für IT-Sicherheitsmassnahmen aufgewendet werden müssen. Es werden aber weniger die Kosten für die IT-sicherheitsrelevanten Produkte evaluiert und dargestellt, sondern das Augenmerk wird speziell auf die versteckten Kosten- und Zeitaufwandfaktoren, die im Zusammenhang mit der IT-Sicherheit stehen, gesetzt.
Die Gefahren aus dem Internet werden in letzter Zeit immer häufiger, daher werden auch immer mehr IT-Sicherheitsmassnahmen im Unternehmen eingesetzt. Doch dies oft bei gleich bleibendem IT-Budget. Das Management sieht nur den budgetierten Aufwand für IT-Sicherheitsprodukte. Die zeitintensiven Wartungen und Überprüfungen der Produkte werden unterschätzt oder ausser Acht gelassen.
Beschränken sich nun die Kosten für optimale IT-Sicherheit auf die IT-Sicherheitsprodukte und den Mehraufwand für IT-sicherheitsrelevante Arbeiten? Oder müssen noch andere Kosten wie Produktivitätsverlust mitberücksichtigt werden?
Auf diese Fragen und speziell auf den zusätzlichen Arbeitsaufwand eines Unternehmens, hervorgerufen durch IT-Sicherheitsmassnahmen, soll diese Semesterarbeit eine Antwort geben. Bei dieser Semesterarbeit wird versucht, IT-Sicherheitsmassnahmekosten mittels Nennung von Kosten- und Zeitaufwandfaktoren transparenter zu machen.

1.2 Für wen ist diese Arbeit gedacht?

Den IT-Mitarbeitern werden die Arbeitsaufwände bekannt sein, sie sollen ihnen aber durch diese Semesterarbeit nochmals ins Bewusstsein gerufen werden, damit sie auch sehen, welche Arbeiten neu durch die IT-Sicherheit auf sie zugekommen sind. Die Semesterarbeit könnte ihnen bei den nächsten Budgetverhandlungen helfen, wenn sie aufzeigen wollen, welche zusätzlichen Arbeiten für die IT-Sicherheit sie erledigen müssen und welche Ressourcen sie dafür benötigen.
Dem Management könnte sie helfen, die Gesamtkosten einer IT-Sicherheitsmassnahme zu erfassen, also nicht nur die Produktkosten. Sie könnte auch eine Unterstützung für die Berechnung des „Return on Security Investment (ROSI)“ sein, der die IT-Sicherheits-kosten mit dem Gefährdungspotential eines Internetangriffs abschätzt.
Durch Aufzeigen einiger Kosten-/Zeitaufwandfaktoren ist für Verantwortliche ersichtlich, wo Kosten oder Zeitaufwand eingespart werden könnten, so zum Beispiel mit Patching im Hintergrund.
Laien bekommen eine kurze Übersicht über die gängigen IT-Sicherheitsmassnahmen und die dafür notwendigen Arbeitsaufwände.

1.3 Kurze Aufgabenanalyse

In dieser Arbeit soll im Allgemeinen auf präventive IT-Sicherheitsmassnahmen eingegangen werden. Wenn jedoch zum Beispiel über das Überprüfen von Anomalien im Netzwerk gesprochen wird, fällt die Trennung von Präventiv- und Sofortmassnahmen nicht immer ganz leicht, so kann es sein, dass hier die Abgrenzung nicht immer genau ist. Daher wird im Folgenden nur noch von IT-Sicherheitsmassnahmen gesprochen, wenn auch ausschliesslich präventive gemeint sind.
Der Fokus wird auf die Grossbetriebe und KMUs gelegt, Heimanwender werden nicht berücksichtigt.
Erwartete Resultate sind ein Systemmodell zu entwerfen, mit dem IT-sicherheitsrelevante Objekte identifiziert und darin Kosten- und Zeitaufwandfaktoren aufgezählt werden, sowie mittels eines Fragenkatalogs an Fallbeispielen die Nützlichkeit und die Vollständigkeit des Modells zu validieren. Die Ziele, die diese Resultate erfüllen sollen, sind oben aufgeführt.

1.4 Vorgehen

Mittels Literatur- und Internetrecherchen wurde die Systemabgrenzung in Kapitel 2 erstellt. Anschliessend wurde der erste Fragenkatalog (Kapitel 8.1) gefertigt, der als Leitfaden für zwei Interviews mit folgender Firma und Organisation dienen sollte.

- **Open System AG** (Interviewpartner: Senior Consultant)
  „Open Systems ist seit 1991 der führende Anbieter für Netzwerk-Sicherheit in der Schweiz. Die Kunden von Open Systems profitieren vom Know-how erfahrener Sicherheitsingenieure, die sich von Beginn an mit den neusten Technologien und Trends der IT-Sicherheit auseinander setzten.“ (www.open.ch)

- **Informatikdienst der ETH Zürich** (Interviewpartner: Mitarbeiter der Gruppe Netzwerk Sicherheit NSG)
  „Die Informatikdienste sind der zentrale Informations- und Kommunikationstechnologieanbieter der ETH Zürich. Die Informatikdienste bieten eine breite Palette von Dienstleistungen für Studierende, Mitarbeiter und Organisationen (Departemente, Institute, Professuren) an.“ (www.id.ethz.ch)

Ziel dieser Interviews war, eine Übersicht der IT-Sicherheitsmassnahmen zu erhalten und zu erfahren, welche Arbeitsaufwände in Bezug zur IT-Sicherheit von IT-Mitarbeitern verlangt werden.
Die Ergebnisse dieser zwei Interviews sind stichwortartig in Kapitel 8.2 zusammengefasst.

Mit diesen Ergebnissen sowie weiteren Literatur- und Internetrecherchen wurde dann das erste Kostenmodell erstellt, welches Kosten- und Zeitaufwandfaktoren der IT-Sicherheitsmassnahmen aufzeigte. Um dieses Kostenmodell und ihre Faktoren zu überprüfen, wurden weitere verschiedene Interviews geführt. Dafür wurde ein zweiter Fragenkatalog (Kapitel 8.3) erarbeitet, der diese Faktoren gliedert und Fragen nach firmeninternen Angaben enthält.
Folgende vier Firmen wurden dazu interviewt.

- **Swisscom** (Interviewpartner: System Engineer)
  „Mit einem Umsatz von 14,6 Milliarden Franken im Jahr 2003 und 19'207 Mitarbeitenden ist die Swisscom-Gruppe das führende Telekom-Unternehmen in der Schweiz. Swisscom bietet das ganze Sortiment an Dienstleistungen und Produkten der

Telekommunikation an und ist in der mobilen und netzgebundenen Sprach- und Datenkommunikation sowie im Internet klarer Marktleader.“ (www.swisscom.ch)

- **Ernst Basler + Partner AG** (2 Interviewpartner: Leiter interner Informatik und Projektleiter im Geschäftsbereich Sicherheit (Bereich Informations- und Informatiksicherheit))
  „Die Ernst Basler + Partner AG ist ein international tätiges Planungs-, Beratungs- und Ingenieurunternehmen. Die Leistungen reichen vom Konzept bis zur Realisierung und von der Lösung fachspezifischer Probleme bis zur Strategie- und Unternehmensberatung.“ (www.eph.ch)

- **Grosses internationales Finanzinstitut** mit Sitz in Zürich (Interviewpartner: Chief IT-Security Architect)

- **Kleine regionale Universalbank** mit Sitz in Schaffhausen (Interviewpartner: Projektleiter E-Business)

Hier wurde ersichtlich, dass es den Unternehmen äusserst schwer fällt, einen Zeitaufwand für die verschiedenen Arbeiten zu beziffern, daher wurden teilweise in gemeinsamen Diskussionen Zeitangaben geschätzt. Ebenso wurde bei allen Firmen nachgefragt, ob sie noch andere versteckte Arbeiten für die IT-Sicherheit sehen. Diese neuen Erkenntnisse flossen dann jeweils ins nächste Interview hinein.

Da den Unternehmen Vertraulichkeit und keine Veröffentlichung ihrer Zahlen versprochen wurde, sind in dieser Semesterarbeit keine Angaben von Zeiten und Kosten der Firmen enthalten. Um aber trotzdem ein Beispiel aufzeigen zu können, wird hier eine fiktive Firma „KIT-S“ kreiert. Die Angaben und Schätzwerte dieser „KIT-S“ wurden mit Hilfe der Ergebnisse aus den Interviews gemacht. Anhand dieser Informationen wurden die Formeln schliesslich berechnet.
Anschliessend wurden diese berechneten Werte nochmals mit einer der vier Firmen durchgegangen und überprüft, ob sie auch realistisch sind. Es wurde eine einfache Delphi-Methode angewendet.

Hiermit möchte ich noch allen Interviewpartnern danken, dass sie sich die Zeit genommen haben, mir Rede und Antwort zu stehen. Vielen Dank für Ihre Unterstützung!

1.5 Bestehende Arbeiten

Es wurden keine veröffentlichten Arbeiten gefunden, die Kosten und Arbeitsaufwände für IT-Sicherheitsmassnahmen durchleuchten und versteckte Kosten und Arbeitsaufwände aufzeigen.
Viele Arbeiten beschäftigen sich mit IT-Sicherheitsmassnahmen, über welche ein Unternehmen verfügen sollte, um seine Systeme sicher zu halten (BITKOM 2003, BSI 1997, BSI 2001, Ernst & Young 2003, Harris 2002, Pohlmann/Blumberg 2004, Sadowsky 2004 u.a.). Die Arbeitsaufwände werden dabei aber gar nicht oder nur teilweise mitberücksichtigt.
Einige IT-Sicherheitsstudien (informationweek.de 2003, KMPG 2002) zeigen auf, welchen IT-Gefahren die Unternehmen ausgesetzt sind, welche IT-Sicherheitsmassnahmen in Unternehmen eingesetzt werden, wie hoch das Gesamtbudget der IT-Sicherheit ist und wie hoch sich die durch Angriffe verursachten Schäden belaufen könnten. Auch hier wird auf

die Arbeitsaufwände nicht detailliert eingegangen sowie auch keine versteckten Kosten aufgezeigt.
Ein aktuelles Thema ist ROSI (Return On Security Investment) (Gerbich 2002b). Viele Unternehmen versuchen diesen Wert zu berechnen, damit sie eine Begründung für die IT-Sicherheitsmassnahmekosten haben. Dabei muss aber das Gefährdungspotential einer IT-Attacke abgeschätzt werden können, was den Unternehmen nicht leicht fällt. Ebenso fliessen die IT-Sicherheitsmassnahmekosten in die Berechnung hinein, aber leider oft nur die Produktkosten, nicht auch die zusätzlichen Arbeitsaufwände und die allfälligen Produktivitätsverluste. Daher wird diese Semesterarbeit auch als eine Unterstützung für weitere ROSI-Arbeiten gesehen.

2 Situationsanalyse

Diese Situationsanalyse durchleuchtet die verschiedenen Elemente in der untenstehenden Systemabgrenzung. Sie zeigt, wieso eigentlich IT-Sicherheitsmassnahmen notwendig sind.

2.1 Systemabgrenzung

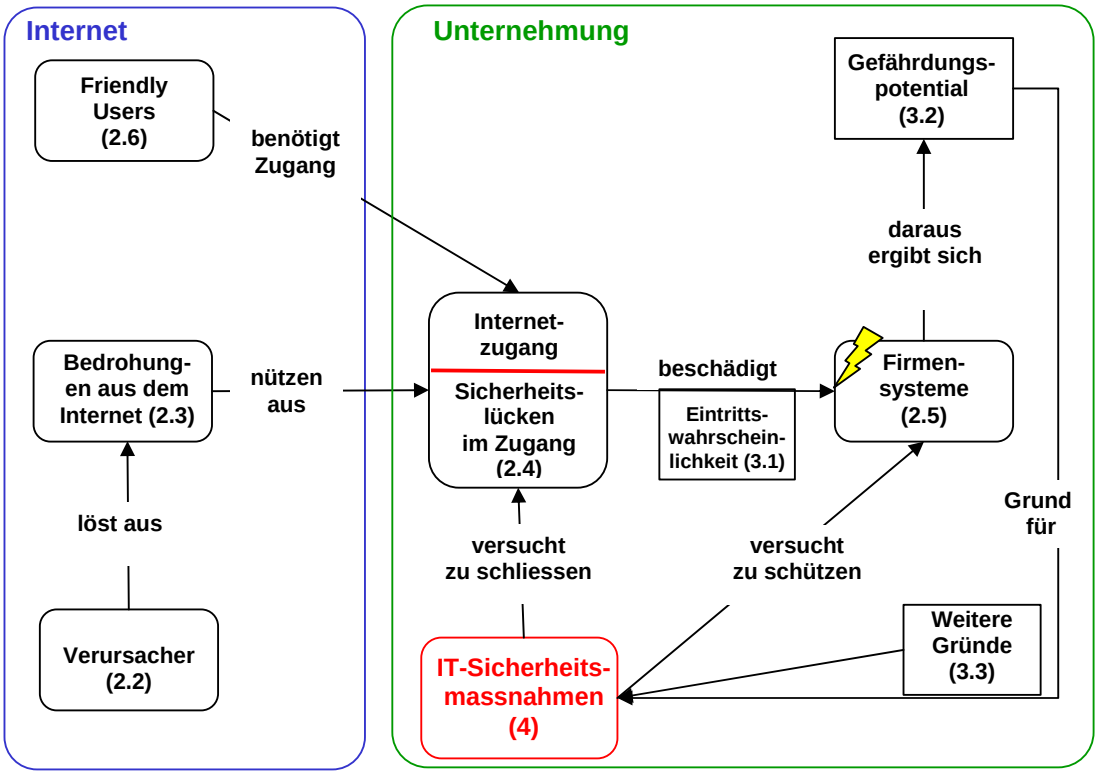

Abb. 2-1: Systemabgrenzung (in Anlehnung an Harris 2002, S. 67)

Die Elemente in der Systemabgrenzung und ihre Beziehungen werden in den nachfolgenden Unterkapiteln und Kapiteln erläutert (Kapitelnummern oben in Klammern). Die Definitionen und Erklärungen wurden in Literatur- und Internetrecherchen gefunden.

2.2 Verursacher von Internetbedrohungen

- **ScriptKids:** Scriptkids benutzen von Crackern programmierte kleine Programme und Scripts, um ihr Ziel zu erreichen. Im Grunde ist jeder der einmal ein Programm benutzt hat, um ein vergessenes Passwort wiederherzustellen, schon ein Scriptkid.

- **Cracker:** Ein Cracker ist jemand, der böswillig in einen entfernten Rechners einbricht und eventuell das System beschädigt. Nachdem Cracker unautorisierten Zugang erhalten haben, zerstören sie wichtige Daten, verweigern Dienste für legitime Benutzer oder verursachen grundsätzliche Probleme im Arbeitsablauf des angegriffenen Rechners.

- **Hacker:** Ein Hacker ist eine Person, die sich für die geheimnisvollen und verborgenen Arbeitsweisen eines jeglichen Betriebssystems interessiert. Hacker sind meistens

Programmierer. Als solche erhalten Hacker ein fortgeschrittenes Wissen über Betriebssysteme und Programmiersprachen. Sie können Sicherheitslöcher in Systemen und die Gründe dafür entdecken. Hacker sind ständig auf der Suche nach weiterem Wissen, teilen freimütig ihre Entdeckungen mit und wollen nicht absichtlich Daten zerstören.

- **Viren-, Würmer-, Trojanerprogrammierer:** (folgend nur Virenprogrammierer genannt) Ein Grossteil der Entwickler von schädlichen Programmcodes (z. B. Viren, Würmer und Trojaner) tut dies aus reiner Freude am Forschen. Nehmen wir als Beispiel Fred Cohen, dem man wohl kaum nachsagen kann, dass er seine Dissertation und die Beispielviren für bösartige Zwecke einsetzen wollte. Ihm ging es dabei einzig und allein um die Forschung im Bereich „sich selbst reproduzierende Software". Ein Indiz dafür, dass Cohens Viren nicht mit bösem Hintergedanken entwickelt wurden, ist, dass sie bis heute nicht in die Aussenwelt freigelassen wurden (Cohen 1987, S. 22ff).
  Ein anderer Teil der Virenprogrammierer frönt ihrer Tätigkeit aufgrund des Triebs nach Anerkennung, Ruhm und Popularität. In der Aggressionspsychologie spricht man von einer Erlangungs-Aggression. Bei dieser hat es der Aggressor (der Virenentwickler) auf die Durchsetzung seiner Ziele (Befriedigung seines Narzissmus) abgesehen (Nolting 1978). Genau dieser Charakter ist es, der die Verbreitung von Viren vorantreibt, denn nur so kann er seine Ziele durchsetzen. Wird ein Virus bekannt, vor allem durch eine fortwährende Medienberichterstattung, hat der Entwickler sein Ziel erreicht. Er findet darin seine Bestätigung und befriedigt so seinen Narzissmus.

- **Spammer:** Spammer verschicken unerwünschte Werbemails. Sie benutzen oft Accounts von kostenlosen eMail-Anbietern nur für eine Massensendung. Dadurch verhindern sie, dass z.B. mit Mailbombing ihr Account blockiert werden kann.
  Neu arbeiten Virenprogrammierer eng mit Spammern zusammen, die dann die Viren-, Würmer- und Trojanerattacken für ihr Spamversenden benützen. Spammer nutzen diese befallenen Rechner zum massenhaften Mail-Versand. Mit Hilfe eines Virus sollen so genannte Trojaner auf mehreren tausend Rechnern installiert werden. Durch die Trojaner können die PCs bei aktivem Internetzugang vom Besitzer unbemerkt von Spammern zum Versenden ihrer E-Mails genutzt werden. Die Versender der Massen-mails lassen sich so noch schwerer identifizieren.

- **Wettbewerber:** Wettbewerber wollen an das Know-how eines anderen Unternehmens. Sie bedienen sich der Cracker, die die Attacken durchführen. Hier geht es um Industriespionage.

- **Mitarbeiter:** Mitarbeiter fügen meistens unbewusst dem System Schaden zu, auf die soll aber nicht speziell eingegangen werden. Es gibt frustrierte Mitarbeiter, die mit Absicht versuchen, dem Unternehmen zu schaden. Sie haben meistens Zugang zu Passwörtern und können daher leicht in wichtige Bereiche eindringen. Das Know-how ist sehr unterschiedlich, oft beschränkt sich die Attacke auf Löschen von Dateien oder Abschalten von Servern. Doch dieser Verursacher einer Bedrohung bestand schon vor der Internetanbindung, daher nicht relevant.

Übersicht der Verursacher

	Know-how	Motivation	Opfer	Ziel des Angriffs
ScriptKids	Gering, verwenden fertige Tools ohne genau zu wissen, was sie tun	Langeweile, Profilierungsgehabe	Willkürlich	Zerstörung und Behinderung, um den eigenen Bekanntheitsgrad zu steigern
Cracker	Hoch, nutzen Schwachstellen in Systemen aus. Gehen logisch vor.	Kriminelle Energie	Dienstleister aller Art wie Banken, Online-Shops etc	Pers. Bereicherung, Zerstörung und Behinderung um den eigenen Bekanntheitsgrad zu steigern
Hacker	Hoch, nutzen Schwachstellen in Systemen aus. Gehen logisch vor.	Sportlicher Ehrgeiz	In der Öffentlichkeit bekannte Unternehmen und Dienstleister	Aufdecken von Schwachstellen im Internet ohne zu zerstören oder sich zu bereichern
Viren-, Würmer-, Trojanerpro-grammierer	Hoch, nutzen Schwachstellen in System aus.	Profilierungsgehabe, Befriedigung seines Narzissmus	Je mehr, je bekannter, desto besser	Zerstörung und Behinderung, um den eigenen Bekanntheitsgrad zu steigern
Spammer	Hoch	Profit	Willkürliche User	Ein Produkt anpreisen und verkaufen. Billigste Werbung.
Wettbewerber	Niedrig, jedoch in Kombination mit Crackern hoch	Kriminelle Energie	Unternehmen mit ähnlichen/gleichen Produkten oder Dienstleistungen	Industriespionage Schädigung des Wettbewerbs durch Behinderung des Geschäftsbetriebes
Mitarbeiter (nicht zwingend aus dem Internet)	Gering bis hoch	Frustration, Verärgerung, Langeweile	Arbeitgeber und Kollegen	Zerstörung, Behinderung

Abb. 2-2: Übersicht der Verursacher (in Ahnlehnung an Koch 1998)

Diese Verursacher lösen die Bedrohungen aus dem Internet aus.

2.3 Bedrohungen aus dem Internet

- **Viren:** Computer-Viren gehören zu den Programmen mit Schadensfunktionen. Als Schaden ist insbesondere der Verlust oder die Verfälschung von Daten oder Programmen anzusehen. Solche Programmfunktionen können sowohl unbeabsichtigt als auch bewusst gesteuert auftreten.

Ein Computer-Virus ist eine nicht selbstständige Programmroutine, die sich selbst reproduziert und dadurch vom Anwender nicht kontrollierbare Manipulationen in Systembereichen, an anderen Programmen oder deren Umgebung vornimmt.
Eine nicht selbstständige Programmroutine bedeutet, dass der Virus ein Wirtsprogramm benötigt. Diese Eigenschaft und seine Befähigung zur Reproduktion führten, in Analogie zum biologischen Vorbild, zu der Bezeichnung "Virus".
Die Möglichkeiten der Manipulation sind sehr vielfältig. Besonders häufig ist das Überschreiben oder das Anlagern des Virus-Codes an andere Programme und Bereiche des Betriebssystems. Dabei wird zunächst der Virus-Code und dann erst das ursprüngliche Programm ausgeführt.
Obwohl Computer-Viren prinzipiell bei jedem Computertyp und Betriebssystem denkbar sind, erlangten sie bei IBM-kompatiblen Personalcomputern (PC), insbesondere bei den weit verbreiteten Windows-Betriebssystemen, die grösste Bedeutung.

Grundtypen von Computer-Viren

- **Boot-Virus:** Der Virus befindet sich im Boot-Sektor einer Diskette bzw. Festplatte oder im Partition-Record (auch Master-Boot-Record oder Partition-Sektor genannt) einer Festplatte. Der Virus wird durch einen Kalt- oder Warm-Start (bzw. bei Daten-Disketten auch erfolglosem Bootversuch) aktiviert. Diese Form der Viren ist weitestgehend ausgestorben, da ihr Hauptverbreitungsweg - die Diskette - kaum noch eingesetzt wird.
- **Klassischer Virus:** Der klassische Virus fügt seinen Codeabschnitt der infizierten Datei an und wartet auf eine entsprechende Aktion, um aktiv zu werden. Dies kann das Starten des Wirtes sein oder auch eine völlig andere Aktion wie z.B. das Eintreten eines bestimmten Datums. Die Funktionsfähigkeit des Wirtes wird durch den Virus nicht eingeschränkt, damit der Befall nicht erkannt wird. Der klassische Virus ist nicht eigenständig sondern benötigt immer einen Wirt. Diese Virusart kann sich nur innerhalb seiner Umgebung verbreiten. Infizierung erfolgt über alle Arten der Datenübertragung.
- **Makro-Virus:** Während sich die bereits genannten Viren anstelle von Programmcode einnisten, benutzen Makro-Viren Steuersequenzen in Daten-Dateien. Moderne Programme erlauben es, häufig benötigte Steuerinformationen mittels einfach erlernbarer Programmiersprachen zu erstellen. Innerhalb der Textformatierung beispielsweise ist diese Funktion nützlich und für den Anwender sehr komfortabel. Allerdings geht der damit gewonnene Komfort zu Lasten der Sicherheit. Denn dies kann zur Programmierung von Makro-Viren missbraucht werden, die beim Arbeiten mit den Daten-Dateien automatisch ablaufen. Sofern die Hauptprogramme nicht nur für ein spezielles Betriebssystem angeboten werden, können auch die damit programmierten Viren plattformübergreifend arbeiten. Makro-Viren haben in den letzten Jahren deshalb starke Verbreitung gefunden.

- **Würmer:** Würmer sind keine klassischen Viren, sondern mit Ihnen verwandte Störprogramme, die auch Viren enthalten können. Im Gegensatz zu Viren können Würmer eigenständig agieren. Sie benötigen keinen Wirt und sind in der Lage sich über das eigene System hinaus zu verbreiten (z.B. „I Love You“).
  Ein Wurm ist ein Programm, das über das Internet Rechner befällt, um sich von diesen aus weiterzuverbreiten. Das Wurmprogramm verbraucht durch die Weiterverbreitung einen grossen Teil der im Netz zur Verfügung stehenden Bandbreite und verursacht somit einen wirtschaftlichen Schaden.

Es kann, ähnlich wie Viren, auch Programmcode enthalten, der auf den infizierten Rechnern Daten löscht oder anderen Schaden anrichtet. (Siehe z.B. den Wurm W32/Mylife.M).
Besonders gefährlich sind auch Würmer, wie z.B. Novarg/Mydoom, die eine sog. Backdoor einrichten und damit den Rechner für Angriffe öffnen. Üblich ist, die Backdoor so einzurichten, dass der befallene Rechner für die Verbreitung von Spam eingesetzt werden kann. So hat z.B. der Wurm Sober.G eine Funktion mit der er ein Programm nachladen kann, das die befallenen Rechner dann zum Versand von Spam mit rechtsextremen Inhalten missbraucht (Sober.H).
Allgemein bekannt wurden eMail-Würmer. Bei diesen enthält eine eMail, z.B. im Anhang, einen Code, der das Adressbuch des Empfängers benutzt, um sich an alle dort enthaltenen Adressen zu senden.

- **Trojaner:** Trojaner sind Programme, die neben scheinbar nützlichen auch nicht dokumentierte, schädliche Funktionen enthalten und diese unabhängig vom Computer-Anwender und ohne dessen Wissen ausführen. Deren Aufgabe ist es, insgeheim Daten (z.B. Passwörter) des jeweilig befallenen Systems zu sammeln und weiterzugeben bzw. zugänglich zu machen oder gar gleich eine Hintertür zu Ihrem System zu implementieren. Bekannte Beispiele sind „BackOrifice“ und „NetBus“. Im Gegensatz zu Computer-Viren können sich Trojanische Pferde jedoch nicht selbständig verbreiten.

- **Spammail:** Spammails sind unaufgefordert zugesandte Massen-Email, die im Internet verbreitet werden. Die Adressaten für die millionenfache Versendung stammen aus Datenbanken von Adresshändlern oder werden durch Programme im Internet ermittelt (in WWW-Seiten, Gästebüchern oder Newsgroups). Durch diesen Massen-versand wird viel Durchsatzmenge beansprucht und den User kostet es Produktivität (Schaumann 2004).

- **DoS/DDoS** (Denial of Service / Distributed Denial of Service): DoS-Angriff ist ein Sammelbegriff für verschiedene Angriffstechniken, die nur zu einem Ergebnis führen sollen: Verweigerung des Dienstes. Diese Angriffstechniken „bombardieren“ ihre Zielsysteme solange, bis diese nicht mehr reagieren. DoS-Attacken nutzen Fehler in Betriebssystemen, Programmen oder Protokollen. Durchgeführt wird der Angriff zum Beispiel mittels vieler Anfragen (nach HTML-Seiten) die sofort abbrechen wenn der Rechner antwortet, um dann erneut eine Anfrage zu starten. Da der Abbruch beim angefragten Rechner verzögert verläuft, kommt es zu einer grossen Zahl von zu bearbeitenden Anfragen.
  Bei einem DDoS-Angriff sucht der Angreifer so viele Systeme nach Schwachstellen ab wie möglich. Sein Ziel ist das Sammeln von Clients, die ferngesteuert über platzierte Trojaner einen kollektiven Angriff auf ein ausgesuchtes Zielsystem durchführen. Das bedeutet, dass man nicht nur das Ziel eines Angriffs sein kann, sondern auch Beteiligter.

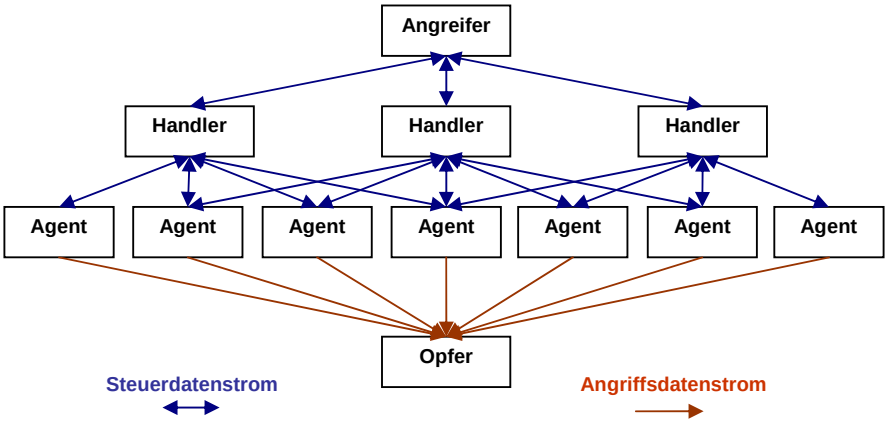

Abb. 2-3: DDoS Netzwerk

- **Cracker-/Wettbewerber-Angriff:** Eindringen in fremde Netzwerke zum Zweck der Schadensverursachung oder des Diebstahls.

- **Hacker-Angriff:** Eindringen in fremde Netzwerke, zwar ohne einen materiellen Schaden zu verursachen, aber es entsteht ein erheblicher Imageschaden für ein Unternehmen, falls ein erfolgreicher Hackerangriff bekannt wird.

Es gibt noch weitere Bedrohungen aus dem Internet, wie Sniffer, Defacement, Portscanning (was von Crackern und Hackern oft angewendet wird). Diese sollen aber hier nicht genauer erläutert werden. (KPMG 2002)

Erst durch die Sicherheitslücken im Zugang werden diese Bedrohungen eine Gefahr für ein Unternehmen, dass jemand/etwas ins System eindringt.

2.4 Sicherheitslücken im Zugang

- **Veraltete Virendefinition:** Neue Viren werden nicht erkennt.

- **Schlechter Spamfilter:** Spammail kommen ohne Hinderung in die User-Emailbox.

- **Schlecht gewartete Firewall:** Zu viele Ports sind offen, schlecht gewartet.

- **Fehlendes Patching:** Technische Systemintegrität ist nicht gewährleistet. Ungepatchte Systeme im Firmennetz.

- **Programmierfehler:** Durch die mangelhafte Überprüfung von Software in Hinblick auf Fehler, die für einen Missbrauch eines Rechnersystems ausgenutzt werden können (z. B. die fehlende Überprüfung eines Parameters bei der Übergabe an eine Unterroutine), entstehen die meisten schwer wiegenden Sicherheitslücken.

- **Konzeptionsfehler:** Durch den Anschluss eines Rechners an das Internet entstehen neue Gefährdungen durch Programme, die für die verschiedenen Dienste notwendig sind. Diese können fehlerhaft konfiguriert sein oder Programmierfehler enthalten. Häufig werden auch Programme gestartet, die nicht notwendig sind und nur zu zusätzlichen Sicherheitslücken führen. Hierzu gehören zum Beispiel Server-

Programme auf einem Rechner, der nur zum Abrufen von Informationen vorgesehen ist.

- **Konfigurationsfehler:** Voreingestellte, umfangreiche und schlecht dokumentierte Konfigurationsdateien führen zu Gefährdungen.

- **Missbrauch von frei verfügbaren Informationen:** Informationen (z. B. Benutzernamen, Rechnernamen, Namen und Version des verwendeten Betriebssystems), können missbraucht oder potenziellen Angreifern ungewollt zur Verfügung gestellt werden.

- **Einfache Passwörter:** Die gebräuchlichste Art der Authentisierung gegenüber einem Rechner beruht auf Passwörtern. Sind diese leicht zu erraten oder anderweitig durch Dritte in Erfahrung (Social Engineering) zu bringen, ist ein Missbrauch möglich.

Diese Sicherheitslücken sind eine grosse Gefahr für das Firmensystem.

2.5 Firmensysteme

Unter Firmensystemen werden hier die Arbeitsstationen, Server, Router und weiteres (Gateway, Datenbanken…) verstanden, die vom Internet her angegriffen werden können.
Sie werden in zwei Arten unterteilt, die IT-User Systeme und die IT-Professional Systeme.

- **IT-User Systeme:** Dazu werden alle Arbeitsstationen gezählt, an denen IT-Users arbeiten. Worksstation, Personal Computer, Laptops und auch Handhelds. Alle Geräte sind mit dem Netz verbunden, haben also direkt oder indirekt Zugang zum Internet.

- **IT-Professional Systeme:** Hierzu gehören alle anderen Systeme (ausgenommen Arbeitsstationen), die in einem Firmennetz vorhanden sein können. Wie zum Beispiel: DNS-Server, Webserver, Mailserver, Datenbank, Fileserver, Printserver, Applikationserver, Internet Gateway, Router und mehr.

Die Beschädigung oder Blockierung verschiedener Systeme durch eine Internetattacke kann für das Unternehmen unterschiedlich gravierend sein. Wenn zum Beispiel ein Personal Computer nicht mehr funktioniert, so wird der Datenverlust nicht sehr gross sein und nur eine Arbeitskraft wird dadurch behindert. Bei einem Applikationsserverabsturz könnten mehrere Personen in ihrer Arbeit blockiert sein, auch ein Datenverlust könnte schlimme Folgen haben. Wenn zum Beispiel an Börsengeschäfte in der Bank gedacht wird, so könnte durch ein Applikationsserverabsturz eine grosse Umsatzeinbusse entstehen. Es gibt noch tausend andere Möglichkeiten, im Allgemeinen kann man sagen, dass es auf den „Wert“ des Systems und die darin gespeicherten Informationen für die Unternehmung ankommt, wie gross der Schaden ist.

Folgende Erwartungen sollten die Firmensysteme und -netze erfüllen:

- **Verfügbarkeit:** Informationen, Systeme und Netze sind verfügbar. Das System muss bei einem Zugriff in einem definierten Zeitraum antworten bzw. bestimmte Aktionen auslösen.

- **Vertraulichkeit:** Die Informationen können von Unbefugten nicht eingesehen werden. Das System ist so aufgebaut, dass nur befugte Personen Zugriff auf die Informationen haben können.

- **Integrität:** Informationen, Systeme und Netze können nicht unbemerkt verändert werden. Das System ist so beschaffen, dass eine Veränderung offensichtlich wird.

- **Authentizität**: Die Identität von Informationen, Systemen, Netzen oder Personen kann zweifelsfrei nachgewiesen werden.

- **Zurechenbarkeit**: Aktionen und Informationen können einer auslösenden Instanz (Person oder System) zugerechnet werden. Die Zurechenbarkeit folgt mitunter aus der Authentizität.

- **Rechtssicherheit und Revisionsfähigkeit**: Alle für den Rechtsverkehr (z.B. Haftung und Gerichtsfestigkeit) in Systemen und Netzen verwendeten Informationen und Vorgänge gegenüber Dritten sind (z.B. im Rahmen einer Wirtschaftsprüfung) nachweisbar.

- **Verbindlichkeit**: Willenserklärungen oder Daten in digitaler Form sind verbindlich. Verbindlichkeit ergibt sich aus dem Nachweis der Authentizität, der Zurechenbarkeit und der Integrität von Daten.

Auf diese Systeme benötigen folgende „Friendly User“ Zugang.

2.6 Friendly Users

- **Business to Consumer:** Der Ausdruck Business to Consumer bezeichnet die Handelsbeziehungen, die über das Internet zwischen Hersteller oder Händler und dem Endverbraucher abgewickelt werden. Die Kunden brauchen Zugang zu verschiedenen Diensten des Unternehmens, wie zum Beispiel zu Internet-Shopping, Internet-Banking oder für Informationssuche.

- **Business to Business:** Business to Business ist die Beschreibung der elektronischen Geschäftsbeziehungen zwischen Unternehmen oder Händlern untereinander. Zum Beispiel ein elektronischer Marktplatz. Er ermöglicht die Zusammenführung von Anbietern und Nachfragern. Er organisiert den elektronischen Handel zwischen Unternehmen. Die Produktdaten werden in elektronischen Katalogen hinterlegt. E-Marktplätze dienen der Beschaffung hochwertiger Güter, der Abwicklung von Routinebestellungen und der engen Zusammenarbeit mit Partnern in einem Netzwerk. Sie bieten Unterstützung im Vorfeld der Verhandlungen, während der Verhandlungsphase (Ausschreibungen, Auktionen...), bei der Abwicklung (Zahlungsverkehr, Logistik...) und in der Servicephase (Wartung, Retouren...) und bieten die Möglichkeit, die Unternehmen und ihre Güter zu präsentieren.

- **Business to Employer:** Der durch Internet- und Intranettechnologie vorangetriebene Veränderungsprozess ist in der Arbeitswelt zurzeit die zentrale Herausforderung, der sich Unternehmen stellen müssen. Dabei geht es nicht mehr nur um die Beziehung zwischen einem Unternehmen und seinen Kunden bzw. seinen Lieferanten (B2C, B2B). Vielmehr stehen die Optimierung der internen Geschäftsprozesse und die Verbesserung der Kommunikation zwischen dem Unternehmen und seinen Mitarbeitern (B2E) im Fokus der Betrachtung. Ein Beispiel ist ein von zu Hause arbeitender Mitarbeiter.

3 Risiko / Schaden

Hier wird auf das Risiko eines erfolgreichen Angriffs sowie auf die möglichen Schäden eingegangen.

3.1 Eintrittswahrscheinlichkeit

Die Eintrittswahrscheinlichkeit, dass ein Angriff aus dem Internet Erfolg hat, ist schwierig zu bestimmen. Es kommt auf die vorgenommenen IT-Sicherheitsmassnahmen an. Unten sind zwei Grafiken aufgezeigt, die die Eintrittswahrscheinlichkeiten von Angriffen sichtbar machen.

Die Zeitschrift InformationWeek machte 2003 eine Studie und stellte folgende Frage:
Von welchen Sicherheitsverstössen waren Sie im vergangenen Jahr am meisten betroffen?
Zu den Telekommunikations-/unautorisierte Zugriffe können hier die Cracker- und Hacker-Angriffe gezählt werden.

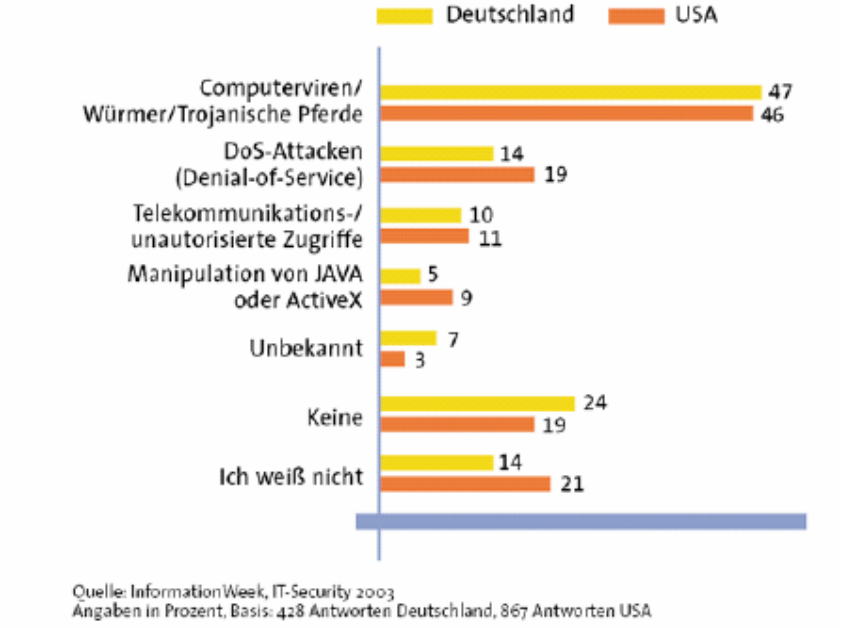

Abb. 3-1: Statistik über Sicherheitsverstösse I (informationweek.de 2003)

Die zweite Grafik zeigt eine prozentual gegliederte Zusammenstellung der Angriffs- und Missbrauchsarten im Jahre 2003.

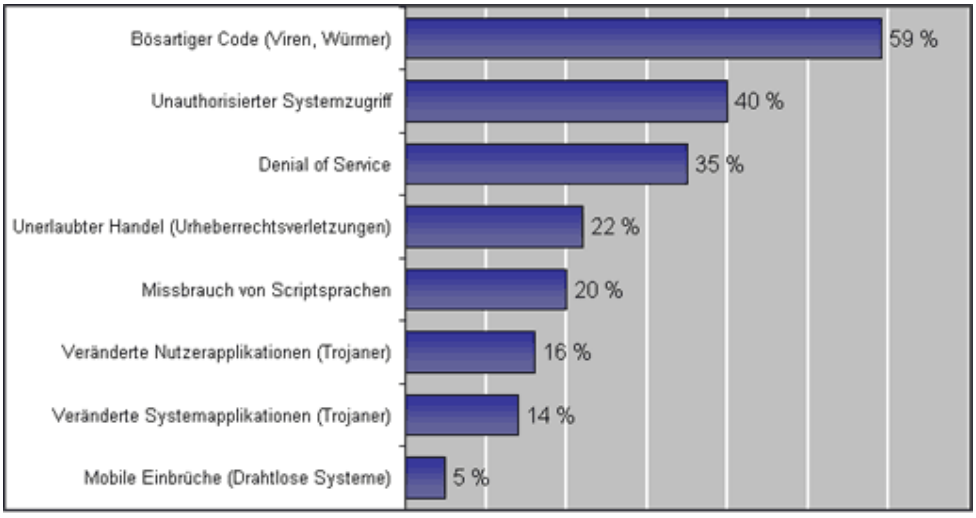

Abb. 3-2: Statistik über Sicherheitsverstösse II (educa.ch 2003)

Die Sicherheitslücken müssten nun den Angriffen mit den jeweiligen Eintrittswahrscheinlichkeiten gegenüberstellen werden. Dies ist hier aber mangels Statistiken nicht möglich. Es wird nur gezeigt, welche Lücken von welchen Angriffen ausgenutzt werden können.

Angriffe / Sicherheitslücken	Viren	Würmer	Trojaner	Spammail	DoS/DDoS	Cracker-Angriffe	Hacker-Angriffe
Veraltete Virendefinition	•	•	•				
Fehlender Spamfilter				•			
Schlecht gewartete Firewall		•	•		•	•	•
Fehlendes Patching		•	•		•	•	•
Programmierfehler	•	•	•			•	•
Konzeptionsfehler	•	•	•			•	•
Konfigurationsfehler	•	•	•			•	•
Missbrauch von f. v. Info.						•	•
Passwörter						•	•

Abb. 3-3: Gegenüberstellung von Bedrohungen mit Sicherheitslücken

3.2 Gefährdungspotential

Durch Verletzung des Systems, entsteht ein Schaden. Wie gross das Gefährdungspotential sein kann, hängt von mehreren Faktoren ob.
Beim Gefährdungspotential wird der mögliche wirtschaftliche Schaden in Relation zur Eintrittswahrscheinlichkeit gesetzt. So wird ein relativ hoher wirtschaftlicher Schaden bei einer kleinen Eintrittswahrscheinlichkeit relativiert, was dann auch beim Sicherheitsaufwand mitberücksichtigt werden muss. Die Zeitdauer einer Störung wird hier in Bezug zum wirtschaftlichen Schaden genommen, und wird daher erst dort betrachtet (Bennett 2004b).

Das Gefährdungspotential berechnet sich nun folgendermassen.

Gefährdungspotential = Eintrittswahrscheinlichkeit · Wirtschaftlicher Schaden

Gefährdungspotential [CHF]
Eintrittswahrscheinlichkeit, dass ein Angriff von aussen Erfolg hat [in Prozent]
Wirtschaftlicher Schaden, den ein Angriff hervorrufen kann [CHF]

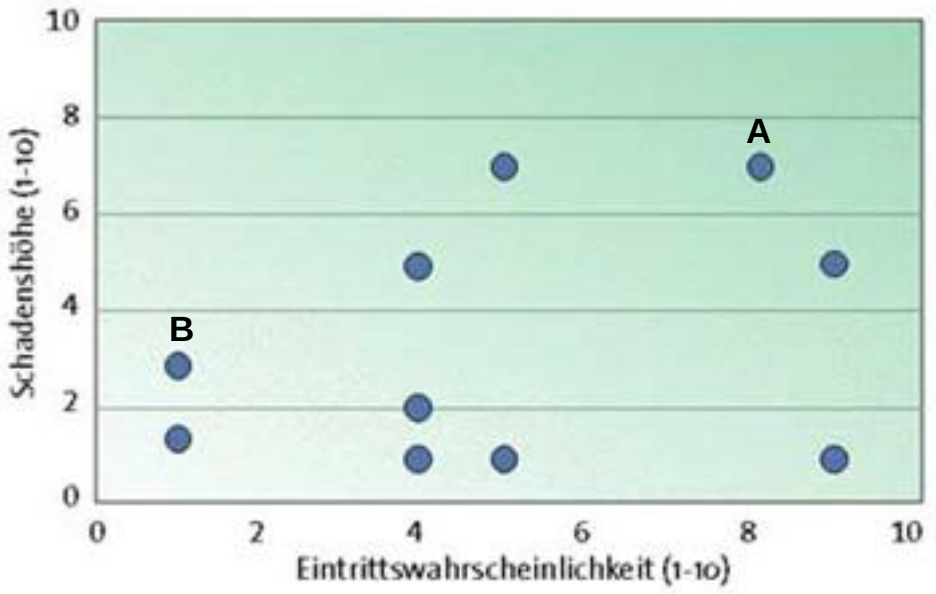

Abb. 3-4: Abschätzung des Gefährdungspotential (Gerbich 2002b)

Je höher die Eintrittswahrscheinlichkeit und zu erwartende Schadenshöhe, desto dringlicher sind Massnahmen zur Minderung des Risikos. Das heisst, das für Punkt A dringliche IT-Sicherheitsmassnahmen notwendig sind, für Punkt B erst in zweiter Priorität.

Eintrittswahrscheinlichkeit

Die Berechnung der Eintrittswahrscheinlichkeit wurde in Kapitel 3.1 schon einmal kurz angedeutet. Die Eintrittswahrscheinlichkeit gibt an, wie gross die Wahrscheinlichkeit ist, dass ein Angriff aus dem Internet Erfolg hat. Zwei Faktoren sind von Bedeutung, die Wahrscheinlichkeit und deren Häufigkeit, dass das Unternehmen angegriffen wird, und die Wahrscheinlichkeit, dass Sicherheitslücken vorhanden sind.
Der erste Faktor, die Wahrscheinlichkeit eines Angriffes sowie deren Häufigkeit, kann aus allgemeinen Statistiken über Angriffe im Netz abgeleitet werden. Es ist zu beachten, dass DoS-Attacken, Hacker und Cracker Angriffe vermutlich nicht alle Firmen gleich betreffen, jedoch machen ScriptKids, Viren, Trojaner und Würmer bei den Firmen keinen Unterschied.
Viel schwieriger ist es festzustellen, mit welchen Wahrscheinlichkeiten Sicherheitslücken in einem Unternehmenssystem vorkommen, die dann von Attacken ausgenutzt werden könnten.

Die Eintrittswahrscheinlichkeit berechnet sich folgendermassen:

Eintrittswahrscheinlichkeit = Angriffs- · Sicherheitslückenwahrscheinlichkeit

Eintrittswahrscheinlichkeit, dass ein Angriff von Aussen Erfolg hat [in Prozent]
Angriffswahrscheinlichkeit, mit welcher Wahrscheinlichkeit ein Angriff auf das Unternehmenssystem durchgeführt wird [in Prozent]
Sicherheitslückenwahrscheinlichkeit, mit welcher Wahrscheinlichkeit, sich Sicherheitslücken im System befinden [in Prozent]

Zwei triviale Beispiele, um die Sicherheitslückenwahrscheinlichkeit (SLW) zu erklären:

- Handelt es sich um ein komplett offenes System, so ist SLW = 100%. Sprich die Eintrittswahrscheinlichkeit wäre gleich der Angriffswahrscheinlichkeit.
- Bei einem komplett geschlossenen System, SLW = 0%, wäre die Eintrittswahrscheinlichkeit = 0.

Da aber SLW nur sehr schwer bis gar nicht berechenbar ist, müssen hier die allgemeinen Statistiken über Angriffe in Firmennetzwerke herangezogen werden, diese stimmen dann ungefähr mit der Eintrittswahrscheinlichkeit überein. Wobei zu sagen ist, dass der Stand der IT-Sicherheit bei den Unternehmen sehr unterschiedlich hoch ist.

Wirtschaftlicher Schaden

Der wirtschaftliche Schaden eines Unternehmens, der durch einen Angriff aus dem Internet entstanden ist, kann folgendermassen unterteilt werden.

- **Daten-/Informationsverlust:** Durch einen Angriff werden Daten gelöscht. Der Schaden kann von sehr klein bis sehr gross variieren. Dies ist erstens abhängig, wie schnell oder ob überhaupt die Daten wiederhergestellt werden können. Bei der Wiederherstellung kann es aber auch sein, dass nur eine ältere Version aus einem Datenbackup wiederhergestellt werden kann, somit geht der Arbeitsaufwand, der in eine Datei seit dem letzten Backup investiert wurde, verloren.
  Zweitens ist es vom Informationsgehalt der Daten abhängig. Wie wichtig er für das Unternehmen ist, wie viel Geld für die Information ausgegeben wurde und ob die Information überhaupt wieder erlangt werden kann.

- **Geheimhaltungsverlust:** Daten und Informationen werden vom Unternehmen entwendet, meistens durch Cracker-Angriffe, von Wettbewerbern angeheuert. Aber auch Trojaner spionieren die Systeme aus und versuchen dann, Informationen nach aussen zu senden. Wieder ist die Schadenshöhe von der Art der Information abhängig. Wie wichtig die Geheimhaltung dieser Informationen ist (Strategiekonzept, Budgetzahlen, Passwörter ..) und welchen Vorteil der Wettbewerber durch diese Informationen erhält, spielt hier eine Rolle.

- **Daten-/Informationsverfälschungen:** Die Daten werden durch einen Angriff verfälscht. Ähnliche Konsequenzen wie beim Datenverlust, nur dass noch dazu die grosse Gefahr besteht, dass die Verfälschungen erst gar nicht bemerkt werden und dann darauf aufbauende Arbeiten nicht korrekt sein könnten. Dies könnte bis zu einem Konkurs des Unternehmens führen.

Bei diesen drei Schadensarten ist es sehr schwierig, den Schaden in CHF zu messen und zu beziffern. Es kommt auf den „Wert“ und die Wichtigkeit der gespeicherten Informationen für das Unternehmen an. Wie lange brauchten sie, sich diese Informationen zu beschaffen, welche Aufwendungen mussten sie machen, diese zu erhalten, was für einen Wert hätten die Informationen für die Wettbewerber.

In Anlehnung an das Paper „An Economic Damage Model for Large-Scale Internet Attacks“ von Dübendorfer/Wagner/Plattner (2004) werden die folgenden Schadensarten beschrieben.

- **Umsatzausfall:** Umsatzausfall entsteht durch entgangene Transaktionen (Verkäufe, Vermietungen…), sei dies weil die Verbindung zum Kunden nicht mehr steht oder interne Firmenabläufe (Bestellwesen…) nicht mehr funktionieren (DoS-Attacke, Serverabstürze…). Es sind Opportunitätskosten, die bei Internet-Shopping Unternehmen sicherlich gravierender sind, als bei einem Ingenieurbüro. Da aber auch B2B immer mehr Verbreitung findet, werden davon auch immer mehr Firmen betroffen sein, wenn ihre Verbindungen nicht mehr funktionieren (Schmid/Weigel 2003).

- **Produktivitätsverlust:** Sind notwendige Dienste für Mitarbeiter gestört (z.B. Fileserverausfall), sind die Mitarbeiter unter Umständen nicht mehr in der Lage, ihre Arbeit vollumfänglich zu erledigen. Es entsteht für das Unternehmen ein Produktivitätsverlust.

Umsatz- und Produktionsverlustsformel (Ausfallzeit-Kosten)(Dübendorfer u.a. 2004):

$$L_D = \frac{E_{ca}}{d_a} \cdot d_o \cdot E_{no} \cdot E_{po} + \frac{R_a}{ds_a} \cdot ds_o \cdot R_o \cdot S_o$$

L_D**:** Ausfallzeit-Kosten [CHF]
E_{ca}: Jährliche Kosten pro Mitarbeiter [CHF/yr]
d_a: Arbeitszeit pro Mitarbeiter und Jahr [h/yr]
d_o: Arbeitsstunden mit Ausfallzeit überlappend [h]
E_{no}: Bei Ausfall betroffene Mitarbeiter [Anz]
E_{po}: Produktivitätsverminderung während des Ausfalls [in Prozent]
R_a: Totaler Jahresertrag [CHF/yr]
ds_a: Betriebsstunden pro Jahr [h]
ds_o: Bei Ausfall betroffene Betriebstunden [h]
R_o: Bei völligem Ausfall betroffener Teilertrag [in Prozent]
S_o: Grad der Betriebsverminderung [in Prozent]

- **Wiederherstellungskosten:** Zur Wiederherstellung des Betriebs eines geschädigten oder gestörten Firmennetzes oder Dienstes müssen Arbeitsstunden aufgewendet werden (Instandsetzung, Kundendienst…), die hohe Kosten verursachen können. Ebenso können weitere Materialkosten anfallen, die aber zu den Personalkosten vernachlässigbar klein sind. Oft werden auch nach einem Schadensfall weitere

sicherheitsrelevante Komponenten installiert, damit ein solcher Schadensfall nicht mehr eintritt. Diese Kosten sollen aber nicht den Wiederherstellungskosten zugerechnet werden, sondern den präventiven Sicherheitsmassnahmen. Diese Wiederherstellungskosten fallen unmittelbar nach Eintreten der Störung an.

Wiederherstellungsformel (Dübendorfer u.a. 2004):

$$L_r = E_r \cdot E_{ch} \cdot d_r + M_c$$

L_r: Wiederherstellungskosten [CHF]
E_r: Anzahl Mitarbeiter im Wiederherstellungsteam [Anz]
E_{ch}: Stundenlohn für einen Mitarbeiter im Wiederherstellungsteam [CHF]
d_r: Wiederherstellungsarbeitsstunden ausserhalb der Bürozeiten [h]
M_c: Kosten für gebrauchtes Material [CHF]

- **Haftbarkeit:** Je nach Vertragslage von Erbringern eines Dienstes zum Kunden können im Störungsfall Haftpflichtansprüche oder Konventionalstrafen des Kunden geltend gemacht werden. Diese Kosten können unter Umständen von Versicherungen abgegolten werden.

Haftbarkeitsformel (Dübendorfer u.a. 2004):

$$L_C = \sum C_c + \sum C_l$$

L_C: Haftbarkeit [CHF]
C_c: Forderungen aus Konventionalstrafen [CHF]
C_l: Forderungen aus anderen Verbindlichkeiten [CHF]

- **Image-/Kundenverlust:** Image- und Kundenverlust hängt sehr stark mit der Kundenzufriedenheit zusammen. Treten Störungen öfters auf und sind Dienste immer wieder einmal blockiert oder abgeschaltet, so nimmt die Zufriedenheit ab und der Kunde wechselt bei gleichwertigen Alternativen das Unternehmen. Diese Störungen können aber nicht nur bestehende Kunden vergraulen, sondern es entsteht für das Unternehmen auch ein Imageschaden, der sich dann bei Neukundenakquirierung bemerkbar machen kann.
  Der Schaden ist hier sehr schwer zu beziffern, bei einem Unternehmen mit Kundenkontakten, die auf eine funktionsfähige Internetverbindung mit dem Unternehmen angewiesen sind, um ihre Geschäfte zu erledigen, sicher mehr, als bei Unternehmen, die das Internet nur als Informationsbasis nützen.
  Dieser Verlust kann einen dauernden Schaden mit sich ziehen.

Kundenverlustsformel (Dübendorfer u.a. 2004):

$$L_{CL} = [C_A(\Delta t) + C_P(\Delta t)] \cdot R_C(\Delta t)$$

L_{CL}: Kundenverlust [CHF]
C_A: Anzahl gegenwärtiger Kundenverlust [Anz]
C_P: Anzahl potentieller Kundenverlust [Anz]
R_C: Durchschnittlicher Ertrag pro Kunde [CHF/yr)
Δt: Intervallzeit [yrs]

Konkrete Beispiele siehe Dübendorfer/Wagner/Plattner 2004 und Schmid/Weigel 2003.

Zusammenfassend
Es bedarf einer individuellen Risiko- und Schadenanalyse von einem Unternehmen, um eine mögliche Schadenshöhe nennen zu können. Ausserdem ist es schwierig festzustellen, wie viele Server und Arbeitsstationen zum Beispiel von einem Virus befallen werden könnten. Es müssen Abschätzungen getroffen werden, wie stark die Nutzung von Services eingeschränkt oder ob es sogar einen Totalausfall geben würde.

3.3 Gründe für Sicherheitsmassnahmen

Nicht nur die Schadensverhinderung gilt als Grund für IT-Sicherheitsmassnahmen, sondern es gibt noch weitere Gründe.

- **Schaden abwenden:** Die oben erwähnten Schäden abwenden (Daten-/Informationsverlust, Geheimhaltungsverlust, Daten-/Informationsverfälschungen, Umsatzausfall, Produktivitätsverlust, Wiederherstellungskosten, Forderung von Dritten, Image-/Kundenverlust)

- **Gewährleistung von:** Verfügbarkeit, Vertraulichkeit, Integrität, Authentizität, Zurechenbarkeit, Rechtssicherheit und Revisionsfähigkeit, Verbindlichkeit (siehe Erklärungen oben).

- **Gesetzliche Anforderungen:** (Morris Internetseite) Das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG in Deutschland) erzwingt präventive Massnahmen zur Risikoerkennung. Informationssysteme und Daten müssen in ein Schutzstufenkonzept integriert werden, damit Probleme vorhersehbar werden und Kunden wie Aktionäre keine bösen Überraschungen erleben.
  Spektakuläre Unternehmenskrisen führten dem Gesetzgeber vor Augen, dass es um die Kontrollmechanismen und die Risikovorsorge nicht genügend bestellt war. Um künftig vor allem die Anleger vor solchen Überraschungen zu schützen, wurde das KonTraG in Deutschland verabschiedet, das am 1. Mai 1998 in Kraft trat (Lang 2003).

- **Anforderungen von Partnern:** Im Business to Business Geschäft wird eine enge Zusammenarbeit der Partner verlangt. Da auch hier das Sprichwort gilt „Die Kette ist nur so stark wie ihr schwächstes Glied.“, ist es wichtig, dass die Anforderungen von Partnern betreffend IT-Sicherheit gewährleistet sind (Pohl 2003).

- **ROSI (Return of Security Investment):** ROSI ist der ROI (Return of Investment) von Informationssicherheit. Einfache Methoden, den ROSI zu messen, sind erst in der Entwicklung. Deshalb behelfen sich die Firmen noch immer mit dem klassischen Ansatz: Zweifel, Angst und Unsicherheit. Von diesen Ängsten geleitet zu werden, ist aber falsch. Am folgenden Beispiel soll aufgezeigt werden, wie vorgegangen werden sollte:
  Ein Intrusion Detection System (IDS) kostet 40'000.- CHF (Vollkosten inkl. Wartung, Personal etc), die Wirksamkeit des Systems beträgt 85 Prozent. Ohne den Einsatz eines IDS tritt etwa ein Schaden von 100'000.- CHF pro Jahr ein; somit beträgt der jährliche Gewinn 45'000.- CHF (100'000 * 85% – 40'000). Was einen ROSI von 112.50% (45'000 / 40'000) ergeben würde, falls kein Fremdkapital gebraucht würde. Da die 45'000.- CHF aber nicht ausbezahlt werden können, sondern dieser Betrag als nicht zu bezahlende Schadenaufwendung gebucht wird (oder eben gar nicht verbucht wird), ergibt es einen ROSI von 0%. Mit dieser Rechnung tun sich viele Unternehmen schwer (Gerbich 2002b).
  Obwohl der Sinn der IT-Sicherheitsmassnahmen mit ROSI am besten gezeigt werden kann, wird diese Begründung erst ganz am Schluss der Frage „Wie rechtfertigen sie Sicherheitsinvestitionen?“ erwähnt, die bei der IT-Security Studie von 2003 gestellt wurde.

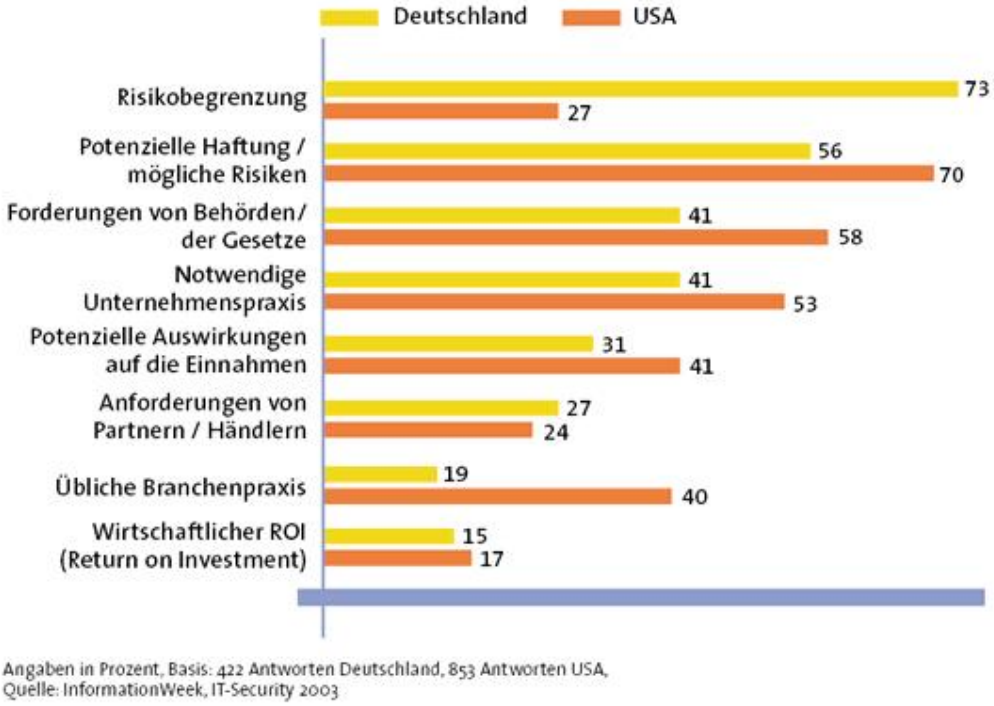

Abb. 3-5: Statistik über Begründungen von Sicherheitsinvestitionen (informationweek.de 2003)

Aus den oben erwähnten Gründen braucht es Sicherheitsmassnahmen (Gerbich 2002a). Da diese Sicherheitsmassnahmen und deren Kosten im Zentrum dieser Arbeit stehen, werden sie in einem speziellen Kapitel beleuchtet.

4 IT-Sicherheitsmassnahmen

Hier werden nur ausgewählte IT-Sicherheitsmassnahmen, die durch die Internetbenutzung notwendig wurden, aufgezeigt, da es sonst den Rahmen dieser Arbeit sprengen würde.
Die Auswahl deckt die wichtigsten IT-Sicherheitsmassnahmen ab, die es für eine sichere Internetbenutzung bedarf. Sie wurde mittels Interviews mit Fachleuten getroffen.
Aber nicht nur die Hard- und Softwarekomponenten spielen eine Rolle, sondern auch der Arbeitsaufwand, der anfällt, um die Sicherheit des Systems zu gewährleisten.

4.1 Systemmodell der IT-Sicherheitsmassnahmen

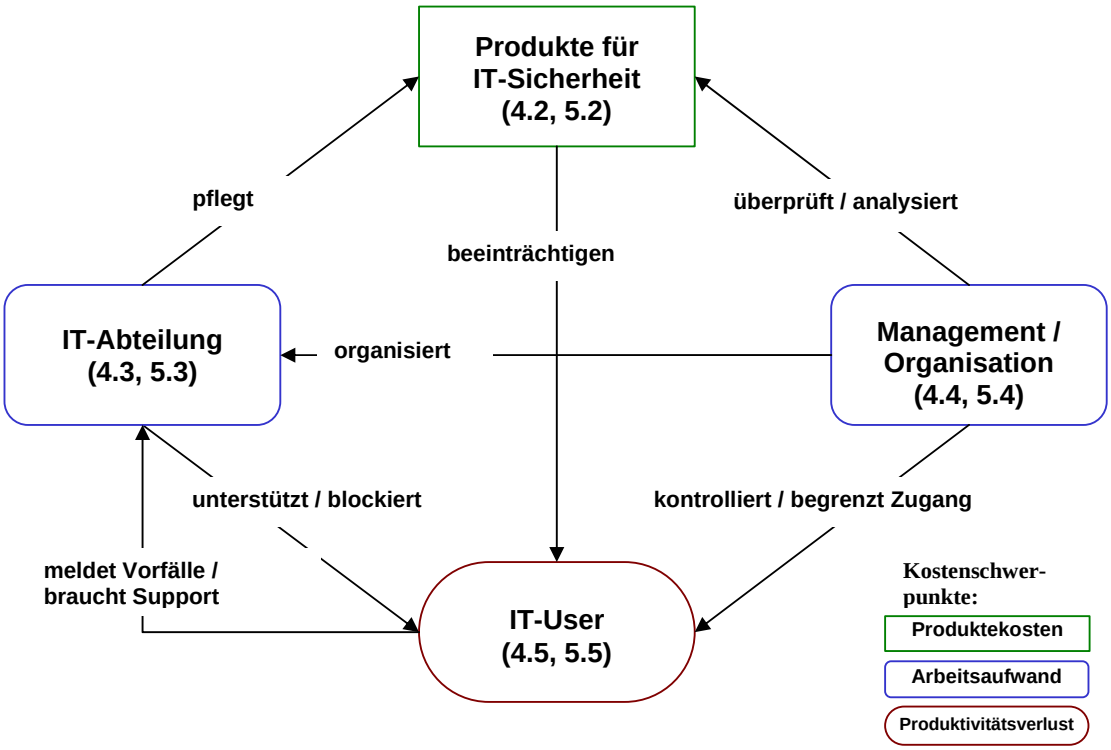

Abb. 4-1: Systemmodell der IT-Sicherheitsmassnahmen

Das Systemmodell ist in vier Bereiche eingeteilt. Der Bereich „Produkte für IT-Sicherheit“ enthält die Produkte, die für die IT-Sicherheit notwendig sind. Diese Produkte müssen von der „IT-Abteilung“ gepflegt werden. Dort sind IT-sicherheitsrelevante Arbeitsaufwände aufgezeigt, die von der IT-Abteilung erledigt werden müssen. Durch die Anbindung des Unternehmens ans Internet und die damit verbundenen Gefahren kommen auch neue Arbeiten auf das „Management und die Organisation“ hinzu, die nicht vergessen werden dürfen. Schlussendlich wird noch auf die „IT-User“ eingegangen, die durch die vermehrten IT-Sicherheitsmassnahmen in ihren Arbeiten beeinträchtigt werden können, was einen Produktivitätsverlust zur Folge haben kann.
Auf diese Teilbereiche wird in den nachfolgenden Unterkapiteln (Zahlen in Klammern) eingegangen

4.2 Produkte für IT-Sicherheit

Es werden hier einige Produktbeispiele aufgelistet, die für die IT-Sicherheit relevant sind, wenn das Firmennetz ans Internet angeschlossen wird. Es wird aber kein Anspruch auf Vollständigkeit erhoben.

- **Firewall:** Eine Firewall dient zur Kontrolle der Kommunikation zwischen zwei Netzen. Im Regelfall wird sie zum Schutz eines Netzes gegen Angriffe aus einem Netz mit einem geringeren Schutzbedarf eingesetzt, zum Beispiel bei der Anbindung eines zu schützenden Teilnetzes an ein organisationsumspannendes Netz oder der Anbindung eines Firmennetzes an das Internet. Eine Firewall ist gleichzeitig sowohl „elektronischer Pförtner", als auch „elektronische Brandschutzmauer". Die Aufgabe der „Brandschutzmauer" besteht darin, das zu sichernde Netzwerk abzuschotten. Schäden, die im unsicheren Netz auftreten, also an der „Aussenseite der Mauer", dürfen nicht in den inneren Bereich (das zu schützende Netzwerk) übergreifen. Die Aufgabe des „Pförtners" ist es, den Zugang zu dem gesicherten Netz und seinen Teilbereichen zu kontrollieren. Benutzer, die auf das zu schützende Netzwerk zugreifen wollen, müssen sich identifizieren und authentisieren. Der Pförtner muss prüfen welche Daten in das Netzwerk und welche aus dem Netzwerk gelangen dürfen. Zudem muss er alle Ereignisse protokollieren, um einen erfolgten Angriff besser nachvollziehen zu können und ggf. Rückschlüsse auf den/die Täter zu gewinnen. (Ernst & Young 2001)

- **Datenbackup-Systeme:** Als Datenbackup werden die Sicherheitskopie eines Datenbestandes bezeichnet, die bei Zerstörung oder Datenverlust die Wiederherstellung der Daten ermöglicht. Datenbackup-Systeme sind nicht erst seit der Internet-benutzung ein Teil der IT-Infrastruktur, nur wurden sie durch die Gefahren aus dem Internet immer wichtiger. Auch die Zeitintervalle zwischen den Backups wurden gekürzt, um bei einem Wiederherstellungsverfahren nicht zu viele Daten und eingesetzte Arbeitszeit zu verlieren. Bei den meisten Unternehmen verläuft das Datenbackup automatisch.

- **Cluster-Systeme:** Die Cluster-Systeme sollen die Dienste, deren Verfügbarkeit rund um die Uhr verlangt wird, unempfindlich gegen Hardwareausfälle machen. Ein Cluster besteht dabei aus mindestens zwei identischen Servern (Nodes), die auf eine gemeinsame Speichergruppe zugreifen. Die beiden Cluster tauschen ein so genanntes Heartbeat-Signal aus, mit dem sie feststellen, ob die zurzeit aktive Node noch einwandfrei arbeitet. Bleibt das Signal aus, so übernimmt die passive Node den aktiven Part. Master und Slave haben die gleiche IP-Adresse, so dass für den Nutzer der Dienste die Umstellung unsichtbar ist.
  Im Gegensatz zu sogenannten Active/Stand-by-Systemen (bei denen ein redundantes System passiv neben dem aktiven System steht, bis es benötigt wird) bieten Clustering ein Active/Active-System an. Dies bedeutet, dass alle Server ihre zugewiesene Aufgabe erfüllen und, bei Ausfall eines Servers, dessen Aufgabe übernehmen.

- **Intrusion Detection System:** Das Ziel der Intrusion Detection-Systeme ist die Erkennung von Sicherheitsverletzungen und eine angemessene, schnelle Reaktion darauf. Hauptaufgaben des IDS sind:
  - Missbrauchserkennung auf der Netzwerkebene
    Erkennung von Angriffen (Denial of Service, SYN-Flooding, PING-Flooding, Pre-Attack Probe (Information über Netzwerke, Angriffe über Portscan-Verfahren), Angriffe über World Wide Web Dienste (Aktive X, Java,..))
  - Rechnersystembasierende Angriffserkennung

Alle wichtigen Audit-Dateien auf dem System werden überwacht und ausgewertet. Bei Erkennung von Angriffen werden Alarme ausgelöst.
- Erkennung von Anomalien
  Erkennung von untypischen System- und Benutzerverhalten.
- Intrusion Response
  Bei Angriffen können verschiedene Gegenmassnahmen (z.B. Alarme über E-Mail, SMS, Unterbrechung der Verbindung, Protokollierung des Angriffs) eingeleitet werden.
- Ereignismeldungen
  Alle Ereignismeldungen können nach verschiedenen Prioritäten (High, Medium, Low) zugeordnet und angezeigt werden.
- Protokollierung / Berichterstattung
  Es werden Log-Dateien geführt und nach verschiedenen Kriterien ausgewertet (grafische Auswertung).

- **Monitoring-Software:** Das vollautomatische Monitoring überprüft konstant sowohl die Hardware (den Server), die Verbindung zum Internet (Bandbreite etc.) wie auch die Lösung selber (Skripte, Datenbank, URL, etc.) auf Funktionsfähigkeit. Wird ein kritischer Status erreicht, kann die Monitoring Lösung automatisch die nötigen Warnmeldungen via SMS und E-Mail direkt an die Verantwortlichen senden. (ecin.de 1999)

- **Audit-Software:** Jedes IT-System, dessen Aufgabe sich mit klaren Prozessen und Prozeduren beschreiben lässt, kann während des Betriebes mit einer Art Checkliste verglichen werden. Beim Auditing wird geprüft, ob das betroffene System innerhalb der vorgegebenen Parameter der Checkliste arbeitet. In vielen Fällen definieren die Sicherheitsrichtlinien bereits solche Audit-Checklisten – zum Beispiel, dass alle Passwörter mindestens acht Zeichen lang und alle sechs Monate geändert werden müssen – , und die Methoden zum Checklistenabgleich sind ebenfalls klar vorgegeben. Audits können also als passive, nicht invasive Sicherheitsüberprüfung von IT-Systemen angesehen werden.

- **VPN (Virtual Private Network):** Bei einem VPN werden Rechner einer bestimmten geschlossenen Benutzergruppe (z.B. eines Unternehmens oder Haushalts) über das Internet miteinander verbunden.
  Die Verbindung ist mittels sog. Tunnels, in denen die Daten nur verschlüsselt übertragen werden, geschützt.
  Über die Hälfte aller europäischen Unternehmen mit mehr als 1000 Beschäftigten nutzen heute für die Datenkommunikation zwischen verschiedenen Standorten bereits Virtual Private Networks (VPNs) auf Basis des Internet-Protokolls (IP). (ecind.de 2004)

- **PKI (Public Key Infrastructure):** PKI ist eine Infrastruktur zur Verwaltung und Distribution von kryptographischen Schlüsseln. PKI ist die Methode mit deren Hilfe nach dem derzeitigen Stand der Technik die Authentisierung, Identifizierung, Vertraulichkeit und Nichtabstreitbarkeit von elektronischen Daten sichergestellt wird.

- **Antivirenprogramm:** Ein Antivirenprogramm schützt die Systeme vor einem Virenbefall, aber nur so gut, wie ihre aktuelle installierte Virensignatur ist.

- **Antispamprogramm:** Ein Antispamprogramm filtert die Spammails aus. Entweder werden die ausgefilterten Emails gleich oder nach einer kurzen Überprüfung gelöscht, oder sie werden mit einem Header im Betreff gekennzeichnet, damit der User weiss, dass es sich um ein Spammail handeln könnte. Wie bei dem Antivirenprogramm ist das Antispamprogramm nur so gut, wie der Filter eingestellt ist.

Diese Systeme müssen installiert und gepflegt werden, was einen Arbeitsmehraufwand von der IT-Abteilung verlangt.

4.3 IT-Abteilung

Wieder werden nur die Arbeitsaufwendungen betrachtet, die sich auf IT-sicherheits-relevante Systeme beziehen. Speziell die Arbeitsaufwendungen, die durch die Internetbenutzung entstanden sind.
Die Arbeitsaufwendungen wurden durch mehrere Interviews und Diskussionen evaluiert. Durch die Interviews wurde deutlich, dass die Abgrenzung von IT-sicherheitsrelevanten Arbeiten und anderen sehr schwierig ist.

- **Aufsetzen der Systeme:** Wie alle anderen Systeme müssen auch die IT-sicherheitsrelevanten Systeme aufgesetzt werden. Dazu kommen Neuinstallationen und das anschliessende Testen.

- **Vermehrter Datenbackupaufwand:** Datenbackups verlaufen meistens jeden Abend automatisch ab. Wie schon erwähnt, gab es solche Backups auch schon vor einer Internetanbindung. Durch diese Anbindung aber und die damit verbundenen Gefahren hat das Datenbackup eine viel grössere Dringlichkeit erhalten. Dies ist so zu verstehen: Wenn es früher bei einem Datenbackup Probleme gab, so hat man teilweise einfach auf den nächsten gewartet. Doch heute ist es unabdingbar, dass jeden Abend ein Datenbackup gemacht wird, da die Gefahr der Datenzerstörung zugenommen hat. Dies hat zur Folge, dass die Dringlichkeit und daher der Problembehebungsaufwand grösser geworden ist.

- **Wartung Firewall:** Mit dem einmaligen Aufsetzen einer Firewall ist es nicht getan. Dies ist ein Irrglauben von vielen kleinen Unternehmen. Eine Firewall lebt von der Aktualität der Software. Allerdings heisst es hier Vorsicht - denn jede neue Version kann auch wieder neue Sicherheitsrisiken bergen. Neue Programme verlangen vielleicht nach neuen offenen Ports, die noch von der Firewall blockiert werden. Hier soll abgewogen werden, ob diese Neuinstallation wirklich benötigt wird. Leider kommt aber bei vielen Unternehmen Funktionalität vor Sicherheit. Die Aktualisierung der Firewallregeln, die den erlaubten und geblockten Verkehr definieren, sollten spätestens alle 2 Monate aktualisiert werden. Neue Trojaner und Viren können sich nur verbreiten, weil veraltete Regeln bzw. Virensignaturen eingesetzt werden (sys2.de 2003).

- **Wartung Antivirenprogramme:** Die oben genannten Virensignaturen entscheiden über den wirklichen Schutz des Programms. Mit einer alten Signatur könnten neue Viren ungehindert in ein Netz einbrechen. Es ist also ein Muss, diese Virensignaturen, -definitionen aktuell zu halten, und zwar bei jedem Rechner. Bei den meisten Firmen funktioniert dies automatisch.
  In regelmässigen Abständen sollte auch ein Virenscan durchgeführt werden, der alle Rechner betreffend Viren untersucht. Auch dies ist automatisierbar, jedoch können

dabei Performanceeinbussen der Rechner entstehen, doch dazu später im Kapitel IT-User.

- **Wartung Antispamprogramme:** Es gibt ebenfalls Spammailsdefinitionen, die das Antispamprogramm auf dem aktuellen Stand hält. Die Filter müssen auch immer wieder einmal mit neuen Filterregeln aktualisiert werden, dies wird meistens manuell vorgenommen. Wenn die Spammails nicht durchgelassen und diese auf einem speziellen Rechner abgespeichert werden, werden sie oft noch von einem Mitarbeiter kurz angeschaut, ob ein Email irrtümlicherweise als Spammail deklariert wurde. So bei einer interviewten Firma, die diese Arbeit täglich macht.

- **Patching:** (englisch Flickwerk). Fehlerbereinigung durch das Ersetzen einzelner Programmteile. Die Unternehmen müssen regelmässig Sicherheitspatchs anwenden, um das Risiko eines zukünftigen Angriffs zu minimieren und ihre Umgebung abzusichern. Um IT-Ressourcen sicher zu halten, ist eine proaktive Sicherheitspatch-Verwaltung notwendig. Dies fängt bei der Patchsuche an, die Klassifizierung und Priorisierung eines gefundenen Patchs, sowie das testen und anschliessende aufspielen. Oft werden auch einige Patchs zu Patchpaketen zusammengefasst und diese dann in gewissen Zeitabständen aufgespielt, damit nicht dauernd einzelne Patchs installiert werden müssen. (ComputerZeitung 2003)
  Die Sicherheitspatch-Verwaltung wird in „Microsoft-Leitfaden zur Sicherheitspatch-Verwaltung“ (Microsoft 2003) detailliert beschrieben und wird deshalb hier nicht weiter vertieft.

- **Logfiles überprüfen:** Das Auswerten von Logfiles ist eine wichtige Angelegenheit, man erfährt zum Beispiel, wo sich Fehler in einer Website eingeschlichen haben und ob auch jemand versucht hat, die Website zu cracken. Doch Logfiles werden nicht nur aus Webzugriffen erstellt, sondern bei jedem anderen Zugang auch, so auch bei einer Firewall. Meistens wird das Logfile auf Anomalien überprüft und bei Bedarf kann sofort reagiert werden. Auch Stichproben werden gemacht, die man dann analysiert, so zum Beispiel bei erhöhtem Emailvolumenverkehr. Jeden Monat sollte ein Report erstellt werden.

- **Kontrollsoftware überprüfen:** Zu den Kontrollsoftwares werden hier Intrusion Detection System, Monitoring- und Audits-Software gezählt. Wie oben schon erwähnt, sollten diese bei Erkennung von untypischen System- und Benutzerverhalten einen Alarm auslösen. Die IT-Mitarbeiter gehen dann diesen Anomalien nach und überprüfen, ob es sich um einen Angriff handelt. Da aber auch oft Falschalarme ausgegeben werden, müssen die IT-Mitarbeiter diese Software ständig darauf abstimmen, damit das nächste Mal nicht der gleiche Falschalarm wieder auftritt. In regelmässigen Abständen sollte, wie bei den Logfiles, ein Report erstellt und nach Oben kommuniziert werden.

- **Self-Attack:** Im Rahmen eines Penetrationstests prüfen Spezialisten die Systeme auf Schwachstellen und Sicherheitsrisiken von aussen. Damit nehmen sie die Rolle eines externen Angreifers ein. Ziel des Tests ist es, die Sicherheitsmechanismen des Systems auf Herz und Nieren zu prüfen und damit die Sicherheit gegen Angriffe auf Vertraulichkeit, Integrität und Verfügbarkeit zu untersuchen. Nach erfolgreichem Abschluss des Tests liegt dem Unternehmen eine Dokumentation über alle Schwachstellen und Sicherheitsrisiken der Systeme vor.

- **Selbststudium, Internetrecherche:** Will ein Mitarbeiter einer Sache (z.B. einer Anomalie im Netzwerk) auf den Grund gehen, so macht er teilweise Internetrecherchen. Evt. sind solche Probleme bereits bekannt. Positiver Nebeneffekt: Der Mitarbeiter erweitert dadurch seinen Wissensstand. Internetrecherchen und Selbststudium müssen nicht unbedingt aus einer Anomalie im Netzwerk entstehen, sondern es ist oft der Wissensdurst und die Neugier, die die Mitarbeiter dazu bewegen. Gerade in der IT-Sicherheit, bei der sich die Produkte in ständigem Wandel befinden und man nie weiss, was die Zukunft noch so alles mit sich bringen wird, ist man auf aktuelles Know-how angewiesen, was Selbststudium und Internetrecherchen unabdingbar macht.
  Wird zum Beispiel bekannt, dass wieder einmal ein Virus sein Unwesen treibt, so wird von den verantwortlichten IT-Mitarbeitern verlangt, dass sie der Sache nachgehen und mögliche Risiken für das eigene Unternehmen evaluieren.

- **IT-Mitarbeiterschulungen:** Ähnlich wie das Selbststudium, nur dass hier vom Unternehmen den IT-Mitarbeitern Seminare und Schulungen angeboten werden. Die Kosten müssen hier nur auf Schulungen mit IT-sicherheitsrelevante Themen bezogen werden.

4.4 Management und Organisation

Die Arbeiten des Managements und der Organisation, welche die IT-Sicherheit durch Internetbenutzung betreffen, werden hier durchleuchtet. Es ist auch gut möglich, diesen Punkt im Arbeitsaufwand der IT-Abteilung unterzubringen. Jedoch werden hier das Management und die Organisation als eine Stufe höher betrachtet. Bei den kontinuierlichen Arbeiten sind zum Beispiel administrative Arbeiten zu nennen. Andere Arbeiten sind mehr Projekt bezogen. Das Problem ist herauszufinden, welchen Anteil die IT-Sicherheit an den Gesamtarbeiten hat. Das Problem mit der Abgrenzung also.

- **Hard- und Softwareeinkauf:** Die Auswahl an Sicherheitshardware und –software wird immer grösser, es kann nun ein Produkt ausgewählt werden, das die Bedürfnisse eines Unternehmens am besten abdeckt. Jedoch muss für dieses Auswahlverfahren viel mehr Zeit in Anspruch genommen werden und es ist auch nicht immer einfach, das passende Produkt für sein Unternehmen zu finden.

- **Systemlandschaft managen:** Die IT-Infrastruktur der Unternehmen wird immer grösser und komplexer. Und da nur schon ein ungepatchter Zugangsserver eine grosse Gefahr für das ganze System darstellen kann („die Kette ist nur so stark wie ihr schwächstes Glied“), ist es von äusserster Wichtigkeit, die Systemlandschaft mit all ihren Komponenten bis ins Detail zu kennen, es sollte in regelmässigen Abständen eine Inventarisierung der Systeme stattfinden. Das Management und die Organisation dieser Systemlandschaft, gerade wenn es Umstrukturierungen gibt, benötigen aber viel Arbeitszeit. Die Systemlandschaft wird mittels Stichproben ständig kontrolliert, ob sie auch mit den theoretischen Plänen übereinstimmt. Bei sehr grossen IT-Infrastrukuren ist die Übereinstimmung aber nur sehr schwer zu kontrollieren.

- **IT-Sicherheitsrichtlinie:** Die wichtigste Positionierung zum Stellenwert der IT-Sicherheit im Unternehmen und zum anzustrebenden Sicherheitsniveau ist die IT-Sicherheitsrichtlinie (Security Policy) der Unternehmensleitung. Sie gibt die Sicherheitsziele für ein zentral organisiertes und unternehmensweit gesteuertes IT-Sicherheitsmanagement und für die umzusetzenden Sicherheitsmassnahmen vor. Diese IT-

Sicherheitsrichtlinie sind in die allgemeine Policy des Unternehmens integriert. Die Einhaltung dieser Richtlinien wird bei den befragten Firmen nur sporadisch überprüft. Es wird an das Verantwortungsbewusstsein der Mitarbeiter appelliert und ihnen auch Vertrauen geschenkt. Erst bei einem erkannten Verstoss wird vorgegangen (bull.at Internetseite).

- **IT-Risikoanalyse:** Die IT-Risikoanalyse dient in erster Linie dazu, die Risiken des IT-Einsatzes sowie die Wirtschaftlichkeit einzelner IT-Sicherheitsmassnahmen transparent zu machen. Dies erfolgt, indem für jede der in der Bedrohungsanalyse ermittelten IT-Bedrohungen zunächst festgelegt wird, wie hoch die Wahrscheinlichkeit ihres Eintretens und wie hoch die monetäre Schadenshöhe ist, die durch das Eintreten der Bedrohung entsteht. Die einzelnen Parameter werden anschliessend in einer Matrix in Relation zueinander gesetzt.
  Durch das Gesetz der Kontrolle und der Transparenz in Deutschland sollte ein Unternehmen aufzeigen, wie hoch das Risiko eines möglichen IT-Schadens sein könnte (Lang 2003).

- **IT-Sicherheitsgutachten:** Durch Penetrationstests von externen Experten kann ein Sicherheitsgutachten erstellt werden, welches wiederum für das Risikomanagement herangezogen werden kann. Durch den Penetrationstest wird man auch auf Lücken aufmerksam gemacht, die dann zu schliessen sind. Vom Verwaltungsrat oder auch von Partnern kann so ein Sicherheitsgutachten von externen Experten verlangt werden.

- **Notfallplan:** Hatte trotz aller Vorsichtsmassnahmen ein Angriffsversuch Erfolg und es ist zum Beispiel ein Virus in das System eingedrungen, so gilt es bestimmte Regeln zu beachten, die die weitere Ausbreitung stoppen. Dafür bedarf es eines Notfallplans, der den Mitarbeitern einen Leitfaden für richtiges Verhalten in die Hand gibt. Dieser Notfallplan sollte immer wieder aktualisiert werden, da die IT-Infrastruktur sich ständig wandelt. Gegebenenfalls sollte der Notfallplan sogar getestet werden. (Microsoft 2003, Kapitel 6)

4.5 IT-User

Die IT-User haben eigentlich nicht direkt etwas mit IT-Sicherheitsmassnahmen zu tun, sie werden aber durch Blockierungen und Beschränkungen, die die IT-Sicherheitsmassnahmen verursachen, in ihrer Produktivität gehemmt. Es ist jedoch auch zu sagen, dass der Funktionalitätsgedanke oft vor dem Sicherheitsgedanken kommt.
Es werden folgende Punkte betrachtet:

- **Beschränkungen:** Durch die immer grösseren Gefahren aus dem Internet wurden die Userrechte immer mehr eingeschränkt. Es kann zum Beispiel sein, dass eine Javaapplikation eines IT-Users, die Informationen aus dem Internet bezieht, durch den Einsatz einer Firewall nicht mehr funktioniert. Oder das Ausführen einer Installationsdatei ist den meistens IT-Usern versagt beziehungsweise bei ihren Arbeitsrechnern ohne Systemadministratorrechte gar nicht möglich, obwohl es sich vielleicht um eine vertrauenswürdigen Datei von einem Kunden handelt. Wie weit aber diese Beschränkungen den IT-User in seiner Produktivität einschränken, ist nur sehr schwer abzuschätzen (Heindl u.a. 2001).

- **Blockierungen:** Unter Blockierung wird hier die Nichtverwendbarkeit des Arbeitsrechners verstanden. Arbeitet ein IT-User ausschliesslich mit seinem Arbeitsrechner

und kann sich bei einer Blockade von diesem nicht mit einer andere Arbeit befassen, so ist die Blockierungszeit mit der Produktivitätsverlustzeit gleichzustellen.
Dies ist zum Beispiel beim Patchen zu beobachten, wobei dieses Verfahren aber sehr unterschiedlich von den Firmen gehandhabt werden kann. Beispiele:

- Das Patchverfahren läuft im Hintergrund, der IT-User merkt nichts, evt. kleinere Performance einbussen → keine Blockierung.
- Das Patchverfahren blockiert den Arbeitsrechner. Der IT-User wird aber gefragt, wann der Patch aufgespielt werden soll, somit kann der Patch in der Mittagspause aufgespielt werden → keine Blockierung.
- Das Patchverfahren blockiert den Arbeitsrechner. Jede Woche wird z.B. am Montagmorgen beim Neustart des Rechners gepatcht, während der Patchzeit ist dann der Arbeitsrechner blockiert.

Bei den dringlichen Patchs werden die Arbeitsrechner gleich nach dem Versenden gepatcht, bei diesen kann dann nicht bestimmt werden, wann der Rechner gepatcht werden soll. Diese Patchs verlangen auch oft nach einem Restart der Arbeitsstationen.
Ähnlich funktioniert es bei einem Virenscan eines Arbeitsrechners, bei solch einem Scan, der meist wöchentlich abläuft, werden die Rechner zwar fast nie blockiert, aber Performanceeinbussen müssen in Kauf genommen werden.
Gibt es ein Problem bei einer IT-Sicherheitsmassnahme, zum Beispiel bei einem gepatchten Arbeitsrechner, so muss ein Supporter vorbei kommen und dem Problem nachgehen, was wieder beinhaltet, dass dann der IT-User in seiner Arbeit blockiert ist.

- **Verunsicherung des IT-User:** Die IT-User werden zum Beispiel durch IT-Sicherheitsinformationen oder Radiomeldungen über aktuelle Viren verunsichert, was dazu führen könnte, dass sie sich via Internet selber informieren oder zum Beispiel bei einem Email von einem Fremden gleich die IT-Hotline anrufen.

- **Schulung, Awareness:** Die Mitarbeiter werden auf die Gefahren aus dem Internet und auf die IT-Sicherheitsmassnahmen aufmerksam gemacht. Was mittels Schulung, Newslettern oder Onlineinformationen vonstatten geht.

- **Spammails:** Trotz Antispamprogramme gelangen immer noch einige Spammails in die Emailbox des IT-Users. Oder, wie oben in Kapitel 4.2 beschrieben, setzt das Antispamprogramm nur beim Betreff ein Spamzeichen, und somit gelangen alle Spammails mit gekennzeichnetem Betreff in die Emailbox. Die Zeit, die sich der User mit diesen Spammails herumschlägt, wird als Produktivitätsverlust gerechnet.

5 Kostenfaktoren und Zeitaufwand für IT-Sicherheitsmassnahmen

Durch die vier in Kapitel 1.4 erwähnten Interviews wurden die Kostenfaktoren validiert und ergänzt. Da von den interviewten Firmen keine Zahlen veröffentlicht werden dürfen, wird unten kurz eine fiktive Firma „KIT-S“ vorgestellt, auf diese sich dann die Beispielberechnungen beziehen. Es mussten auch einige Schätzwerte angenommen werden, da es den interviewten Firmen nicht immer möglich war, eine präzise Angabe zu machen.
Der hier gezeigte Zeitaufwand der verschiedenen Arbeiten kann bei den Unternehmen sehr unterschiedlich sein, auch wenn die Unternehmen eine ähnliche Grösse haben. Es ist nur in Ansätzen möglich, den Zeitaufwand mittels der Parameter „Anzahl Systeme“ oder „Anzahlt Mitarbeiter“ zu berechnen, daher wird es hier oft bei einem Zeitaufwandparameter belassen. Dieser ist sehr firmenspezifisch und muss daher von den Firmen selbst durch detailliertes Protokollieren aller Arbeitsabläufe und –zeiten bestimmt werden.

Produkte für IT-Sicherheit

IT-Abteilung
- Aufsetzen von IT-sicherheitsrelevanten Systeme
- Wartungsarbeiten
- Vermehrter Datenbackupsaufwand
- Patching
- Logfiles/Kontrollsoftware überprüfen
- Self-Attacks
- Selbststudium, Internetrecherche
- IT-Mitarbeiterschulungen

Management und Organisation
- Hard- und Softwareeinkauf
- Systemlandschaft managen
- IT-Sicherheitsrichtlinie
- IT-Risikoanalyse
- IT-Sicherheitsgutachten
- Notfallplan

IT-User
- Beschränkungen
- Blockierungen
- Verunsicherung des IT-Users
- Schulung, Awareness
- Spammails

Abb. 5-1: Kurzübersicht nachfolgender Kosten-/Zeitaufwandanalysen

5.1 Vorstellung einer fiktiven Firma „KIT-S“

„KIT-S“ ist im Finanzdienstleistungssektor tätig. Die Dienste „Internet-Banking“ und „Internet-Portal“ werden angeboten. Das Funktionieren ihrer IT-Infrastruktur ist von äusserster Wichtigkeit, denn es werden beinahe alle Arbeiten am Arbeitsrechner erledigt. Ebenso ist der Internetzugriff für das Unternehmen unabdingbar. Der Datenschutz wird in der Firma gross geschrieben, auf keinen Fall dürfen Unbefugte an die geheimen Daten gelangen.

Zahlen:

Umsatz:	3'000'000'000.- [CHF]
Mitarbeiter:	200 [Anz]
Mitarbeiter in IT-Abteilung:	20 (5 befassen sich bewusst mit IT-Sicherheit) [Anz]
IT-Budget:	10'000'000.- [CHF]
IT-Sicherheits-Budget:	nicht ausgewiesen
Arbeitsrechner:	210 [Anz]
Server:	70 [Anz]

Die IT-sicherheitsrelevanten Arbeiten werden neben allen anderen Arbeiten in der IT-Abteilung erledigt, daher nicht speziell ausgewiesen.

Weiter wird folgendes angenommen:

Jahresarbeitszeit in Stunden:	1'800 [h]
Arbeitstage pro Jahr:	225 [d]
Arbeitsstunden pro Tag:	8 [h]
Arbeitsplatzkosten pro Stunde:	140.- [CHF]

5.2 Produkte für IT-Sicherheit

Im vorhergehenden Kapitel wurden einige Produktbeispiele, die für die IT-Sicherheit bei Internetbenutzung wichtig sind, aufgelistet. Nicht jedes Unternehmen setzt aber die gleiche Technologie und die gleichen Produkte ein, weshalb grosse Unterschiede zwischen den einzelnen Firmen entstehen können.
Die Kosten dieser Produkte sind am besten erfassbar, da sie aus einem detaillierten IT-Budget herausgelesen werden können. Falls sicherheitsrelevante Soft- und Hardware mit allen anderen Produkten ausgewiesen werden, muss die Beschaffungsliste durchgecheckt werden. Teilweise ist es aber schwierig, eine Abgrenzung zwischen den IT-sicherheits-relevanten Produkten und anderen Produkten vorzunehmen, denn gewisse Produkte können auch nur zum Teil IT-sicherheitrelevant sein, wie zum Beispiel bei einem Komplettangebot einer Bankensoftware.

Die Kosten werden in Anschaffungskosten und in wiederkehrende Kosten unterteilt. Grosse Anschaffungskosten können über 3-5 Jahre buchhalterisch abgeschrieben werden.
Generell ist der Hardwareanteil an den Produktgesamtkosten 1/3, für Software 2/3.

Kosten für IT-sicherheitsrelevante Produkte	=	Anschaffungskosten (Hardware/Software) + Wiederkehrende Kosten (Lizenzen/Wartungen)

Beispiel „KIT-S“:
Annahmen:
- Da es „KIT-S“ eine fiktive Firma ist, sind die Ausgaben nicht detailliert bekannt. Erfahrungsgemäss wird für das IT-Sicherheitsbudget zwischen 4-8 Prozent geschätzt.

	Kosten pro Jahr
IT-sicherheitsrelevante Produkte	**420'000.- [CHF]**

5.3 IT-Abteilung

Bei den folgenden Berechnungen steht der Zeitaufwand für eine Arbeit im Vordergrund. Dieser durchschnittliche Zeitaufwand ist variabel, weshalb jedes Unternehmen ihren IT-Aufwand selbst schätzen muss. Eine allgemein gültige Aussage wäre unrealistisch. Um einen möglichst exakten Zeitaufwand berechnen zu können, müsste der Arbeitsaufwand über einen längeren Zeitraum detailliert erfasst werden. Auch die Abgrenzung, zwischen IT-sicherheitsrelevante Arbeiten und anderen IT-Arbeiten, bereitet den Unternehmen Schwierigkeiten. (cirosec.de (Internetseite))
In diesem Kapitel wird aufgezeigt, welche verschiedenen Arbeiten in einer IT-Abteilung für die IT-Sicherheit anfallen und wie sich diese zusammensetzen.
Wenn nicht anders erwähnt, sind der Zeitaufwand und andere Angaben immer pro Jahr angegeben.

Aufsetzen von IT-sicherheitsrelevanten Systeme:
Wie alle anderen Systeme müssen auch die IT-sicherheitsrelevanten Systeme aufgesetzt oder neu installiert werden. Dazu gehört ebenso das anschliessende Testen wie auch die Dokumentation.

Zeitaufwand fürs Aufsetzen	=	Anzahl Neuinstallationen pro Jahr * (Installation + Testen + Dokumentationserstellung)

Beispiel „KIT-S“:
Annahmen:
- Anzahl IT-sicherheitsrelevante Systeme neu aufsetzen oder installieren = 2 pro Jahr
- Installationsdauer = 1 Manntag (8 h)
- Testdauer pro Installation = 2 Manntage (16 h)
- Dokumentationserstellung = ½ Manntag (4 h)

	Berechung in Stunden	Zeitaufwand pro Jahr	Kosten pro Jahr
Installation	2*8	16.00 [h]	2'240.- [CHF]
Testen	2*16	32.00 [h]	4'480.- [CHF]
Dokummentation	2*4	8.00 [h]	1'120.- [CHF]
Aufsetzen	**2*(8+16+4)**	**56.00 [h]**	**7¨840.- [CHF]**

Wartungsarbeiten:
Antivirenprogramme und Spamfilter müssen aktuell gehalten werden. Eine neue Virensignatur wird bei den meisten Unternehmen automatisch aufgespielt, daher ist bei diesen Unternehmen kein Aufwand notwendig. Die neuen Spammailsdefinitionen werden auch meistens automatisch installiert. Die Aktualisierungsfunktionskosten werden mit den Lizenzkosten abgedeckt. Spamfilterregeln können eingekauft oder selbst definiert werden. Bei einigen Unternehmen schaut ein Mitarbeiter noch vor dem Löschen der Spammails alle aussortierten Emails an, ob eines vielleicht irrtümlich als Spam behandelt wurde.
Die Wartungsarbeiten der Firewall werden nicht so kontinuierlich durchgeführt, es wird zum Beispiel nur bei Neuinstallationen geprüft und abgewogen, ob ein neuer Port geöffnet werden sollte. Meistens findet die Wartung der Firewalls einmal pro Jahr statt, was aber nicht ausreichend ist, jedes Quartal wäre mindestens wünschenswert.

Zeitaufwand für Wartungsarbeiten	=	Allg. Filterregeln festsetzen + automatische Aktualisierungsinstallationen überprüfen + (Anzahl ausgefilterte Spammails pro Jahr * Spammailüberprüfungsdauer pro Spammail) + (Anzahl Firewalls * Wartungsdauer pro Firewall und Jahr)

Beispiel „KIT-S“:
Annahme:
- Allg. Filterregeln festsetzen = 2 Manntage pro Jahr (16 h)
- automatische Aktualisierungsinstallation überprüfen = 1 Minute pro Tag (0.0166 h)
- Anzahl ausgefilterte Spammails pro IT-User = 15 pro Tag
- Spammailüberprüfungsdauer pro Spam = ½ Sekunde (0.0001388 h), sehr kurz, da z-B Globalspam gleich gelöscht werden können
- Anzahl Firewalls = 3
- Wartungsdauer pro Firewall und Jahr = 2 Manntage (16 h, ½ Manntag pro Quartal)

	Berechung in Stunden	Zeitaufwand pro Jahr	Kosten pro Jahr
Filterregeln festsetzen	16	16.00 [h]	2'240.- [CHF]
Aut. Aktual. Uberprüfen	0.0166*225(Tage)	3.75 [h]	525.- [CHF]
Spammailsüberprüfung	15*200(IT-User) *0.0001388 *225(Tage)	93.75 [h]	13'125.- [CHF]
Wartung Firewall	3*16	48.00 [h]	6'720.- [CHF]
Wartungsarbeiten		**161.50 [h]**	**22'610.- [CHF]**

Spammailkontrolle kann auch auf die User abgewälzt werden, indem einem Spammail am Anfang des Betreffs ein Spamzeichen hinzugefügt wird. So kann der User selbst prüfen, ob es sich wirklich um ein Spammail handelt.

Vermehrter Datenbackupaufwand:
Die Datenbackups laufen bei den meisten Unternehmen automatisch ab. Aber durch die Internetgefahren ist ein Datenbackup noch dringlicher geworden, daher muss auf Probleme sofort reagiert werden. Früher hat man eher auf das nächste Datenbackup warten können. Durch die Problembehebung entsteht vermehrter Aufwand beim Datenbackup.

Zeitaufwand für vermehrte Datenbackups	=	Anzahl Probleme beim Datenbackup * Problembehebungsdauer pro Problem

Beispiel „KIT-S“:
Annahmen:
- Anzahl aufgetretene Probleme im Jahr = 1% der verschiedenen Datenbackups (Anzahl Arbeitstage * durchgeführter Datenbackups pro Tag)
- Datenbackups pro Tag = 1
- Problembehebungsdauer = 4 Stunden

	Berechung in Stunden	Zeitaufwand pro Jahr	Kosten pro Jahr
Vermehrte Problembehebung bei Datenbackups	2.25*4	**9.00 [h]**	**1'260.- [CHF]**

Patching:
In einem Artikel aus dem Internet wurde folgende Aussage gemacht:
„Nach einer neueren Untersuchung nimmt das Aufspielen von Patchs fast 10 Prozent des Arbeitsaufwands einer EDV-Abteilung in Anspruch, bei manchen Firmen sogar mehr. Trotzdem liegen bei den wenigsten Firmen konkrete Richtlinien für das Installieren von Patchs vor.“ (Bennett 2004a)

Die Interviews führten zu unterschiedlichen Ergebnissen. Die Taktik zum Beispiel einer interviewten Firma ist, nicht der Firstmover bei einem Patchverfahren zu sein, somit ersparen sie sich teilweise das Testen, da andere Unternehmen schon ihre Erfahrungen mit dem Patch gemacht haben. Wiederum geht das auf Kosten der Sicherheit.
10 Prozent des Arbeitsaufwands einer EDV-Abteilung scheint hier den interviewten Firmen viel, aber es ist nicht klar, ob beim oben erwähnten Bericht die Kontrolle und das Kennen der Systemlandschaft zum Patchverfahren hinzugezählt werden. Diese Kontrollen und das Kennen der Systemlandschaft schlagen gerade bei grossen Firmen schwer ins Gewicht. In dieser Arbeit wird dies aber in einem separaten Punkt bearbeitet.
Auch die Intervalle des Patchens sind bei den Firmen sehr unterschiedlich. Bei einigen wird jede Woche an einem bestimmten Tag ein möglicher Patch aufgespielt, bei anderen nach Bedarf. Der Patchzeitpunkt hängt auch von der Dringlichkeit des Patchs und der Wichtigkeit des zu patchenden Systems ab.
Nicht bei jedem Patch handelt es sich um einen IT-sicherheitsrelevanten Patch, aber es ist schwierig, diese separat aufzuführen. Denn von den Unternehmen werden Patchpakete zusammengestellt, die unterschiedliche Patchs enthalten, diese werden dann nach einer Testphase auf die Rechner installiert. Solch ein Paket wird vielleicht jeden Monat kreiert und installiert. Hat der Patch aber hohe Priorität, sollte sofort gehandelt werden und alle Systeme mit diesem Patch upgedated werden (Gerbich u.a. 2003).
Das Aufspielen der Patchs kann bei den meisten grösseren Firmen automatisch ausgelöst werden, daher spielt die Anzahl der Rechner beim Patchaufspielen keine Rolle, bei den kleineren Firmen muss aber vielleicht der Systemadministrator bei jedem Rechner mittels einer CD den Patch installieren, was den Zeitaufwand in die Höhe schnellen lässt.
Die Unternehmen sind bemüht, ihre Systeme zu standardisieren, damit sie weniger verschiedene Patchpakete zusammenstellen müssen, auch die Anzahl an Patchproblemen wird dadurch geringer. Dieser Punkt wurde aber nicht in die Formel übernommen.

Ein Patchvorgang kann folgendermassen aussehen: Patchinformationssuche, Patchpaket zusammenstellen, Patch testen, Patch aufspielen und evt. Problembehebungen. Dringliche Patchs werden nicht zu Paketen zusammengestellt, da sie sofort installiert werden müssen. Der Produktivitätsverlust der IT-User ist hier nicht berücksichtigt, folgt später in Kapitel 5.5.

Zeitaufwand fürs Patching	=	Patchinformationssuche + Anzahl Patchpakete * (Patchpaket zusammenstellen + Patch testen + Patch aufspielen + Anzahl Probleme pro Patchvorgang * Problembehebungdauer pro Problem) + Anzahl dringlicher Patchs * (Patch testen + Patch aufspielen + Anzahl Probleme pro Patchvorgang * Problembehebungdauer pro Problem)

Beispiel „KIT-S“:
Annahmen:
- Patchinformationssuche (Newsletter und Internetrecherche) = 15 Minuten pro Woche (0.05 h pro Tag)
- Anzahl Patchpakete pro Jahr = 12 (jeden Monat ein Paket)
- Anzahl dringlicher Patchs pro Jahr = 4
- Patchpaket zusammenstellen = 2 Manntage (16 h)
- Patchpaket / Patch testen = 3 Manntage (24 h)
- Patchaufspielen = automatisch = Aufwand gleich 0 (Userblockierung später)
- Anzahl Probleme = 1% aller gepatchten Systeme (2.8 von 280 Systeme)
- Zeitdauer Problembehebung = 2 Mannstunden pro Problem

	Berechung in Stunden	Zeitaufwand pro Jahr	Kosten pro Jahr
Patchinformationssuche	0.05*225(Tage)	11.25 [h]	1'575.- [CHF]
Patchpakete zst., t., a.	12*(16+24+0)	480.00 [h]	67'200.- [CHF]
Patchpakete Problembeh.	12*2.8*2	67.20 [h]	9'408.- [CHF]
Dringliche Patchs t., a.,	4*(24+0)	96.00 [h]	13'440.- [CHF]
Patchs Problembehebung	4*2.8*2	22.40 [h]	3'136.- [CHF]
Patching		**676.85 [h]**	**94'759.- [CHF]**

Logfiles/Kontrollsoftware überprüfen:
Bei den Logfiles gehen einige Unternehmen nach dem Stichprobeverfahren vor, andere beobachten Datenvolumen, grössere Firmen analysieren die Logfiles systematisch.
Die Logfiles werden auf Anomalien geprüft, wird eine gefunden, geht man der Sache nach. Die Kontrollsoftware (wie IDS, Monitoring- und Audit-Software) lösen bei einer Anomalie einen Alarm aus, was für den IT-Mitarbeiter eine grosse Hilfe bei der Erkennung von untypischen Benutzer- und Systemverhalten ist. Aber nicht jede Anomalie ist eine Attacke von aussen, es gibt in dieser Hinsicht einige Falschalarme, die auch überprüft werden. Die Parameter der Kontrollsoftware sollten bei diesen Falschalarmen immer

analysiert und gegebenenfalls neu gesetzt werden, damit sich die Falschalarme nicht ständig wiederholen.
Reporte sollten kontinuierlich erstellt und nach Oben kommuniziert werden.

Zeitaufwand für Logfiles- / Kontrollsoftware-überprüfung	=	Logfiles/Kontrollsoftware überprüfen + Anomalien nachgehen + Kontrollsoftware warten + Reporte erstellen

Beispiel „KIT-S“:
Annahmen:
- Zeitdauer der Logfiles-/Kontrollsoftwareüberprüfung = 1 Mannstunde pro Tag
- Anzahl Anomalien pro Jahr = 26 (jede zweite Woche eine)
- Zeitdauer der Anomalienachforschung und evt. Kontrollsoftware-Wartung = 2 Mannstunden
- Reporting = 4 Mannstunden pro Monat

	Berechung in Stunden	Zeitaufwand pro Jahr	Kosten pro Jahr
Logfilesüberprüfungen	1*225(Tage)	225.00 [h]	31'500.- [CHF]
Anomalien nachgehen und evt. Wartung der K-SW	26*2	52.00 [h]	7'280.- [CHF]
Reporting	4*12(Monate)	48.00 [h]	6'720.- [CHF]
Logfilesanalyse		**325.00 [h]**	**45'500.- [CHF]**

Self-Attacks:
Self-Attacks werden in Form eines Penetrationstest durchgeführt. Das System wird dabei auf Schwachstellen überprüft und anschliessend ein Report erstellt. Penetrationskosten können von der Grösse und der Komplexität der simulierten Angriffe abhängen. Die Häufigkeit dieser Tests ist ebenfalls sehr unterschiedlich, meistens werden sie als Projekt durchgeführt.

Zeitaufwand für Self-Attacks	=	Anzahl Self-Attacks pro Jahr + Anzahl verwendete Mannstunden (inkl. Reporting)

oder

Kosten für Self-Attack-Projekt	=	Projektkosten in Budget

Beispiel „KIT-S“:
Annahmen:
- Anzahl Self-Attacks = 1 pro Jahr
- Dauer eines Penetrationstest = 15 Manntage (120 h)

	Berechung in Stunden	Zeitaufwand pro Jahr	Kosten pro Jahr
Self-Attacks	1*120	**120.00 [h]**	**16'800.- [CHF]**

Selbststudium, Internetrecherche:
Die immerwährende Weiterentwicklung der Technologien in der IT-Sicherheit und die ständig neuen Bedrohungen aus dem Internet verlangen von den IT-Mitarbeitern, speziell von denen, die sich mit IT-Sicherheit befassen, kontinuierliche Weiterbildung. Dies geschieht aber seltener in offiziellen Fortbildungskursen, als vielmehr im Selbststudium. Da das Internet eine grosse Informationsquelle bietet, gerade wenn es um die IT-Sicherheit geht, wird oft auf dieses zugegriffen.

Zeitaufwand für Selbststudium/ Internetrecherchen	=	Anzahl IT-Mitarbeiter, die sich mit IT-Sicherheit befassen * (Dauer der Internetrecherchen + Dauer des Selbststudium)

Beispiel „KIT-S“:
Annahmen:
- Anzahl IT-Mitarbeiter, die sich bewusst mit IT-Sicherheit befassen = 5
- Dauer der Internetrecherchen betreffend IT-Sicherheit = 1 Stunde pro Tag
- Dauer des Selbststudium = wird in der Freizeit gemacht

	Berechung in Stunden	Zeitaufwand pro Jahr	Kosten pro Jahr
Internetrecherchen	5*1*225(Tage)	**1125.00 [h]**	**157'500.- [CHF]**

IT-Mitarbeiterschulungen:
Ähnlich wie das Selbststudium, es werden jedoch von Unternehmerseite Seminare und Schulungen den IT-Mitarbeitern angeboten. Die Problematik der Berechnung besteht darin, den anteilmässigen IT-sicherheitsrelevanten Teil des Seminars zu bestimmen. Während der Schulungszeit geht beim Mitarbeiter Arbeitszeit verloren, die aber in der untenstehenden Formel nicht berücksichtigt wird. Teilweise müssen die Mitarbeiter auch während ihrer Freizeit an Schulungen teilnehmen.

Kosten für IT-Mitarbeiterschulung	=	IT-Mitarbeiterschulungsbudget * Anteil an IT-sicherheitsrelevanten Schulungen

Beispiel „KIT-S“:
Annahmen:
- Weiterbildungsbudget = CHF 200'000.-
- Anteil der Weiterbildung betreffend IT-Sicherheit = durchschnittlich 25% (die 5 IT-Sicherheitsfachleute mehr, andere weniger)
- Ohne Arbeitszeitverlust (in Budget kalkuliert)

	Kosten pro Jahr
IT-Mitarbeiterschulung	**50'000.- [CHF]**

5.4 Management und Organisation

Das Management und die Organisation werden hier losgelöst von der IT-Abteilung betrachtet. Es werden teilweise übergeordnete Themen behandelt, die aber auch in vielen Unternehmen in der IT-Abteilung bearbeitet werden können. Bei den kontinuierlichen Arbeiten sind zum Beispiel administrative Arbeiten zu nennen. Andere Arbeiten sind mehr Projekt bezogen.

Die Schwierigkeit besteht auch hier, eine Abgrenzung zwischen IT-sicherheitsrelevanten Arbeiten und anderen Arbeiten vorzunehmen. Oft sind IT-sicherheitsrelevante Arbeiten Bestandteile eines Projekts, einer Neuorganisation etc.

Hard- und Softwareeinkauf:
Durch die grosse Auswahl an IT-Sicherheitsprodukten, wird der administrative Aufwand beim Einkauf immer grösser. Zuerst müssen die Bedürfnisse ans Produkt genau festgelegt werden. Verschiedene Produkte und auch ihre Preise werden dann miteinander verglichen, bevor die Entscheidung für ein Produkt fällt. Die Unternehmen gehen dabei wie bei ihren anderen Einkäufen vor.
Der Vorgang sieht zum Beispiel folgendermassen aus:
Evaluieren der Bedürfnisse, Marktrecherche/Produktübersicht, grobe Bewertung von Produkt und Anbieter (Vertrauenswürdigkeit), Auswahl von zwei Produkten, Demotest, detaillierte Bewertung der Produkttests, Antrag stellen, Kauf.
Der dafür benötigte Zeitaufwand ist stark vom Investitionsvolumen abhängig.

Zeitaufwand für HW und SW Einkauf	=	Evaluierung der Bedürnisse + Marktrecherche/Produktübersicht + grobe Bewertung von Produkt und Anbieter + Demotest (2 – 3 Produkte) + detaillierte Bewertung der Produkttests + Antrag stellen + Preisverhandlung und Kaufabschluss

oder

Kosten für HW/SW-Einkauf Projekt	=	Evaluierung, Testen und Bewertung sind im Gesamtprojekt schon einberechnet

Beispiel „KIT-S“:
Annahmen:
- Einmaliges Investitionsvolumen im Jahr = CHF 50'000.-
- Folgende Zeiten wurden in Abhängigkeit mit der Investitionssumme geschätzt
- Evaluieren der Bedürfnisse = 8 Mannstunden (Meeting plus Report)
- Produktübersicht = 8 Mannstunden (teilweise in täglichen Internetrecherchen enthalten)
- Grobe Bewertung des Produktes und des Anbieters = ½ Mannstunde
- Demotest mit 2 Produkten = je 2 Manntage (total 32 h)
- Detaillierte Bewertung des Produkttests = 8 Mannstunden
- Antrag stellen = 15 Minuten bei einem Meeting mit Entscheidungsträgern, wird aber meistens nirgends ausgewiesen, daher hier auch nicht berücksichtigt.
- Preisverhandlungen und Kaufabschluss = auch keine Berücksichtigung

	Berechung in Stunden	Zeitaufwand pro Jahr	Kosten pro Jahr
Evaluieren d. Bedürfnisse	8	8.00 [h]	1'120.- [CHF]
Produktübersicht	8	8.00 [h]	1'120.- [CHF]
Grobe Bewertung	0.5	0.50 [h]	70.- [CHF]
Demotest	32	32.00 [h]	4'480.- [CHF]
Detaillierte Bewertung	8	8.00 [h]	1'120.- [CHF]
HW/SW-Einkauf		**48.50 [h]**	**7'910.- [CHF]**

Es soll hier einfach darauf hingewiesen werden, dass sich die Investition nicht nur auf den Einkaufspreis beschränkt.

Systemlandschaft managen:
Der Zeitaufwand für die Kontrolle und die Organisation der Systemlandschaft ist stark von der Grösse der IT-Infrastruktur und deren Komplexität abhängig. Die Wichtigkeit des Kennens der Systemlandschaft und damit verbundenen Inventarisierung wurde oben schon erwähnt. Wird angenommen, dass die Komplexität mit der Grösse der IT-Infrastruktur und Anzahl verschiedener Betriebssysteme korreliert, so wird die Formel von der Anzahl Server, Arbeitsrechner und Betriebssysteme abhängig.
Das Managen der Systemlandschaft kann aber nicht nur zu den Kosten für die IT-Sicherheit betreffend Internetanbindung addiert werden, denn es wurde nicht erst durch die Internetanbindung und deren Gefahren notwendig, aber die Bedeutung hat zugenommen. Gerade wenn zum Beispiel ans Patching gedacht wird, wo jeder Rechner gepatcht werden soll, ohne Ausnahmen.
Aus den Interviews geht hervor, dass dieser Aufwand immer grösser wird.

Zeitaufwand für Systemlandschaft managen	=	Faktor abhängig von Anzahl Rechnern * Faktor abhängig von Anzahl Betriebssystemen * Anteil der IT-Sicherheit an Systemlandschaftsaufwand * Mannstunde

Die Abhängigkeit des Systemlandschaftmanagens von der Komplexität (Anzahl Rechner und Betriebssysteme) zu bewerten, ist sehr schwierig, es müssten wahrscheinlich Sektoren (wie 1 – 100 Rechnern, 100 – 1000 usw.) gewählt werden, die dann mit einem Faktor belegt werden.

Beispiel „KIT-S“:
Annahmen:
- Es werden hier keine Faktorannahmen gemacht, nur einen Wert geschätzt, der von den verschiedenen Interviews abgeleitet wurde.

	Kosten pro Jahr
Systemlandschaft managen	**50'000.- [CHF]**

IT-Sicherheitsrichtlinie:
Eine IT-Sicherheitsrichtlinie ist in die allgemeine Policy des Unternehmens integriert. Ist einmal eine Policy erstellt, werden nur noch kleine Änderungen vorgenommen. Der Inhalt der IT-sicherheitsrelevanten Punkte ist bei den Unternehmen sehr unterschiedlich, sollte daher von jedem selber geschätzt werden. Wie schon erwähnt, wird die Einhaltung der Richtlinien nur sehr sporadisch überprüft, den Mitarbeitern wird einfach vertraut.

Zeitaufwand für IT-Sicherheitsrichtlinie	=	Anteil der IT-Sicherheit an allg. Policy * (Policy Erstellung (einmalig) + Policy Aktualisierung (jährlich) + Gegen Vorstösse vorgehen)

Beispiel „KIT-S“:
Annahmen:
- Dauer der Policyerstellung = 20 Manntage (160 h)
- Policy wird nach fünf Jahren komplett neu erstellt → 32 h pro Jahr
- Aktualisierung = 1 Manntag pro Jahr (8 h)
- Anteil IT-Sicherheit = 20%
- Nachgegangene Verstösse IT-Sicherheit = 1% der Mitarbeiter (2 von 200 Mitarbeitern)
- Durchschnittliche Vorgehensdauer bei Verstössen = 4 Mannstunden

	Berechung in Stunden	Zeitaufwand pro Jahr	Kosten pro Jahr
Policy erstellen	20% *32	6.40 [h]	896.- [CHF]
Aktualisierung	20% *8	1.60 [h]	224.- [CHF]
Nachgegangenen Verstössen	2*4	8.00 [h]	1'120.- [CHF]
IT-Sicherheitsrichtlinie		**16.00 [h]**	**2'240.- [CHF]**

IT-Risikoanalyse:
Eine IT-Risikoanalyse wird nicht von jedem Unternehmen gemacht. Will das Unternehmen aber den „return on security investment“ oder eine Risiko-/Schadensabgrenzung berechnen, so sollte ein Riskmanagement-Projekt über die IT-Sicherheit im Unternehmen lanciert werden. Dabei werden oft Externe miteinbezogen, die hier aber nicht berücksichtigt werden.

Zeitaufwand für IT-Risikoanalyse	=		Dauer der Risikoanalyse
		*	Anzahl involvierter Mitarbeiter

oder

Kosten für IT-Risikoanalyse	=	Projektkosten in Budget

Beispiel „KIT-S“:
Annahmen:
- Risikoanalyse wird einmal im Jahr vorgenommen
- Dauer des Riskmanagement-Projektes = 10 Tage (80 h)
- Involvierte Mitarbeiter = 4
- Ohne Kosten von Externen

	Berechung in Stunden	Zeitaufwand pro Jahr	Kosten pro Jahr
Risikoanalyse	80*4	**320.00 [h]**	**44'800.- [CHF]**

IT-Sicherheitsgutachten:
Vom Verwaltungsrat oder auch von Partnern kann ein Sicherheitsgutachten von Externen verlangt werden. Dies geschieht meistens mit einem Penetrationstest von externen IT-Experten, daher entsteht für das Unternehmen nur ein geringfügiger Arbeitsaufwand (bei der Präsentation des Gutachtens zum Beispiel, was hier aber nicht berücksichtigt wird).
Die Kosten des Gutachtens sollten budgetiert sein.

Kosten für IT-Sicherheitsgutachten	=	Projektkosten in Budget

Beispiel „KIT-S“:
Annahmen:
- Alle zwei Jahre wird ein Sicherheitsgutachten verlangt, Kosten = 40'000.-

		Zeitaufwand pro Jahr	Kosten pro Jahr
IT-Sicherheitsgutachten		**Externe**	**20'000.- [CHF]**

Notfallplan:
Welche Massnahmen sollten bei einem erfolgreichen Angriffsversuch ergriffen werden? Wer sollte was tun? Nach welchen Schritten sollte vorgegangen werden? Diese und noch weitere Fragen sollten in einem Notfallplan beantwortet sein.
Die Erstellung und Aktualisierung eines Notfallplanes sieht ähnliche Arbeitsschritte wie bei den IT-Sicherheitsrichtlinien vor. Es ist oft Projekt bezogen. Das Kennen der Systemlandschaft ist für die Erstellung eines Notfallplans von grosser Bedeutung. Um den Notfallplan zu optimieren, ist ein Durchspielen, Testen notwendig.

Zeitaufwand für Notfallplan	=	Notfallplan erstellen + Durchspielen, Testen + Aktualisierung

oder

Kosten für Notfallplan-Projekt	=	Projektkosten in Budget

Beispiel „KIT-S“:
Annahmen:
- Notfallplan erstellen = 20 Manntage (160 h, 5 Tage mit 4 Mitarbeitern)
- Notfallplan gilt für zwei Jahre → 80 h pro Jahr
- Dauer des Testens = 8 Manntage (64 h, 2 Tage mit 4 Mitarbeitern)
- Durchspielen und Testen = nach Erstellung, sprich alle 2 Jahre → 32 h pro Jahr
- Beim Testen keine Behinderungen der anderen IT-User
- Aktualisierung wenn kein neuer erstellt wird = 8 Mannstunden alle 2 Jahre (→ 4 h)

	Berechung in Stunden	Zeitaufwand pro Jahr	Kosten pro Jahr
Notfallplan erstellen	160:2	80.00 [h]	11'200.- [CHF]
Testen	64:2	32.00 [h]	4'480.- [CHF]
Aktualisierung	8:2	4.00 [h]	560.- [CHF]
Notfallplan		**116.00 [h]**	**16'240.- [CHF]**

5.5 IT-User

Die IT-User haben eigentlich nicht direkt etwas mit IT-Sicherheitsmassnahmen zu tun, sie werden aber durch Blockierungen, Beschränkungen und Ablenkungen, die die IT-

Sicherheitsmassnahmen verursachen, in ihrer Produktivität gehemmt. Auf diese Produktivitätsverluste wird hier eingegangen.

Beschränkungen:
Eine quantitative Aussage zu machen, wie hoch der Produktivitätsverlust bei Beschränkungen durch IT-Sicherheitsmassnahmen liegt, ist äusserst schwierig. Es müssten auch die emotionalen Werte der Mitarbeiter (Ärger, Einsicht der IT-Sicherheits-massnahmen) betrachtet werden, die die Produktivität ebenfalls tangieren. Auf eine Formel wird hier verzichtet, da sie keinen Sinn ergeben würde.

Blockierungen:
Beim Patchen zum Beispiel kann der Arbeitsrechner eines IT-Users blockiert sein, diese Formel bezieht sich auf so einen möglichen Fall. Wie in Kapitel 4.5 beschrieben, gibt es verschiedene Arten, die Systeme zu patchen, darum folgende Regeln:
- Patchen im Hintergrund (→ keine Blockierung), Punkte 1 – 4 von der Formel weg-lassen.
- Patchzeitpunkt bei Patchpaketen bestimmbar (→ keine Blockierung), Punkt 3 von der Formel weglassen.
- Bei dringlichen Patchs wird gleich gepatcht, ohne Zeitpunktentscheidung.
- Punkte 5 – 8 von der Formel betreffen die Problembehebungsdauer.

Produktivitäts-verlust bei Patching-Blockierungen	=	Patchaufspielzeit	1
		* Anzahl IT-User	2
		* (Anzahl Patchpakete	3
		+ Anzahl dringlicher Patchs)	4
		+ (Anzahl Patchpakete	5
		+ Anzahl dringlicher Patchs)	6
		* Anzahl Probleme pro Patchvorgang	7
		* Problembehebungdauer pro Problem	8

Beispiel „KIT-S“:
Annahmen:
- Die Arbeitsrechner sind während dem Patchen blockiert und der IT-User kann auch nicht entscheiden, wann ein Patchpaket gepatcht werden soll, somit fällt bei der Formel nichts weg.
- Jeder IT-User sitzt während des Patchaufspielen am Arbeitsrechner und wartet.
- Anzahl Patchpakete pro Jahr = 12
- Anzahl dringlicher Patchs pro Jahr = 4
- Patchaufspielzeit = 15 Minuten (0.25 h)
- Probleme = 1% aller gepatchten Arbeitsrechner (2.1 von 210 Arbeitsrechner)
- Zeitdauer Problembehebung = 2 Mannstunden pro Problem
- Patchprobleme bei Servern und dadurch Arbeitseinschränkung nicht berücksichtigt.
- Anzahl IT-User = 200

	Berechung in Stunden	Zeitaufwand pro Jahr	Kosten pro Jahr
Patchpakete aufspielen	0.25*200*12	600.00 [h]	84'000.- [CHF]
Dringliche Patchs aufsp.	0.25*200*4	200.00 [h]	28'000.- [CHF]
Patchpaket Problembeh.	(12+4)*2.1*2	67.20 [h]	9'408.- [CHF]
Patch-Blockierung		**867.20 [h]**	**121'408.- [CHF]**

Verunsicherung des IT-Users:
Es soll hier nur erwähnt werden, dass die IT-Sicherheitsmassnahmen und Meldungen von Internet-Attacken, die IT-User verunsichern könnten. Durch diese Verunsicherung können Kosten und Produktivitätsverlust durch Hotline-Anrufe, Internetrecherchen oder Diskussionen am Arbeitsplatz entstehen.
Da die Reaktionen durch Verunsicherung sehr unterschiedlich sein können und vom Mitarbeiter abhängig sind, können keine Kosten evaluiert werden. Eventuell könnten die Hotline-Anrufe untersucht werden, indem die IT-sicherheitsrelevanten Anrufe gezählt werden. Auf eine Abschätzung wird hier aber verzichtet.

Schulung, Awareness:
Die Mitarbeiter werden auf die Gefahren aus dem Internet und auf die IT-Sicherheitsmassnahmen aufmerksam gemacht. Was mittels Schulung, Newslettern oder Onlineinformationen vonstatten geht.

Produktivitätsverlust während Awareness	=	Anzahl IT-User * Informationsdauer über IT-Sicherheit

Beispiel „KIT-S“:
Annahmen:
- Anzahl IT-User = 200
- Informationsdauer = 30 Minuten pro Jahr (0.5 h)

	Berechung in Stunden	Zeitaufwand pro Jahr	Kosten pro Jahr
Awareness	200 * 0.5	**100.00 [h]**	**14'000.- [CHF]**

Spammails:
Die Zeit, die sich der User mit Spammails herumschlägt, sollte zum Produktivitätsverlust gerechnet werden. Die Zeit pro Spammail hängt auch wieder stark vom einzelnen User ab. Wie unter Wartungen beschrieben, können die Spammails von einem Mitarbeiter aus der IT-Abteilung überprüft werden, oder es wird ein Spamzeichen im Betreff eines Spammails vom Antispamprogramm hinzugefügt, davon hängt die Verweildauer und Anzahl Spammails pro Tag ab (Biswas 2004).

Produktivitätsverlust während Spammails	=	Anzahl IT-User * Anzahl Spams pro User pro Jahr * Verweildauer pro Spam

Beispiel „KIT-S“:
Annahmen:
- Anzahl IT-User = 200
- Anzahl Spammails pro Mitarbeiter pro Tag = 15 (Spamzeichen im Betreff)
- Verweildauer = 5 Sekunde (0.001388 h)

	Berechung in Stunden	Zeitaufwand pro Jahr	Kosten pro Jahr
Spammails	200*15*225(Tage) *0.001388	**937.50 [h]**	**131'250.- [CHF]**

5.6 Kostenbeispielübersicht der fiktiven Firma „KIT-S“

Nochmals die Zahlen zu KIT-S:

Umsatz:	3'000'000'000.- [CHF]
Mitarbeiter:	200 [Anz]
Mitarbeiter in IT-Abteilung:	20 (5 IT-Sicherheit) [Anz]
IT-Budget:	10'000'000.- [CHF]
IT-Sicherheits-Budget:	nicht ausgewiesen
Arbeitsrechner:	210 [Anz]
Server:	70 [Anz]

Übersicht der Kosten für IT-Sicherheitsmassnahmen:

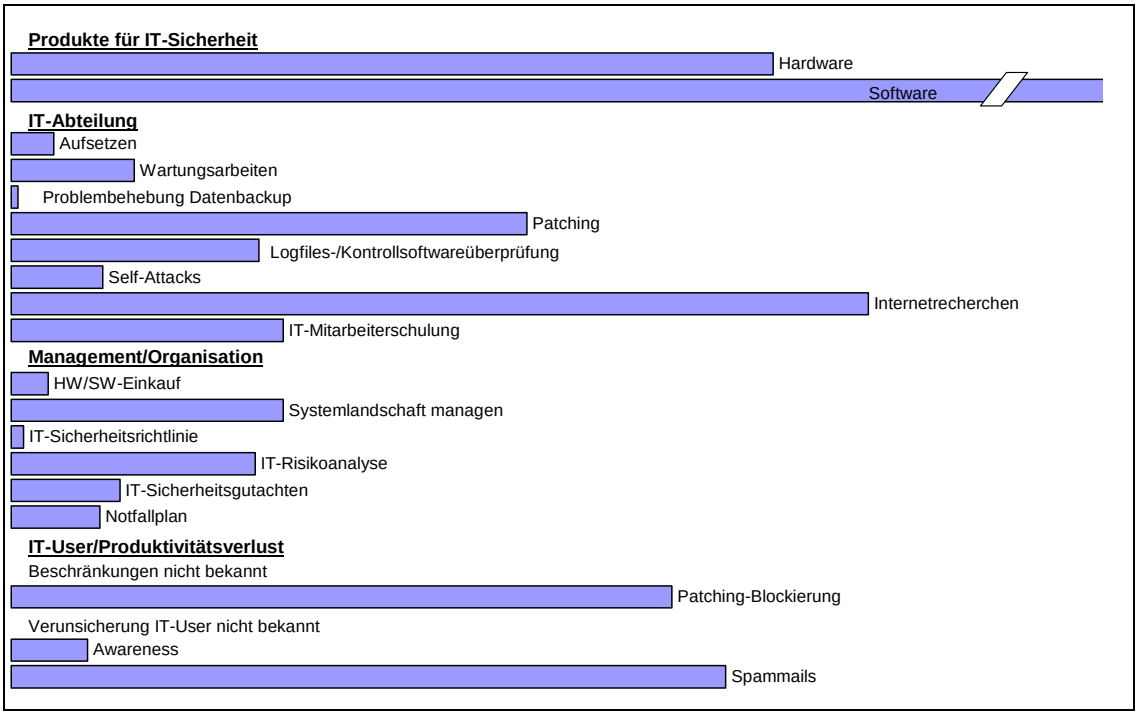

Abb. 5-2: Kostenbeispielübersicht der „KIT-S“

Absolute Kosten aus den Beispielrechnungen:

	Kosten:	Relativ zu IT-Budget
Produkte für IT-Sicherheit:	420'000.- [CHF]	4.20 %
IT-Abteilung:	396'000.- [CHF]	3.96 %
Management/Organisation	141'000.- [CHF]	1.41 %
Gesamt Zusatzkosten ohne IT-User:	**957'000.- [CHF]**	**9.57 %**
IT-User/Produktivitätsverlust:	266'000.- [CHF]	(2.66 %)
Gesamt Zusatzkosten:	**1'223'000.- [CHF]**	**(12.23 %)**

Die Kosten für die IT-sicherheitsrelevanten Produkte sind am besten ausgewiesen. Die Schwierigkeit ist aber hier, die IT-sicherheitsrelevanten Produkte von den anderen abzugrenzen, gerade wenn zum Beispiel an eine Komplettsoftware für eine Bank gedacht wird, welcher Anteil mit IT-Sicherheit zu tun hat.
Anders sieht es mit den Kosten für die Arbeitsaufwände aus. Viele Arbeiten werden gemacht, ohne dass sie speziell in einer Kostenrechnung ausgewiesen werden. Zum Beispiel Patching oder Internetrecherchen, die viel Zeit in Anspruch nehmen. Hier müssten

die Verantwortlichen über eine längere Zeit genauesten ihren Tagesablauf protokollieren, um festzustellen, wie hoch ihr Zeitaufwand für die verschiedenen Arbeiten ist.
Der Produktivitätsverlust der IT-User wird nicht ins IT-Budget genommen. Das Unternehmen muss sich aber bewusst sein, dass auch Kosten durch IT-Sicherheits-massnahmen beim IT-User entstehen können. Falls sich zum Beispiel die Firma „KIT-S“ entscheidet, das Patching-Verfahren im Hintergrund ablaufen zu lassen, so vermeidet sie einen Produktivitätsverlust von CHF 112'000.- (siehe Kapitel 5.5 Blockierung: 84'000 + 28'000).

6 Fazit

Diese Semesterarbeit untersucht, mit welchen verschiedenen Kosten- und Zeitaufwandfaktoren die Internet-Nutzer wie Grossbetriebe und KMUs für einen optimalen Schutz ihrer Firmensysteme rechnen müssen.
Es wurde ein Systemmodell erstellt, dass folgende Bereiche durchleuchtet: Produkte für IT-Sicherheit, IT-Abteilung, Management/Organisation und IT-User. In diesen Bereichen wurden die Kosten-, Zeitaufwandfaktoren sowie mögliche Produktivitätsverluste untersucht.
Es kristallisierte sich schnell heraus, dass neben den Kosten für die IT-sicherheitsrelevanten Produkte noch einige weitere ins IT-Sicherheitsbudget einfliessen sollten. So die Kosten des Mehraufwands in den IT-Abteilungen und im Management, sowie evt. auch die Kosten des Produktivitätsverlusts der IT-User, die durch die IT-Sicherheitsmassnahmen in ihrer Arbeit beeinträchtigt werden. Folgende Arbeiten sind mit grossem Zeitaufwand und hohen Kosten verbunden: Patching, Logfiles-/Kontrollsoftwareüberprüfungen, Wartungsarbeiten, Internetrecherchen (in der IT-Abteilung), Projekte wie IT-Sicherheitsgutachten, IT-Risikoanalyse oder Systemlandschaft managen (im Management) sowie der Produktivitätsverlust der IT-User durch die Patching-Blockierung ihrer Arbeitsstation oder der Ablenkung durch Spammails.

Ein einfaches Kostenmodell mit einfachen Parametern, wie zum Beispiel Anzahl Rechner oder Anzahl IT-User, konnte nicht erstellt werden. Zu gross sind die Unterschiede der Unternehmen, was ihre Grösse, und noch viel bedeutender, was ihre IT-Sicherheitsbedürfnisse angeht. Daher konnte mit einfachen Parametern keine vernünftige Berechnung gemacht werden. So wurden in den Formeln verschiedene Arbeitsaufwände aufgelistet, die für gewisse IT-Sicherheitsmassnahmen notwendig sind.
Das Problem besteht darin den Zeitaufwand für die verschiedenen Arbeiten zu evaluieren. Die Interviewpartner konnten diese Zeitangaben meistens schätzen. Jeder Mitarbeiter im Unternehmen müsste seine Arbeitsabläufe und –zeiten protokollieren, damit sich der Zeitaufwand für verschiedene Arbeiten genau bestimmen lässt. Oder, wie beim Beispiel der fiktiven Firma „KIT-S“, müssen die Unternehmen Schätzwerte annehmen und mit diesen die Formeln berechnen.

Diese Semesterarbeit soll den Unternehmen die wichtigsten Kriterien für die Berechnung der IT-Sicherheit aufzeigen. Anhand eines Berechnungsbeispiels werden die Kosten für die IT-Sicherheitsprodukte, der Zeitaufwand der IT-Abteilung und des Managements, sowie der Produktivitätsverlust bei den IT-Usern berücksichtigt. Daraus ableitend kann der ROSI (Return On Security Investment) berechnet werden.

Weitere mögliche interessante Arbeiten wären:

- Ein quantitatives Fallbeispiel, wobei eine Unternehmung mehrere Wochen beobachtet wird und ihre Arbeitsaufwände genauestens protokolliert werden.
- Ein Vergleich Outsourcing und Insourcing der IT-Sicherheitsmassnahmen. Wie fährt ein Unternehmen besser.
- Kosten-Nutzenanalyse, ROSI. Berechnungen einiger Beispiele.

7 Literaturverzeichnis

Bennett, M. (2004a)
Patchen hält das Personal auf Trab, Artikel aus IT Week 07.04.2004
http://www.vnunet.de/it/strategie/article.asp?ArticleID=20040407009

Bennett, M. (2004b)
Kosten für Ausfallzeiten: Unternehmen sind planlos, Artikel aus IT Week vom 26.04.2004
http://www.vnunet.de/it/strategie/article.asp?ArticleID=20040423008

Biswas, C. (2004)
So viele Computerviren wie noch nie, Artikel aus NZZ am Sonntag vom 02.05.2004
http://www.nzz.ch/2004/05/02/wi/page-article9KKCR.html

BITKOM (2003)
Sicherheit für Systeme und Netze in Unternehmen: Einführung in die IT-Sicherheit und Leitfaden für erste Maßnahmen, Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V., 2. überarbeitete Auflage, Berlin, 2003

BSI (1997)
Bundesamt für Sicherheit in der Informationstechnik, IT-Grundschutzhandbuch 1997: Massnahmenempfehlungen für den mittleren Schutzbedarf, BSI, Bonn 1997

BSI (2001)
Bundesamt für Sicherheit in der Informationstechnik: Leitfaden IT-Sicherheit: IT-Grundschutz kompakt, BSI, Bonn, 2001

bull.at (Internetseite)
Erstellung oder Überarbeitung eines Informations-Sicherheitskonzepts (Information Security Policy), Internetseite
http://www.bull.at/security/security-B.htm

cirosec.de (Internetseite)
Methodik von Renditeanalysen bei Experten umstritten: IT-Leiter rechnen bei Sicherheit selten nach, Internetseite
http://www.cirosec.de/pages/presse/berichterstattung/cz_28102002_02.html

Cohen, F. (1987)
Computer Viruses - Theory and Experiments, Computers & Security, Volume 6, 1987

ComputerZeitung (2003)
Spezialwerkzeuge lindern Patch-Beschwerden, Artikel aus Computer Zeitung Ausgabe 46/03 Seite 9, 2003
http://www.industrienet.de/O/125/Y/84057/VI/10062520/VS/Gora/default.aspx?O=125&Y=84057&VI=10062520&VS=GORA

DDoSVax (Internetseite)
http://www.tik.ee.ethz.ch/~ddosvax/

Dübendorfer, T., Wagner, A., Plattner, B. (2004)
An Economic Damage Model for Large-Scale Internet Attacks, 13th IEEE International Workshops on Enabling Technologies: Infrastructures for Collaborative Enterprises (WET ICE 2004); Workshop on Enterprise Security, Modena, Italy

ecin.de (1999) (Internetseite)
Monitoring per Software: Bespitzelung oder notwendige Kontrolle? Artikel vom 23.12.1999
http://www.ecin.de/sicherheit/monitoring/

ecin.de (2004) (Internetseite)
Virtuelle Private Netze: Massgeschneiderte Sicherheit, Artikel vom 05.02.2004
http://www.ecin.de/sicherheit/vpn/

educa.ch (2003) (Internetseite)
IT-Sicherheit im Bildungswesen, Gefahren / Problemfälle, Internetseite, 2003
http://www.educa.ch/dyn/9.asp?url=111426.htm

Ernst & Young (2001)
BSI Firewall Studie II, 2001
http://www.bsi.bund.de/literat/studien/firewall/fwstud01/fwstud.pdf

Ernst & Young (2003)
Global Information Security Survey 2003, IT-Security Studie von Ernst & Young, 2003
http://www.ey.com/global/download.nsf/International/TSRS_-_Global_Information_Security_Survey_2003/$file/TSRS_-_Global_Information_Security_Survey_2003.pdf

Gerbich, S. (2002a)
Blind oder blauäugig, Artikel aus Informationweek vom 12.09.2002
http://www.informationweek.de/index.php3?/studien/studie18a.htm

Gerbich, S. (2002b)
Warten auf ROSI, Artikel aus Informationweek vom 24.10.2002
http://www.informationweek.de/index.php3?/channels/channel46/022228.htm

Gerbich, S., Foley, J., v. Hulme, G. (2003)
Virenschutz: Fix it baby, Aritkel aus Informationweek vom 09.10.03
http://www.informationweek.de/index.php3?/channels/channel38/032032a.htm

Harris, S. (2002)
All in one: CISSP Certification, McGraw-Hill/Osborne, Berkeley (USA), 2002

Heindl, E., Bücking, J., Emmert, U. (2001)
Der IT-Sicherheitsexperte: Rechtliche und technische Aspekte der Internetnutzung, Addison-Wesley Verlag, München, 2001

informationweek.de (2003) (Internetseite)
Was für ein Sommer! IT-Security Studie 2003, Artikel aus Informationweek vom 11.09.2003
http://www.informationweek.de/print.php3?/channels/channel35/031814.htm

Keizer, G. (2004)
Gartner: Worms Jack Up the Total Cost of Windows, Artikel aus TechWeb News vom 05.05.2004
http://www.techweb.com/wire/story/TWB20040505S0008

Koch, H. (1998)
Netzwerksicherheit, Internetseite, 1998
http://www.computec.ch/dokumente/allgemein/netzwerksicherheit2/netzwerksicherheit.html

KPMG (2002)
Sekundärstudie: Kümmern sich Unternehmen zu wenig um ihre IT Security? Studie: ABCD: Ergebnisse aus verschiedenen IT-Sicherheitsstudien (KPMG), 2002
http://www.itk-trends.de/0232_02.htm

Kyas, O., a Campo, M. (2002)
IT-Crackdown: Sicherheit im Internet, mitp-Verlag, 2. Auflage, Bonn, 2002

Lang, F. (2003)
Sind Sie sicher? Ein Gesetz macht IT-Sicherheit zur Pflicht, IT-Security Consulting GmbH, München, 2003
http://www.fjlang.de/downloads/beratung/management/Ein%20Gesetz%20macht%20die%20IT.pdf

Microsoft (2003)
Microsoft-Leitfaden zur Sicherheitspatch-Verwaltung, Microsoft Corporation, 2003
http://download.microsoft.com/download/0/c/6/0c68401c-f74d-4b23-ad5c-de22c29e8dbd/Sonstige/secpatch.pdf

Müller, S. / Köhler, C. 2001
Frauenhofer Anwendungszentrum: Angriffsmöglichkeiten auf Netzwerke und Unternehmensdaten, 2001
http://www.computec.ch/dokumente/allgemein/angriffsmoeglichkeiten_auf_netzwerke/angriffsmoeglichkeiten_auf_netzwerke.pdf

Morris, G. S. (Internetseite)
Computer Security and the Law, Internetseite
http://csrc.nist.gov/publications/secpubs/cslaw.txt

Nolting, H. (1978)
Lernfall Aggression, Rowolth Taschenbuch Verlag, 1978

Peterson, L. L., Davie, B. S. (2000)
Computernetze: Ein modernes Lehrbuch, dpunkt.verlag, 1. Auflage, Heidelberg, 2000

Pohl, H. (2003)
Stiefkind IT-Sicherheit?, Interview aus SAP INFO vom 01.03.2004
http://www.sap.info/index.php4?ACTION=noframe&url=http://www.sap.info/public/de/article.php4/Article-13616403f7766c65b1/de

Pohlmann, N., Blumberg, H. (2004)
Der IT-Sicherheitsleitfaden: Das Pflichtenheft zur Implementierung von IT-Sicherheitsstandards im Unternehmen, mitp-Verlag, Bonn, 2004

Sadowsky, G. (2004)
Information Technology Security Handbook, Internetseite, 2004
http://www.infodev-security.net/handbook/

Schaumann, P. (2004)
Spam und Computerkriminalität, Internetseite
http://philipps-welt.info/spam.htm#spam

Schmid, J., Weigel, P. (2003)
Semesterarbeit: Wirtschaftliche Auswirkungen von DDoS Attacken auf Backbone-Provider, ETH Zürich, 2003

Sikora, A. (2003)
Security im Überblick, tecchanel.de (ausgedruckte Version), 2003

Stalling, W. (2000)
Network Security Essentials: Applications and Standards, Prentice-Hall, New Jersey, 2000

sys2.de (2003) (Internetseite)
Wartung einer Firewall, Interseite, 2003
http://www.sys2.de/mod.php?mod=webpage&op=view&wid=8&PHPSESSID=183d0dff31026c6e5e14ccf341542a80

Szallies, D., Längsfeld, C. (2001)
Seminararbeit: Netzwerksicherheit, Technische Universität Darmstadt, 2001

8 Anhang

8.1 Interview-Fragenkatalog über Sicherheit bei Internetbenutzung

Durch die Internetbenutzung der Unternehmen entstehen neue Aufgaben, die die IT-Abteilungen zusätzlich erledigen müssen. Da die Systeme dauernd online sind, sind sie ständigen Attacken aus dem Internet ausgesetzt. Ausserdem interessieren bei dieser Semesterarbeit besonders die versteckten Arbeitsaufwände und Kosten, um die Systeme zu sichern.

1. Wie hoch betrachten Sie folgende Attacken aus dem Internet?

	sehr niedrig	niedrig	mittel	hoch	sehr hoch
Viren	☐	☐	☐	☐	☐
Tojaner	☐	☐	☐	☐	☐
Würmer	☐	☐	☐	☐	☐
Hackerangriffe	☐	☐	☐	☐	☐
Passwort Cracking	☐	☐	☐	☐	☐
DoS/DDoS Attacken	☐	☐	☐	☐	☐
Email fälschen	☐	☐	☐	☐	☐
Sind Ihnen noch weitere Attacken aus dem Internet bekannt?					
……...	☐	☐	☐	☐	☐
……...	☐	☐	☐	☐	☐
……...	☐	☐	☐	☐	☐

2. Wie hoch schätzen Sie die Notwendigkeit folgender Schutzmassnahmen ein?

	sehr niedrig	niedrig	mittel	hoch	sehr hoch
Antivirensoftware	☐	☐	☐	☐	☐
Firewalls	☐	☐	☐	☐	☐
IDS (Intrusion Detection S.)	☐	☐	☐	☐	☐
Monitoring, Auditing, Reporting Tools	☐	☐	☐	☐	☐
VPN Virtual Private Network	☐	☐	☐	☐	☐
Automatisches Daten-Backup	☐	☐	☐	☐	☐
Mitarbeiter Schulung	☐	☐	☐	☐	☐
Würden Sie noch weitere wichtige Schutzmassnahmen vorschlagen?					
……...	☐	☐	☐	☐	☐
……...	☐	☐	☐	☐	☐
……...	☐	☐	☐	☐	☐

3. Ein Antivirusprogramm ist immer nur so gut, wie seine Virenmusterdatenbank. Wie sehen Sie es, um die Virusdefinitionen aktuell zu halten? Zeitaufwand für Updates? User selbst dafür zuständig? Zentral? Täglich? Wöchentlich?

4. Wie oft sollte eine Firewall gewartet werden? Geschätzter Arbeitsaufwand pro Monat? Ungefährer Arbeits- und Kostenaufwand für die Instandsetzung von einer Firewall.

5. Näheres über Monitoring, Auditing und Reporting Tools? Arbeitsaufwand mit diesen Tools?

6. Intrusion Detection Systems? Wie arbeitsintensiv?

7. Daten Backup? Mehr seit Internetnutzung? Wie oft? Automatisch? Können Viren übernommen werden?

8. Allgemeine Verwaltung von Sicherheitssysteme, Zeitaufwand?

9. Sich selbst attackieren, um Schwachstellen herauszufinden. Soll das durchgeführt werden? Wer sollte das durchführen?

10. Welche Personen sind für die IT-Sicherheit bei Internetbenutzung zuständig? Wie viel wird auf die User abgewälzt?

11. Sehen Sie noch weitere Punkte, die durch die Internetbenutzung auf ein Unternehmen zukommen?

12. Gibt es sonstige versteckte Kosten, die auf den ersten Blick nicht ersichtlich sind?

8.2 Interviews betreffend Sicherheit bei Internetbenutzung

Für diese Interviews wurde ein kurzer Fragenkatalog erstellt und den Interviewpartnern zugesandt. Dieser Fragenkatalog gab dem Interview eine lose Struktur, von der aber auch oft gewollt abgewichen wurde. Anhand dieses Fragenkatalogs konnten sich die Interviewpartner vorbereiten und um Gespräch diente er als Leitfaden.

Hiermit möchte ich auch gleich meinen Interviewpartnern danken, dass sie mir ihre wertvolle Zeit geopfert haben und mir Rede und Antwort standen. Es waren sehr interessante Gespräche.

Inhalte der Interviews in Stichworten.

Interview mit Stefan Lampart, Open Systems AG, am 21.04.04
Interview mit Urs Meile, ETH Zürich, am 22.04.04

- Zwei Betrachtungsweisen der Attacken, die Gefahr und die Wahrscheinlichkeit
- Zu den genannten Gefahren wurden noch folgende hinzugefügt: Spyware (Trojaner), Fishing (Emailbekanntgabe), Browser Hack (Hackerangriff via Browser)
- Frühere Hackerangriffe vermehrt von professionellen Hackern, die dann auch mehr Firmen und Organisationen mit grosser Bekanntheit gehackt haben. Heute gibt es viele „Script-Kiddis Attacken“, das heisst, dass im Internet Scripts vorhanden sind, die einfach zu bedienen sind und mit denen ein Hackerangriff unternommen werden kann. Bei diesen Hacks werden auch KMU vermehrt angegriffen.
- Zu den aufgelisteten Schutzmassnahmen wurden noch folgende genannt: Worse Proxy (Testumgebung zum Testen), Verschlüsselungen von Emails, Secure Emails, PKI, Anti Spam Software, PATCHEN
- Gerade das Patchen wird als das Wichtigste angesehen, da die Lücken bei ungepatchten Systemen am meisten für Angriffe genutzt werden
- Policy für User, dass sie nur mit aktuell gepatchten Rechnern ins Internet gehen
- In jedem Fall Benachrichtigung, falls neue Patchs vorhanden sind
- Ganz wichtig, dass die Server sofort bei einem neuen Patch upgedated werden.
- Patchroutinen einführen, automatisches Patchen, User muss nur noch bestätigen, Admin geht persönlich vorbei (sehr aufwändig)
- Das Patchen wird am zeitintensivsten betrachtet.
- Emergency Management, Notfallszenario. Was passiert, wenn ein System ausfällt? Bei ETH im Aufbau.
- Mit Redundanz der Systeme kann schnell bei einem Notfall eingegriffen werden, ist aber sehr teuer, es braucht zwei Systeme dafür (Hotstandby)
- Bei Systemprogramminstallationen wie auch beim Patchen sollte erst die Vertraulichkeit getestet werden. Ist plötzlich ein wichtiger Service nicht mehr erreichbar? Das beinhaltet aber, dass man eine Testumgebung hat, die dem Original entspricht, mindestens ansatzweise → teuer.
- Neue Programme verlangen vielleicht nach neuen Ports, die noch von der Firewall blockiert werden, nicht einfach öffnen, sondern abwägen. → Leider kommt aber Funktionalität oft vor Sicherheit.
- IDS, Monitoring, Logfiles müssen reportiert und kommuniziert werden, eher aufwändig

- Hohe Selbstausbildung verlangt. Virenaktualität, Know How. → können sich KMUs Experten leisten. Reicht einer? Stellvertreterproblematik, wenn nur einer Zugang hat und Systeme kennt.
- Laptop ans Firmennetzwerk anschliessen ist ein grosses Problem. Laptop könnte z.B. Viren enthalten. Varianten: Virenscan immer am Anfang durchführen sowie System überprüfen, ob alle neue Patchs installiert wurden (mittels Distributionserver), oder Policy einführen, was den Laptopbenutzern einige Anwendungen im Heimgebrauch verbietet (Durchführbarkeit?)
- Server und Arbeitsrechner sollten täglich mit evt. neuen Patchs und Virendefinitionen versehen werden
- Benutzungen einschränken, dass nicht jeder alles machen kann. Gefahren vorbeugen.
- User auf Patchs aufmerksam machen
- Sehr wichtig: Technologische System Integrität → Patching
- Eigene Überprüfung auf Verletzlichkeit, Selfattack
- Awareness bei den Mitarbeitern selten

8.3 Fragenkatalog für die Errechnung von IT-Sicherheits-massnahmen durch Internetbenutzung

Durch die Internetbenutzung der Unternehmen entstehen neue Aufgaben, die die IT-Abteilungen zusätzlich erledigen müssen. Da die Systeme dauernd online sind, sind sie ständigen Attacken aus dem Internet ausgesetzt. Ausserdem interessieren bei dieser Semesterarbeit besonders die versteckten Arbeitsaufwände und Kosten, um die Systeme zu sichern. Dieses Interview hat zum Ziel, Bereiche mit versteckten IT-Sicherheits-Kosten aufzuzeigen und diese grob abzuschätzen. Dieser Fragenkatalog soll Ihnen als Informationsbasis dienen, damit Sie wissen, was für Fragen auf Sie zukommen. Die Fragen werden dann beim Interview noch genauer erläutert.
Ihre Angaben werden vertraulich behandelt. Darauf basierende Veröffentlichungen werden nur Prozentzahlen und konsolidierte Zahlen aller befragten Unternehmen enthalten und werden keine Rückschlüsse auf Ihre hier genannten Zahlen ermöglichen.

Alle Angaben betreffen das Jahr 2003. Beträge in CHF. Falls genaue Angaben nicht machbar sind, bitte nennen Sie Schätzwert.

A. Allgemeine Angaben.	
Firma: ……..……...……	
Name: ……..……...……	
- Funktion: ……..……....	
- Kontakt für Rückfragen (Email, Tel.): ……..……..	
- Tätigkeitsgebiet des Interviewten (in Stichworten): ……	
…….	
…….	
Anzahl Mitarbeiter in der IT-Abteilung 2003:	…….
Anzahl Mitarbeiter in der IT-Abteilung 1998:	…….
Ungefähre Höhe des IT-Budget 2003:	…….
Ungefähre Höhe des IT-Budget 1998:	…….
Ausgaben 2003 für IT-Sicherheit in Prozent zum IT-Budget 2003:	…….
Ausgaben 1998 für IT-Sicherheit in Prozent zum IT-Budget 1998:	…….
Erklärung des Unterschieds (wegen grösserer IT-Infrastruktur, IT-Sicherheit?): …….	
…….	
…….	
Durchschnittlicher Stundenlohn eines IT-Mitarbeiter:	…….
Durchschnittlicher Stundenlohn eines IT-Users:	…….

B. Angaben zum Verantwortlichkeitsbereich.	
Anzahl Mitarbeiter im Verantwortlichkeitsbereich:	…….
- davon IT-User mit Internet-, Intranetanschluss (in Prozent):	…….
Vorhandene Beschränkungen des Internet Zugangs für die IT User (z.B. kein P2P, Freemail):	
…….	
…….	
…….	
Anzahl zu betreuende Arbeitsplätze mit PCs und Workstations:	…….
Anzahl zu betreuende Laptops und Handhelds:	…….
Anzahl zu betreuende Server:	…….

C. Kosten der Produkte für die IT-Sicherheit.	
Jährliche Ausgaben für die IT-Hardware (jährliche Abschreibungen):	……
- davon für IT-sicherheitsrelevante Systeme (spezielle Router, Firewall etc) in Prozent:	……
- davon für redundante System in Prozent:	……
Jährliche Ausgaben für Software und Lizenzen:	……
- davon für IT-Sicherheitssoftware (Antiviren-, Antispamprogramme, Monitoring-SW, Auditing-SW, IDS etc.) in Prozent:	……

D. Arbeitsaufwand der IT-Abteilung für die IT-Sicherheit. Alle Fragen beziehen sich auf IT-sicherheitsrelevante Systeme (Angaben in Mannstunden pro Woche oder Prozent der gesamten Arbeit)	
Aufsetzen der Systeme, Neuinstallationen inkl. Testen:	……
Vermehrte Datenbackups:	……
Wartung Firewall:	……
Wartung Virenschutz:	……
Wartung Spamschutz Firmen-Emails:	……
Patching, technische Systemintegrität gewährleisten:	……
- Intervall (diskontinuierlich, täglich, wöchentlich ..):	……
- Informationsbeschaffung, Patchsuche (Internetrecherchen, Newsletter durchlesen, Selbstschulung etc.):	……
- Patch-Pakete zusammenstellen:	……
- Patch testen:	……
- Patch aufspielen bei Server:	……
- Patch aufspielen bei Workstations:	……
- Überzeit bei Extremfall (Bsp: Freitagabend neuer wichtiger Patch):	……
Self-Attacks durchführen:	……
Logfiles überprüfen:	……
Reagieren auf Falschalarme:	……
Reporte erstellen:	……
Internet-Userzugänge kontrollieren und beschränken:	……
Selbststudium, Internetrecherchen	……
IT-Mitarbeiterschulung:	……
Webseite schützen:	……
Shopping-Systeme	……
Bitte weitere grosse Arbeitsaufwände nennen: ……...……...	
……	
……	
……	

E. Management und Organisation. (Kosten pro Jahr, Fragen auch wieder auf IT-Sicherheit)	
Sicherheitspolicy erstellen/aktualisieren:	……
Policy-Einhaltung überprüfen:	……
Risiko-, Schadensanalyse betreffend Lücken in der IT-Sicherheit:	……
Kosten für externe Sicherheitsgutachten (inkl. Penetration Testing)	……
Notfallplan erarbeiten, testen (durchspielen), aktualisieren:	……

F. Produktivitätsverlust bei den IT-Users. (Stunden pro Woche)	
Blockierung der Rechner bei Patching:	…….
Informationsmails betreffend IT-Sicherheit durchlesen:	…….
Verunsicherungen durch IT-Sicherheitsinformationen → Hotline anrufen:	…….
Produktivitätsverlust durch Funktionseinbussen (umständlichem Arbeiten wegen der IT-Sicherheit):	…….
Schulungen, Awareness:	…….
Anzahl Spam- und Virenmails pro Woche:	…….
Sehen Sie noch weitere Gründe für Produktivitätsverlust: ……...…….	
…….	
…….	
…….	

G. Nennen Sie Tätigkeitsbereiche bzw. Tätigkeiten, die seit dem Anschluss der Firma ans Internet stark im Aufwand und Umfang gewachsen sind.
…….
…….
…….
…….

H. Sehe Sie noch weitere versteckte Kosten.
…….
…….
…….
…….

I. Schaden, Beispiel Virenbefall	
Anzahl Virenbefälle im 2003, wo Systeme gesäubert oder neu installiert werden mussten:	…….
Ungefähre Anzahl PC/Server, die durchschnittlich befallen werden:	…….
Durchschnittliche Mannstunden, um einen Virenbefall zu beheben:	…….
Durchschnittlicher Zeitraum, an dem PC/Server nicht zur Verfügung stehen:	…….
Durchschnittliche Umsatzeinbussen:	…….
Durchschnittliche Schaden (Daten-, Informations-, Wissensverlust):	…….
Weitere Angaben: ……...……...	
…….	
…….	
…….	

Vielen Dank für Ihre Mithilfe !

8.4 Abbildungsverzeichnis