Wirtschaftlichkeitsbetrachtung von IT-Sicherheitsmechanismen

Prof. Dr. Norbert Pohlmann

Fachhochschule Gelsenkirchen

Fachbereich Informatik

Neidenburger Straße 43

45877 Gelsenkirchen

norbert.pohlmann@informatik.fh-gelsenkirchen.de

Zusammenfassung

IT-Schutzmaßnahmen sind kein Selbstzweck. Mit Hilfe von IT-Schutzmaßnahmen kann das Risiko bei der Nutzung von IT-System reduziert werden. In diesem Artikel werden die Kosten der IT-Schutzmaßnahmen aus unterschiedlichen Blickwinkeln betrachtet. Da eine IT-Schutzmaßnahme eine Investition für die Zukunft ist, sollten die Kosten-Nutzen-Aspekte schon bei der Planung besonders berücksichtigt werden.

1 Einführung

Die Aufgabe von IT-Systemen ist es, die Geschäftsprozesse zu verbessern und dadurch Kosten zu reduzieren oder den Umsatz zu steigern und letztlich mehr Profit zur erzielen. Alles dient dem Zweck der Bestandssicherung und Gewinnmaximierung.

Dies kann erreicht werden, indem die Aufgaben

- vereinfacht oder beschleunigt (z.B. E-Mail als Kommunikationsmittel),
- Abläufe störungsfreier oder flexibler gestaltet (z.B. keine Medienbruch, Verwendung von mobilen Geräten - arbeiten von zu Hause oder von unterwegs),
- Mitarbeiter von Routineaufgaben entlastet (z.B. kein Medienbruch, EDV – System für die Verwaltung, nicht immer alles neue mit Excel),
- Mitarbeiter bei komplexen Aufgaben unterstützt werden (z.B. CAD – Systeme, Statische Berechnungen) und
- die globale wirtschaftliche Ausdehnung einfach ermöglicht wird (z.B. die Nutzung des Internets oder Angebote über Web International verfügbar machen oder E-Mail als Kommunikationsmedium nutzen oder Videokonferenz nutzen, um mit internationalen Geschäftspartnern Absprachen zu treffen).

Das Ziel einer geschäftlichen Tätigkeit ist in diesem Sinne, dass IT-Systeme wirtschaftlich sein müssen!.

Dies kann durch unterschiedliche Prinzipien erreicht werden:

- **Minimax-Prinzip**
  Bei gleichbleibendem Output (Umsatz), den Input (Kosten) minimieren
  (Kostenorientierung)
  - Durch weniger Kosten wird mehr Profit erzielt.

- **Maximin-Prinzip**
  Bei gleichbleibendem Input (Kosten), den Output (Umsatz) maximieren
  (Produktivitäts- und Umsatzorientierung)
  - Durch mehr Umsatz bei gleichen Kosten wird mehr Profit erzielt.
- **Optimax-Prinzip**
  Gleichzeitige Minimierung des Inputs (Kosten) und Maximierung des Outputs (Umsatz).
  - Kosten reduzieren bei gleichzeitiger Umsatzsteigerung ist der Traum jedes Unternehmensleiters und steigert den Profit.

Diese Prinzipien haben nichts mit IT-Sicherheit zu tun, sie stellen wirtschaftliche Ziele einer unternehmerischen Tätigkeit da. Dabei kann die Bewertung der Wirtschaftlichkeit nach den folgenden Aspekten durchgeführt werden:

- **Nach Kostenaspekten:**
  - Total Cost of Ownership
    - Kosten für Anschaffung, Schulung, Installation, Betrieb, Wartung und Ersatz von IT-Systemen und IT-Sicherhietsmaßnahmen
    - Entspricht der Kapitalwert-Methode
      (Was kostet ein Investment in der Summe aller Aspekte, die berücksichtigt werden müssen?)

- **Nach Nutzenaspekten:**
  - ROI = Return on Investments
  - Nutzen den Kosten gegenübergestellt
    (Was nützt ein Investment bezüglich Kostenminimierung und/oder Umsatzsteigerung, wann hat sich eine Investition amortisiert, d.h. die Anschaffungskosten für eine Investition werden durch den mit der Investition erwirtschafteten Ertrag gedeckt? Je schneller eine Deckung erzielt wird, um so schneller kann ein Gewinn, z.B. durch das Investment von IT-Sicherheitsmaßnahmen, generiert werden.)

Die Bedrohungen sind für alle Organisationen und Unternehmen gleich. Der Unterschied liegt in der Verwundbarkeit, wenn ein Schaden auftritt. Durch die oft geringen finanziellen Reserven und Möglichkeiten Geld zu beschaffen, ist die Verwundbarkeit bei klein- und mittelständischen Unternehmen (KMUs) oft ungleich höher als bei sehr großen Unternehmen. Die größte Gefahr für den Mittelstand ist das fehlende Bewusstsein für die Notwendigkeit der IT-Sicherheit. Aber gerade die vielen geschäftsführenden Gesellschafter, deren Existenz unmittelbar mit dem Geschäftserfolg verknüpft ist, sollten hier wachsam sein. Von daher gilt gerade im Mittelstand: IT-Security ist Chefsache!

Nach einer Information Week Studie von 10/2002 basieren 82 % der IT-Entscheidungen auf einer ROI-Analyse. In wirtschaftlich schlechten Zeiten, wird nur investiert, wenn für Investment ein Nachweis erbracht werden kann, der aufzeigt, dass dadurch schnell ein höherer Profit erzielt werden kann. Das Problem bei der IT-Sicherheit ist, dass dieser Nachweis sehr schwierig ist. Das Thema IT-Sicherheit ist immer noch neu für viele Unternehmen und besonders für viele Chefetagen.

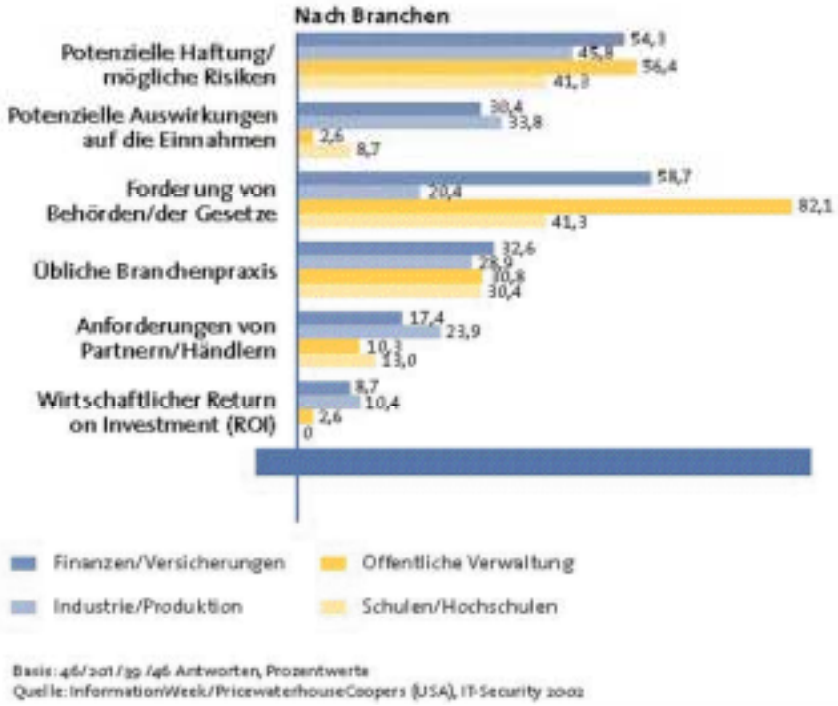

Abb. 1: Gründe für das Investment in IT-Sicherheit in Deutschland (Information Week)

Die Grafik zeigt deutlich, dass in Deutschland die Gründe für ein IT-Sicherheitsinvestment hauptsächlich durch die Forderung von Behörden und Gesetzen und die Angst vor Haftung begründet werden. Eine Return-on-Investment-Berechnung nach wirtschaftlichen Gesichtspunkten wird eher selten durchgeführt.

2 IT-Sicherheitsrisiken und -investment

Ein besondere Aspekt, der bei dem IT-Investment betrachtet werden muss, ist, dass die Risikominimierung nicht linear mit dem Investment steigt.

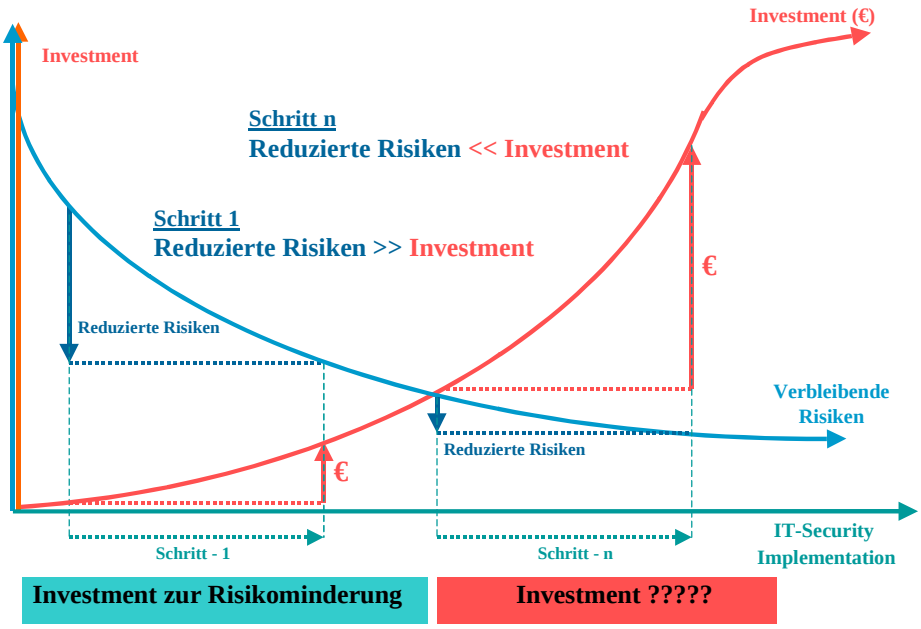

Abb. 2: IT-Sicherheitsrisiken und -investment

Die Graphik zeigt, dass in einem ersten Schritt mit einem kleinen Investment eine große Risikominimierung erzielt werden kann (Reduzierte Risiken >> Investment). Wird aber weiter investiert, dreht sich

das Verhältnis. Mit einem hohen Investment in weiteren Schritten kann nur noch eine kleine Risikominimierung erreicht werden (Reduzierte Risiken << Investment).
Aus dieser Betrachtung können zwei Schlüsse gezogen werden:

1. Das Pareto-Prinzip (80/20-Regel) gilt auch für die IT-Sicherheit

- Mit 20% der möglichen IT-Sicherheitsmaßnahmen richtig eingesetzt, kann 80% Schutz vor potentiellen Bedrohungen erreicht werden.
- Das bedeutet, dass mit dem Einsatz der richtigen IT-Sicherheitsmaßnahmen durch einen relativ geringen Aufwand, ein vernünftiger Grundschutz für IT-Systeme hergestellt werden kann.

2. Wenn ein Grundschutz bereits implementiert ist, wird notwendiges weiteres Investment in Sicherheit sehr groß und ist "wirtschaftlich" nicht mehr sinnvoll.

- Es kann aber andere Gründe, außer der Wirtschaftlichkeit, geben, das Investment dennoch durchzuführen. Diese sind z.B.
  - gesetzliche Notwendigkeiten
  - im militärischen Bereich, zum Schutz der Gesellschaft
  - Schutz von Leib und Leben
  - Angst
  - übertriebenes Sicherheitsgefühl

3 Total Cost of Ownership - Kostenaspekte

Im Folgenden soll anhand des Beispiels des Investment in ein Firewall-System abgeschätzt werden, wie groß der Aufwand ist, ein Firewall-System anzuschaffen und zu betreiben.

Der Aufwand für ein Firewall-System kann unter dem Gesichtspunkt des Gesamtaufwandes in drei Phasen unterteilt werden.

- Beschaffungsphase eines Firewall-Systems
- Installationsphase eines Firewall-Systems
- Aufrechterhaltung des Betriebs eines Firewall-Systems

Die Aufwendungen, die in diesem Abschnitt benannt werden, sind reale Aufwendungen, die unabhängig vom jeweiligen Zeitpunkt erbracht werden müssen. Aufwand wird auf Tage gerundet, wobei davon ausgegangen wird, dass sechs Stunden Aufwand einen Arbeitstag ausmachen. Bei den angegebenen Aufwendungen wird davon ausgegangen, dass über das Firewall-System potenziell 1000 Mitarbeiter der Organisation kommunizieren dürfen.

Die Personalkosten werden mit EUR 750,- pro Tag veranschlagt. Falls die angegebenen Leistungen von Fachfirmen durchgeführt werden, muss wahrscheinlich mit einem höheren Kostenbetrag gerechnet werden.

3.1 Beschaffungsphase

In der Beschaffungsphase muss von der Organisation eine Firewall-Sicherheitspolitik festgelegt werden, die als Grundlage für den Betrieb des Firewall-Systems dient. Hier ist besonders wichtig, den Schutzbedarf des zu schützenden Netzes mit den Rechnersystemen zu analysieren, damit eine richtige Sicherheitsanforderung festgelegt werden kann.

Mit den definierten Randbedingungen der Sicherheitspolitik der Organisation kann dann die Produktauswahl eines Firewall-Systems beginnen, z. B. durch Einholen von Angeboten, Testinstallationen, Referenzbewertung etc. Dabei muss im Vorfeld festgelegt werden, nach welchen Kriterien ein Produkt bewertet werden soll.

Wichtig in dieser Phase ist, dass auch infrastrukturelle, personelle und organisatorische Sicherheitsmaßnahmen vorbereitet werden, damit die nächste Phase eingeleitet werden kann.

Aufwand für die Beschaffungsphase

Falls die Organisation noch keine generelle Sicherheitspolitik erarbeitet hat und diese im Rahmen der Firewall-Beschaffung erstellt werden muss, ist der Aufwand in der Beschaffungsphase zu berücksichtigen. Die Erstellung einer Sicherheitspolitik kann je nach Größe der Organisation und je nach Schutzbedarf zwischen zwei Wochen und drei Monaten liegen.

Für die Auswahl eines Firewall-Produktes ist der Aufwand abhängig vom Produktauswahlverfahren sehr unterschiedlich, je nachdem, ob z. B. nur mithilfe von Prospekten ausgewählt wird oder Testinstallationen mehrerer Firewall-Systeme mit Aufbau eines Testsystems stattfinden sollen. Der Aufwand liegt in der Regel zwischen zwei Wochen und drei Monaten.
Die Definition und Vorbereitung der infrastrukturellen, personellen und organisatorischen Sicherheitsmaßnahmen kann zwischen einer Woche und vier Wochen liegen.
Die Anschaffungskosten für ein Firewall-Produkt liegen zwischen 5 000 EUR und 75 000 EUR, abhängig vom Maß an Sicherheit/Vertrauenswürdigkeit, das es erbringen kann, und seiner Leistungsfähigkeit.

Installationsphase eines Firewall-Systems

In der Installationsphase gliedern sich die Aufwendungen für ein Firewall-System in mehrere Unterpunkte.

- Installation des Firewall-Systems: Diese Phase umfasst alle infrastrukturellen Sicherheitsmaßnahmen, die zum sicheren Betrieb eines Firewall-Systems notwendig sind.
- Inbetriebnahme des Firewall-Systems: In dieser Phase ist es sinnvoll, entsprechend den Vorgaben der Sicherheitspolitik Benutzerprofile für bestimmte Mitarbeitergruppen zu definieren, damit die Eingaben des Regelwerkes später mithilfe dieser Benutzerprofile schneller erfolgen können. Nach Formulierung dieser Profile werden die Benutzer, die über das Firewall-System kommunizieren dürfen, mit ihren Rechten in das Security Management eingetragen.
- Sonstige Sicherheitsmaßnahmen: In der Installationsphase ist es wichtig, dass weitere Sicherheitsmaßnahmen wie z. B. die Schulung der Benutzer durchgeführt werden, damit diese den richtigen Umgang mit dem Firewall-System lernen und dadurch unnötige Schwierigkeiten beim Betrieb vermieden werden, Organisationsanweisungen schreiben, usw..

Die folgenden Tabellen sollen zeigen, welche zeitlichen und finanziellen Aufwendungen für die Beschaffungs- und Installationsphase einzuplanen sind.

Beschaffungsphase	Zeitaufwand	Minimale Kosten	maximale Kosten
Sicherheitspolitik	zwei Wochen bis drei Monate	EUR 7 500	EUR 45 000
Auswahl eines - Produktes	zwei Wochen bis drei Monate	EUR 7 500	EUR 45 000
weitere Sicherheitsmaßnahmen	eine bis vier Wochen	EUR 3 750	EUR 15 000
Produktkosten		EUR 5 000	EUR 75 000

Tabelle1:Aufwand und Kosten für die Beschaffungsphase

Installationsphase	Zeitaufwand	Minimale Kosten	maximale Kosten
Installation des - Firewall-Systems	2 bis 5 Tage	EUR 1 500	EUR 3 750
Inbetriebnahme des Firewall-Systems	3 bis 10 Tage	EUR 2 250	EUR 7 500
Sonstige Sicherheitsmaßnahmen	3 Wochen bis 3 Monate	EUR 11 250	EUR 45 000

Tabelle 2:Aufwand und Kosten während der Installationsphase

Anschaffungskosten	Minimale Kosten	maximale Kosten
Summe	EUR 38 750	EUR 236 250

Tabelle 3:Kosten der Beschaffungsphase und Installationsphase

3.2 Aufrechterhaltung des Betriebs

Der Aufwand für die Aufrechterhaltung des Firewall-Systems kann unter verschiedenen Gesichtspunkten betrachtet werden.

Rechteverwaltung

Ein Firewall-System ist prinzipiell so aufgebaut, dass es nach Eintrag sämtlicher Rechte vollkommen selbstständig und ohne aktive Eingriffe eines Administrators betrieben werden kann.

Aus unterschiedlichen Gründen kann jedoch ein personeller Eingriff notwendig werden, und zwar zur Einrichtung neuer Mitarbeiter bzw. zur Änderung der Rechte schon eingetragener Mitarbeiter. Je nach Anzahl und Änderungen der definierten Benutzerprofile ergibt sich ein sehr unterschiedlicher personeller Aufwand des Administrators für diese Aufgaben.

Rechenbeispiel: Für die Eintragung eines neuen Mitarbeiters oder für die Veränderung der Rechte eines schon eingetragenen Mitarbeiters benötigt der Administrator im Schnitt zehn Minuten. Die Veränderung der Mitarbeiterzahl in einer Organisation, die über das Firewall-System kommunizieren darf, wird in unserem Beispiel mit 5 % im Monat veranschlagt.

Das bedeutet bei 1000 Mitarbeitern, die potenziell über das Firewall-System kommunizieren dürfen, dass 50 Veränderungen im Monat stattfinden, d. h., für die Rechteverwaltung ist ein Zeitaufwand von 500 Minuten im Monat, also ca. neun Stunden im Monat bzw. 18 Tage im Jahr notwendig.

Analyse der Logbuchdaten

Für die Analyse der Logbuchdaten, die vom Firewall-System generiert werden, ist ein Aufwand für den Administrator einzukalkulieren. Auch hier kann der personelle Aufwand sehr unterschiedlich ausfallen. Bei Firewall-Systemen, die eine automatische Vorauswertung durchführen, ist der Zeitaufwand für den Administrator weitaus geringer als bei Firewall-Systemen, bei denen der Administrator die Logbuchdaten selbst auswerten muss.

Rechenbeispiel: Für die Analyse der Logbuchdaten werden in der Woche drei Stunden veranschlagt. Dies bedeutet einen Aufwand von zwei Tagen im Monat bzw. 24 Tagen im Jahr.

Einrichtung neuer Dienste

Da die TCP/IP-Technologie einer starken Dynamik und permanenten Veränderung unterworfen ist, muss davon ausgegangen werden, dass das Firewall-System im Abstand von drei bis sechs Monaten ein Update durchführen muss, um den neuen Anforderungen gerecht zu werden. Diese Updates erfordern ebenfalls einen bestimmten Zeitaufwand, da sie getestet werden müssen, um garantieren zu können, dass der Betrieb des Firewall-Systems weiterhin gesichert möglich ist.

Rechenbeispiel: Für diese Arbeit müssen pro Update zwei Tage vorgesehen werden, das bedeutet im Schnitt sechs Tage im Jahr.

Genereller administrativer Aufwand für das Firewall-System

Für den sicheren Betrieb des Firewall-Systems müssen Backups des aktuellen Regelwerks und der Logbuchdaten, Löschen der Protokolldaten auf dem Security Management etc. durchgeführt werden.

Rechenbeispiele: Für diese generellen Arbeiten muss ein Aufwand von drei Stunden pro Woche d. h., zwei Tagen im Monat bzw. 24 Tagen im Jahr, berücksichtigt werden.

Auswertung der Logbuchdaten auf dem Security Management

Da das Security Management eines Firewall-Systems sehr sicherheitskritisch ist, muss ein Revisor in regelmäßigen Abständen alle Aktionen der Administratoren des Management Systems mithilfe der Logbuchdaten im Security Management überprüfen.

Rechenbeispiel: Für diese Arbeit sollen drei Stunden im Monat berücksichtigt werden, d. h. sechs Tage im Jahr.

Sicherer Betrieb eines Firewall-Systems

Damit mithilfe eines Firewall-Systems ein effektiver Schutz für die Kommunikation zwischen dem unsicheren Netz und dem zu schützenden Netz gewährleistet werden kann, müssen die folgenden Bedingungen erfüllt werden:

- Das Firewall-Konzept muss in das IT-Konzept der Organisation eingebunden werden.
- Der Betrieb des Firewall-Systems muss auf eine umfassende Sicherheitspolitik aufbauen.
- Das Firewall-System muss korrekt installiert sein.
- Das Firewall-System muss korrekt administriert werden.

Aus diesem Grund ist eine regelmäßige Überprüfung der umgesetzten Sicherheitsmaßnahmen notwendig. Hierbei soll festgestellt werden, ob die unterschiedlichen Sicherheitsmaßnahmen richtig eingehalten werden.
Diese Überprüfung muss alle Sicherheitsmaßnahmen einschließen, die für den sicheren Betrieb des Firewall-Systems verantwortlich sind.

- Technische Sicherheitsmaßnahmen
  - Durch regelmäßige Tests sollte überprüft werden, ob die in der Sicherheitspolitik festgelegten Regeln korrekt umgesetzt worden sind.
  - Es sollte ein Integrationstest des Firewall-Systems initialisiert werden, der überprüft, ob das Firewall-System und das Regelwerk unversehrt sind.
- Infrastrukturelle Sicherheitsmaßnahmen
  - In regelmäßigen Abständen sollte überprüft werden, ob die infrastrukturellen Sicherheitsmaßnahmen (zugangsgesicherter Raum, geschützte Leitungsführung, Dokumentation und Kennzeichnung der Verkabelung des Firewall-Systems usw.) eingehalten werden.
- Organisatorische Sicherheitsmaßnahmen
  - In zyklischen Abständen muss überprüft werden, ob neue Verbindungen unter Umgehung des Common Point of Trust (Firewall-System) geschaffen wurden.
  - Die Logbuchdaten müssen regelmäßig überprüft werden, ob z. B. Angriffe stattgefunden haben.
- Personelle Sicherheitsmaßnahmen
  - In regelmäßigen Abständen sollten Aktionen eingeleitet werden, die das Sicherheitsbewusstsein erhöhen: Rundschreiben, Schulungen, Informationsveranstaltungen.

Durchzuführende Maßnahme	**Aufwand**
Technische Sicherheitsmaßnahmen	4 Tage pro Jahr
Infrastrukturelle Sicherheitsmaßnahmen	4 Tage pro Jahr
Organisatorische Sicherheitsmaßnahmen	4 Tage pro Jahr
Personelle Sicherheitmaßnahmen	12 Tage pro Jahr
Zusammenfassung	**24 Tage pro Jahr**

Tabelle 4:Aufwendungen für den sicheren Betrieb eines Firewall-Systems

Durchzuführende Maßnahme	**Aufwand**
Rechteverwaltung	18 Tage pro Jahr
Analyse der Logbuchdaten	24 Tage pro Jahr
Einrichtung neuer Dienste	6 Tage pro Jahr
Genereller administrativer Aufwand	24 Tage pro Jahr
Auswertung der Logbuchdaten auf dem Security Management	6 Tage pro Jahr
Sicherer Betrieb eines Firewall-Systems	24 Tage im Jahr
Zusammenfassung	**102 Tage pro Jahr**

Tabelle 5:Aufwendungen für die Aufrechterhaltung des Betriebs eines Firewall-Systems

Bei der Aufrechterhaltung des Betriebs eines Firewall-Systems, bei dem 1 000 Benutzer unter den beschriebenen Annahmen über das Firewall-System kommunizieren dürfen, ergibt sich ein Kostenaufwand von ca. EUR 76 500 im Jahr. Das sind ca. EUR 76,50 Kosten pro Benutzer im Jahr.

3.3 Zusammenfassung: Total Cost of Ownership

Aufwendungen für ein Firewall-System sind zum einen die Anschaffungskosten, die zwischen EUR 38 750 und EUR 236 250 liegen können, und die Kosten für die Aufrechterhaltung des Betriebs eines Firewall-Systems, die in unserem Rechenbeispiel, bei dem 1000 Benutzer über ein Firewall-System kommunizieren und eine große Anzahl von Veränderungen vorausgesetzt wurden, mit EUR 76 500 im Jahr veranschlagt.

Diese Zahlen hängen sehr stark von der Struktur und der Größe der Organisation ab. Außerdem müssen die folgenden Aspekte berücksichtigt werden:

- Welches Firewall-System wird verwendet?
- Wie gut ist das Firewall-Konzept?
- Anzahl der Benutzer, die über das Firewall-System kommunizieren dürfen
- Veränderung der Kommunikationsprofile
- Qualifikation der Administratoren des Security Managements
- Betriebszeiten
- Weitere Dienste, die zusätzlich angeboten werden:
  - Modem Server
  - Intranet Server
  - Internet Server usw.
- Veränderungen der Benutzer
- Veränderung der Netzstruktur
- Tiefe der Auswertung der Logbuchdaten
- Verwendetes Authentikationsverfahren
  - S/KEY (es müssen immer wieder neue Passwörter zur Verfügung gestellt werden)
  - Security Token (wird nur einmal eingerichtet)

4 Kosten-Nutzen-Betrachtung im Hinblick auf das zu tragende Risiko

In diesem Abschnitt wird eine Kosten-Nutzen-Betrachtung im Hinblick auf das zu tragende Risiko diskutiert.

Am Beispiel einer Bank mit ca. 1.000 Mitarbeitern soll eine Kosten-Nutzen-Betrachtung im Hinblick auf das zu tragende Risiko eines Firewall-Systems durchgeführt werden. Dabei wird angenommen, dass ohne den Einsatz eines Firewall-Systems die Wahrscheinlichkeit eines erfolgreichen Angriffs sehr hoch ist.

Angenommener Profit der Bank: EUR 25.000.000/Jahr

Kosten eines Firewall-Systems (Total Cost of Ownership)

- Anschaffungskosten: EUR 250.000 (1 % vom Profit)
- Betriebskosten: EUR 80.000/Jahr

Beschreibung eines möglichen Angriffs

Eine Bank wird von einem Hacker über das Internet angegriffen. Dieser kopiert sich aus dem zu schützenden Netz der Bank die Namen und Kontostände der 500 wichtigsten Kunden. Diese werden dann im Internet veröffentlicht, Fernsehen und Presse berichten und die Bank erleidet dadurch einen enormen Imageverlust.

Möglicher Schaden durch diesen Angriff

Durch den enormen Imageverlust wechseln sehr viele Kunden zu einer anderen vertrauenswürdigeren Bank, wodurch die angegriffene Bank einen Schaden hat, der wie folgt angenommen wird:

- sofort: EUR 12.500.000 (50 % vom Gewinn)
- mittelfristig: EUR 2.500.000/Jahr

4.1 Diskussion der Kosten-Nutzen-Betrachtung

Unter der Voraussetzung, dass der Angriff mit Hilfe eines Firewall-Systems verhindert worden und kein Schaden aufgetreten wäre, hätte sich die Investition in ein Firewall-System gelohnt. Mit der Investition von 1 % des Gewinns kann der Bank ein Schaden erspart werden, der sich auf ein Vielfaches der Investition beläuft (in diesem Beispiel das 60fache). Eine solche Investition ist offenkundig sehr sinnvoll.

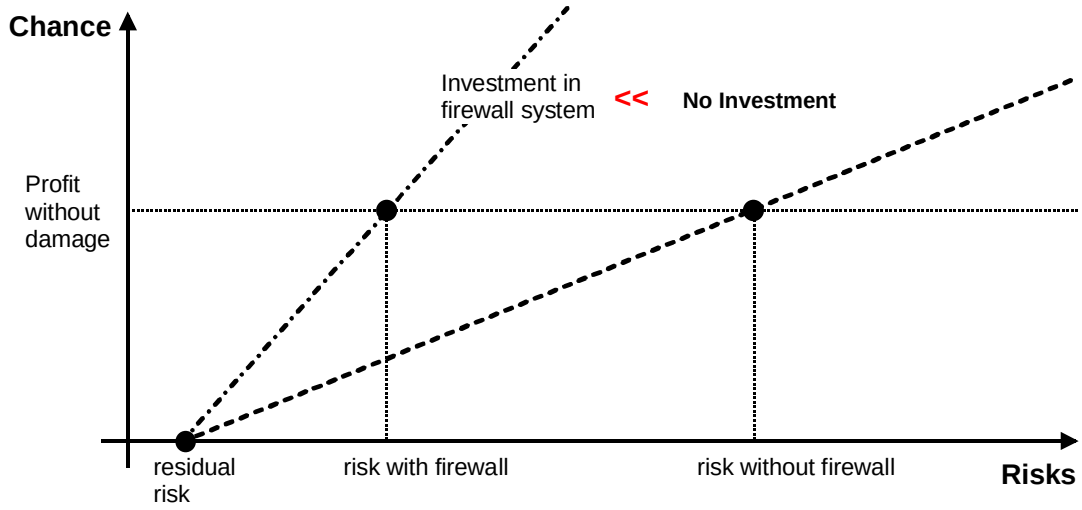

Abb. 3: Investment in Sicherheitsmechanismen und die Wahrscheinlichkeit eines bestimmten Profits

Mit Bekanntwerden des Angriffs werden auch Nachahmungstäter animiert, ebenfalls einen Angriff durchzuführen. Daher steigt das Risiko, erneut Opfer zu werden, und zu den Aufwendungen zur Behebung des Schadens kommen die Aufwendungen für die Anschaffung eines geeigneten Firewall-Systems, um weiteren Angriffen vorzubeugen.
Aus diesem Grund kann eine anfängliches "No Investment" später sehr viel Kosten verursachen.
Nach einer Studie von IDC steigen in den meisten Fällen nach einem größerem Sicherheitsvorfall die IT-Sicherheitsausgaben (survey released in March 2002 by IDC, Mass.).

4.2 Wahrscheinlichkeit eines bestimmten Profits

Die folgende Abbildung stellt dar, wie das Investment in Sicherheitsmechanismen vom eigenen Schutzbedarf und der Wahrscheinlichkeit, einen bestimmten Profit erreichen zu können, abhängt.

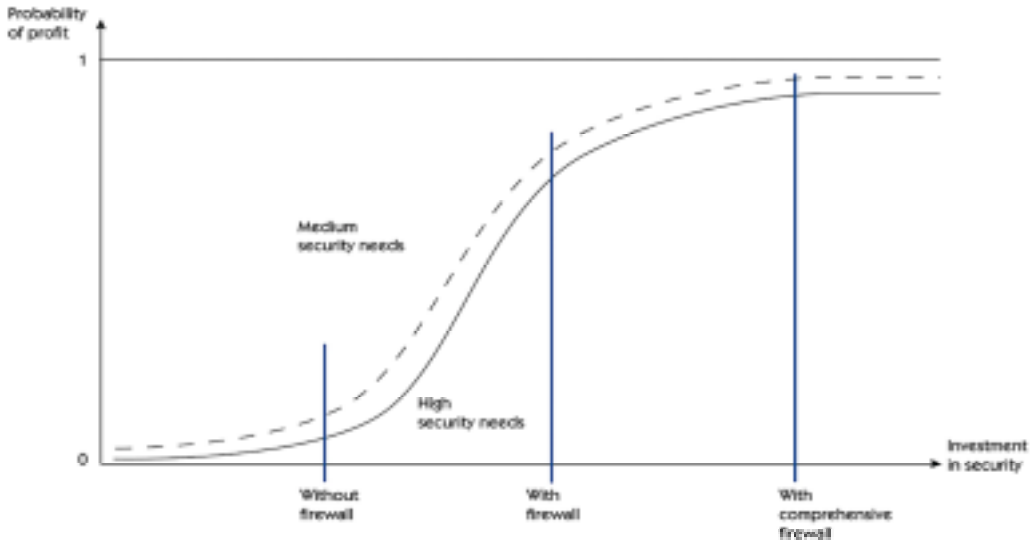

Abb. 4: Investment in Sicherheitsmechanismen und die Wahrscheinlichkeit eines bestimmten Profits

Die Abbildung zeigt, dass in Bereichen mit hohem Schutzbedarf (z. B. in Finanzinstituten) höhere Investitionen in Sicherheitsmaßnahmen notwendig sind, um die gleiche Chance auf einen bestimmten Gewinn zu bewahren.

Mit den Investitionen in Sicherheitsmechanismen steigt auch die Wahrscheinlichkeit, einen bestimmten Profit zu erreichen. Das heißt, die Anschaffung von Sicherheitssystemen wie Firewall-System, VPN, Intrusion Detection und Viren-Scanner ist ein Investment in die Absicherung des Gewinns. Die Wahrscheinlichkeit auf einen bestimmten Gewinn wird um so höher, je höher die Ausgaben für Sicherheitsmechanismen sind. Der Gewinn kann durch diese Maßnahmen allein aber nie hundertprozentig sicher sein, da immer ein Restrisiko bestehen bleibt.

Die Wahrscheinlichkeit der Gewinnerzielung hängt auch vom Schutzbedarf und damit von der Eintrittswahrscheinlichkeit eines Angriffs ab. Bei höherer Eintrittswahrscheinlichkeit steigt auch der Schutzbedarf vor einem Angriff.

Ist der Schutzbedarf sehr hoch, ist die Wahrscheinlichkeit auf einen Profit geringer als bei niedrigem Schutzbedarf.

Bei Verzicht auf Sicherheitsmechanismen ist dieser Unterschied viel größer als mit hohem Einsatz von Sicherheitsmechanismen, da die Eintrittswahrscheinlichkeit eines Angriffs bei niedrigem Schutzbedarf kleiner ist. Letztendlich ist die Unternehmensleitung für die Sicherheit in einem Unternehmen verantwortlich und muss über das richtige Kosten-Nutzen-Verhältnis entscheiden.

Die Unternehmensleitung ist gut beraten, wenn sie einen gewissen Prozentsatz des Gewinns als Gewinnversicherung für die IT-Sicherheit ausgibt. Dieser Prozentsatz wird bei Unternehmen, deren Image als vertrauenswürdiges Unternehmen die Basis ihres Erfolges darstellt (beispielsweise bei Banken und Versicherungen), höher liegen als bei Unternehmen wie Speditionen und Brauereien, bei denen die IT-Security in bezug auf das Image eine untergeordnete Rolle spielt.

5 Return on Security Investment RoSI - Nutzenaspekt

Im Folgenden soll eine Return on Security Investment (RoSI) Berechnung vorgestellt und an Hand eines Beispiels veranschaulicht werden.

RoSI bedeutet, dass bei der Betrachtung aller Kosten (auch die, die durch Schäden verursacht werden) aufgezeigt werden kann, ob und wann ein Investment in IT-Sicherheitsmaßnahmen zur einem Return on Investment führt oder nicht.

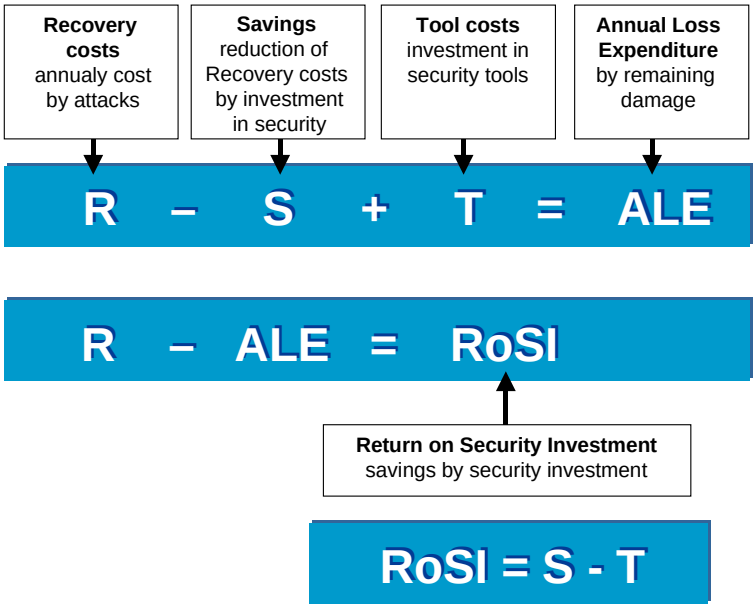

Abb. 5: Return on Security Investment

Beschreibung der Abkürzungen:

- Recovery Cost - R (Kosten der wahrscheinlichen Schäden)
  Diese Kosten beschreiben alle Aufwendungen, die notwendig sind, um bei einem aufgetretenen Schaden wieder den ursprünglichen Zustand herzustellen. Sie werden in die Gesamtkosten der geschäftlichen Tätigkeiten mit einbezogen. Die Recovery Cost hängen von dem tatsächlichen Eintritt von Schäden ab, müssen aber aus Erfahrungswerten für die Zukunft abgeschätzt werden.
  Hinweis:
  In den Recovery Cost können aber auch Aspekte wie die Erhöhung der Fremdkapitalkosten durch Basel II mit einfließen, die in Zukunft immer wichtiger werden. Falls keine geeigneten IT-Sicherheitsmaßnahmen eingeführt sind, müssen die Unternehmen für z.B. Investitionskredite mehr Zinsen zahlen. Dieses Mehr an Zinsen ist ein Schaden, der auftritt, weil keine angemessene IT-Sicherheit im Unternehmen vorhanden ist. Durch geeignete Investitionen in Tools kann der Schaden verhindert werden. Ein weiterer Aspekt ist die Reduzierung des Prämienaufwands für die IT-Versicherung, falls IT-Sicherheitsmaßnahmen eingesetzt werden.
- Savings - S (Reduzierung der Kosten der wahrscheinlichen Schäden)
  Beschreiben der Kosten, die durch die Einführung von IT- Sicherheitsmechanismen (Tools) gespart werden, weil sie mit einer sehr hohen Wahrscheinlichkeit einen erfolgreichen Angriff verhindert haben. Auch diese Kosten müssen abgeschätzt werden.
- Tool Cost - T (Kosten für IT-Sicherheitsmaßnahmen)
  Diese sind die vollständigen Kosten (Total Cost of Ownership - TCO) für die IT- Sicherheitsmechanismen, die potentiellen Angriffe mit einer hohen Wahrscheinlichkeit verhindern sollen.

- Annual Loss Expenditure - ALE (verbleibende Kosten)
  Das sind die verbleibenden Kosten (Schaden) nach einem Investment in Sicherheitsmechanismen.
- Return on Security Investment - RoSI (gesparte Kosten, erzielter Profit)
  Einsparungen der Recovery Cost (Schäden), die durch das Investment in Sicherheitsmechanismen erzielt wurden.

Hinweis:
Solange T, die TCO der IT-Sicherheitsmaßnahmen, kleiner sind als S, die Reduzierung der Kosten, ist RoSI positiv.

5.1 Beispiel: Notebookverluste

In diesem Beispiel soll anhand der Verluste von Notebooks exemplarisch eine Berechnung des Return on Security Investment durchgeführt werden.

Als erstes wird diskutiert, wie wahrscheinlich der Verlust oder der Diebstahl eines Notebooks ist, und welcher Schaden dabei auftreten kann.

Wie hoch ist die Wahrscheinlichkeit des Verlustes eines Notebooks?

Jeder der die Verantwortung von Notebooks im Unternehmen hat, weiß wieviele Notebooks jährlich aus nachvollziehbaren und nicht nachvollziehbaren Gründen verschwinden. Dennoch ist die offene Kommunikation darüber in den Unternehmen unüblich. Die meisten bekommen ein neues Notebook ohne lange Analysen darüber durchzuführen, warum und wie das alte Notebook abhanden gekommen ist. Da die meisten sowieso alle 2 bis 3 Jahre ein neues Notebook bekommen, geht die Verlustrate gerade in großen Unternehmen und Organisationen oft in der Masse der neuen Notebooks unter.

Wenn wir aber die unterschiedlichen Studien (www.compuclamp.com, www.microsaver.com, www.ebiz.za, World Security Corporation, ...), über verlorene oder gestohlene Notebooks analysieren, ist das Ergebnis, dass im Schnitt **6% der Notebooks** jährlich gestohlen (verloren) gehen (Eintrittswahrscheinlichkeit).

Wie hoch ist der Schaden, wenn die Daten, die auf einem Notebook gespeichert sind, von Dritten missbräuchlich verwendet werden?

Auch der Schaden, der auftritt, wenn ein Notebook z.B. durch die Konkurrenz gestohlen wird, kann der Besitzer des Notebooks am besten bemessen. Die Schwierigkeit, die hier auftritt ist, dass der Schaden oft nicht genau analysiert werden kann, sondern durch Reduktion des Umsatzes und des Gewinns nur schwer zu beziffern ist. Wenn wir aber betrachten, dass die meisten Notebooks eines Unternehmens von der Unternehmensleitung, den Vertriebsleuten und die wichtigsten Entwicklern verwendet werden, die mit ihrem Notebook auf Reisen gehen oder von zu Hause arbeiten, wo die Eintrittswahrscheinlichkeit höher ist und hier oft alle wichtigen Unternehmensinformationen wie z.B. Preiskalkulationen, Entwicklungsdaten, Finanzanalysen, Lieferanten Einkaufspreise, usw, gespeichert sind, fällt es nicht schwer zu erkennen, dass der mögliche Schaden sehr groß sein kann.

Wenn wir die unterschiedlichen Studien (Computer Security Institut - Crime&Security Survey, Security Issuess and Trends, ...) über die Schäden von verlorenen Notebooks analysieren, kommen wir zu dem Ergebnis, dass im Schnitt der **Schaden pro gestohlenes Notebook über € 10.000 liegt**. Dies ist nur der Schaden, der durch mißbräuchliche Verwendung der Daten entsteht, der Verlust der Hardware, Software und Wiederherstellung eines Ersatzgerätes muss noch zusätzlich betrachtet werden (€ 2.000,-- bis 4.000,--).

Sicherheitssystem zum Schutz der Informationen, die auf einem Notebook gespeichert sind.

Um die Kosten abzuschätzen, die notwendig sind ein Notebook angemessen zu schützen, wird angenommen, dass ein Festplattenverschüsselungsprodukt verwendet wird. Das Festplattenverschlüsselungsprodukt arbeitet mit einer Boot-Authentikation, d.h. der Benutzer muss sich beim Hochfahren des Notebooks erst über die Eingabe eines Passwortes authentisieren. Alle Daten auf dem Notebook sind auf der Festplatte nur in verschlüsselter Form vorhanden. Nachdem sich der Benutzer authentisiert hat, werden durch das Sicherheitssystem die Daten, die verwendet werden, jeweils für die Verarbeitung entschlüsselt und in verschlüsselter Form wieder auf der Festplatte gespeichert. Wenn ein Dieb

dieses Notebook stiehlt, kann er zwar z.B. durch den Ausbau der Festplatte an die Daten gelagen, da diese aber verschlüsselt sind, kann er sie nicht für sich verwenden, und daher mit den Informationen auf dem Notebook keinen Schaden für den Besitzer anrichten.

Der Schaden für den Benutzer bleibt bei dem Verlust des Notebooks mit der installierten Software (2.000 bis 3.000 €) und die Wiederbeschaffung und Fertigstellung eines neuen Notebooks begrenzt.

Die Anschaffung eines solchen Sicherheitssystems kostet ca. € 110,--, d.h. im Schnitt ca. 4% des Anschaffungspreises.

5.2 Return on Security Investment RoSI - Berechnung

Als Beispiel wird ein Unternehmen angenommen, bei dem 500 Mitarbeiter ein Notebook besitzen und für die Arbeit mit schätzenswerten, wertvollen Daten verwenden.

Annahmen:

- Schaden durch den Verlust der gespeicherten Daten,
  pro gestohlenes Notebook = € 10.000,--
- Die Anzahl der Notebooks, die jedes Jahr gestohlen werden,
  wird mit 6% = 30 Notebooks angenommen (Eintrittswahrscheinlichkeit).

Tool Cost - T (Kosten für das Festplattenverschüsselungsprodukt)

- Einmalige Lizenzkosten: 500 * € 110 = € 55.000
- Für die weiteren Kosten von Installation, Roll-Out und Verwaltung wird im ersten Jahr € 10.000,-- und in den folgenden Jahren € 5.000,-- angenommen.

Savings - S (vermiedener Schaden)

- 30 Notebooks * € 10.000 = € 300.000,--
- Hier wird nur der Schaden durch die mißbräuchliche Verwendung der gespeicherten Daten betrachtet.

In der folgenden Tabelle sind die Kosten für die IT-Sicherheitsmaßnahmen und der potentielle Verlust auf vier Jahre eingetragen.

Calculation					**In total**
Time span	1st year	2nd year	3rd year	4th year	4 years
Initial costs	**€55.000**	**--**	**--**	**--**	**€55.000**
Implementation/ Roll-out, Admin	**€10.000**	**€ 5.000**	**€ 5.000**	**€ 5.000**	**€ 25.000**
Reduced costs??	**--**	**--**	**--**	**--**	**--**
Value of no losses from security breaches	**€ 300.000**	**€ 300.000**	**€ 300.000**	**€ 300.000**	**€1.200.000**
ROI 1st year	**€235.000**				
ROI 2nd year		**€530.000**			
ROI 3rd year			**€ 825.000**		
ROI 4th year				**€1.1.20.000**	**€1.120.000**

Tabelle 6: Return on Security Investment RoSI - Berechnung: 1. Beispiel

Hier kann aufgezeigt werden, dass schon im ersten Jahr ein ROI von € 235.000,-- erzielt werden kann. Nach vier Jahren liegt der ROI bei € 1.120.000.

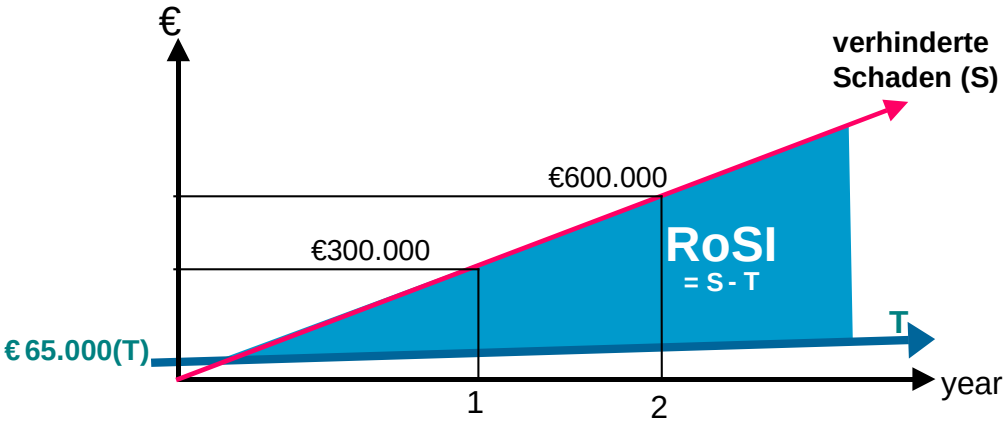

Abb. 6: Return on Security Investment

Diese Grafik zeigt deutlich, dass das Investment T, in Festplattenverschlüsselung, kleiner ist als der verhinderte Schaden S, der durch die mißbräuchliche Verwendung der gespeicherten Daten auftreten würde.

Ein weiteres Beispiel mit anderen Annahmen:

In der folgenden Tabelle werden die Annahmen für den Schaden und die Eintrittswahrscheinlichkeit anders angenommen.

Annahmen:

- Schaden durch den Verlust der gespeicherten Daten,
  pro gestohlenes Notebook = € 5.000,--
- Die Anzahl der Notebooks, die jedes Jahr gestohlen werden,
  wird mit 3% = 15 Notebooks angenommen (Eintrittswahrscheinlichkeit)..

Tool Cost - T (Kosten für das Festplattenverschüsselungsprodukt)

- Einmalige Lizenzkosten: 500 * € 110 = € 55.000
- Für die weiteren Kosten von Installation, Roll-Out und Verwaltung wird im ersten Jahr € 10.000,-- und in den folgenden Jahren € 5.000,-- angenommen.

Savings - S (vermiedener Schaden)

- 15 Notebooks * € 5.000 = € 75.000,--

Calculation					**In total**
Time span	1st year	2nd year	3rd year	4th year	4 years
Initial costs	**€55.000**	**--**	**--**	**--**	**€55.000**
Implementation/ Roll-out, Admin	**€10.000**	**€ 5.000**	**€ 5.000**	**€ 5.000**	**€ 25.000**
Reduced costs??	**--**	**--**	**--**	**--**	**--**
Value of no losses from security breaches	**€75.000**	**€ 75.000**	**€ 75.000**	**€ 75.000**	**€300.000**
ROI 1st year	**€10.000**				
ROI 2nd year		**€80.000**			
ROI 3rd year			**€ 150.000**		
ROI 4th year				**€220.000**	**€220.000**

Tabelle 7: Return on Security Investment RoSI - Berechnung: 2. Beispiel

Auch bei diesem Beispiel kann aufgezeigt werden, dass schon im ersten Jahr ein ROI von € 10.000,-- erzielt werden kann. Nach vier Jahren liegt der ROI bei € 220.000.

Weitere Beispiele, bei denen eine RoSI-Berechnung in der Regel einfach durchgeführt werden kann, sind:

- Viren-Scanner
  - Hier haben die meisten Unternehmen in den letzten Jahre selber Zahlen über die Kosten, die durch Schäden bei Virenbefall aufgetreten sind, zur Verfügung.
- SingleSineOn (SSO) oder Authentikation mit biometrischen Verfahren
  - Hier kann der Einspareffekt durch Helpdesk Kosten sehr gut nachgewiesen werden.
- Elektronische Rechnungen mit digitaler Signatur
  - In diesem Bereich gibt es Studien, die aufzeigen, dass mit Hilfe einer elektronischen Rechnung sehr viel Geld gespart werden kann. Statt € 1,40 für eine normale Papierrechnung mit handgeschriebener Unterschrift versendet, oder € 0,40 für eine elektronische Rechnung mit digitaler Signatur, z.B. per E-Mail versendet.

6 Gesamtwirtschaftliche Betrachtung von IT-Sicherheit

In der Industriegesellschaft war die Sicherheit von Produktionsanlagen wichtig. In der heutigen Informationsgesellschaft ist die Sicherheit von IT-Systemen von hoher Bedeutung. Informationen (Informationsgüter, digitale Produkte) erlangen erstmals eine überragende Bedeutung für Produktion und Konsum. Die Produktionsweise prägt die Gesellschaft. Es ist deshalb durchaus zulässig, von der Entstehung einer Informationsökonomie auf die Entstehung einer Informationsgesellschaft zu schließen /Welz2000/.

Bei der gesamtwirtschaftlichen Betrachtung kann von statischen und dynamischen Aspekten gesprochen werden, wenn die mangelnde IT-Sicherheit diskutiert wird.

Statische Aspekte der mangelnden IT-Sicherheit führen zu einem Verlust an Effektivität und Effizienz im privaten wie öffentlichen Sektor und belasten somit die Leistungsfähigkeit der Volkswirtschaft insgesamt. Dies kann punktuell, d. h. bei einzelnen Unternehmen oder in einzelnen Sektoren, besonders gravierende Folgen haben.

Dynamische Aspekte der mangelnden IT-Sicherheit vermindern und behindern die Nutzung der rapide wachsenden Vorteile digitaler Technologien und Märkte, z. B. wegen höherer Kosten und geringerer Akzeptanz, und führen indirekt zu einem Verzicht auf strategische Vorteile aus einer Marktdominanz.

Es bleibt abzuwarten, ob die Verantwortlichen in Wirtschaft und Behörden selbst für die notwendige Sicherheit sorgen, oder ob über Gesetze Vorschriften erlassen werden müssen, damit eine ausreichende Sicherheit unserer Informationsgesellschaft erreicht werden kann.

Das Problem gesetzlicher Vorschriften ist, dass diese international sein müssten, damit sie im globalem Internet greifen könnten. Die Bemühungen um eine internationale Gesetzgebung haben bei der G8 erst in Jahr 2000 begonnen und werden sicherlich fünf bis zehn Jahre benötigen.

7 Zusammenfassung

Die Wirtschaftlichkeit von IT-Sicherheitsmaßnahmen ist ein zunehmend wichtiger und sehr komplexer Punkt, mit dem sich die Verantwortlichen in Unternehmen, Behörden, aber auch die Regierungen, in einer gesellschaftlichen Verantwortung auseinandersetzen müssen.

Dennoch gibt es Maßnahmen zur IT-Sicherheit, die rein wirtschaftlich nicht sinnvoll sind und dennoch durchgeführt werden, wie z.B. als gesetzliche Notwendigkeit, wenn es um die Sicherheit von Menschen geht, Militär, Angst, übertriebenes Sicherheitsgefühl.

Wenn wir in der Lage sind, Schaden nicht nur zu qualifizieren, sondern zu quantifizieren, dann können wir, wie aufgezeigt wurde, ein Return of Security Investment – RoSI berechnen und erzielen.

Um diesen Aspekt erfüllen zu können, müssen wir anfangen, die Angriffe und die resultierenden Schäden so gut wir möglich zu dokumentieren. Dazu benötigen wir in Zukunft geeignete Hilfsmittel.

Durch die neuen Rahmenbedingungen des Risikomanagements, die z.B. durch Basel II auf alle Unternehmen zukommen, wird ein weiterer Aspekt der Wirtschaftlichkeitsberechnung von IT-Sicherheitsmaßnahmen berücksichtigt werden müssen.

8 Literatur

H. Blumberg, N. Pohlmann: "Der IT-Sicherheitsleitfaden“, ISBN 3-8266-0940-9, MITP-Verlag, Bonn 2004

N. Pohlmann: "Firewall-Systeme - Sicherheit für Internet und Intranet, E-Mail-Security,
Virtual Private Network, Intrution Detection-System, Personal Firewalls", 5. aktualisierte und erweiterte Auflage, ISBN 3-8266-0988-3; MITP-Verlag, Bonn 2003

N. Pohlmann: „Kosten und Nutzen von Firewall-Systemen – Betriebswirtschaftliche Betrachtung einer IT-Sicherheitsmaßnahme”, IT-Sicherheit – Praxis der Daten- und Netzsicherheit, DATAKONTEXT-Fachverlag, 1/2001