Wie wirtschaftlich sind IT-Sicherheitsmaßnahmen?

Norbert Pohlmann

Institut für Internet-Sicherheit
Wetsfdälische Hochschule Gelsenkirchen
Fachbereich Informatik
Neidenburger Straße 43
45877 Gelsenkirchen

pohlmann@internet-Sicherheit.de

Zusammenfassung

IT-Sicherheitsmaßnahmen sind kein Selbstzweck. Mit Hilfe von IT-Sicherheitsmaßnahmen kann das Risiko bei der Nutzung von IT-Systemen erheblich reduziert und damit ein Schaden verhindert werden. In diesem Artikel sollen die Kosten und der Nutzen der IT-Sicherheitsmaßnahmen betrachtet und bewertet werden. Da eine IT-Sicherheitsmaßnahme eine Investition für die Zukunft ist, sollten die Kosten-Nutzen-Aspekte schon bei der Planung von IT-Sicherheitsmaßnahmen besonders berücksichtigt werden.

Einführung

Die Aufgabe von IT-Systemen ist es, die Geschäftsprozesse in Unternehmen zu optimieren 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 z.B. dadurch erreicht werden, dass die Aufgaben vereinfacht oder beschleunigt werden, z.B. durch die Nutzung der E-Mail-Anwendung als ein einfaches und schnelles Kommunikationsmittel. Abläufe können mit der Hilfe von IT-Systemen störungsfreier oder flexibler gestaltet werden, z.B. keine Medienbruch mehr, die Verwendung von mobilen Geräten (Notebooks, PDAs, usw.) und damit das Arbeiten von zu Hause oder von unterwegs. Mitarbeiter können von Routineaufgaben entlastet und bei komplexen Aufgaben unterstützt werden, z.B. durch die Nutzung von CAD – Systemen. Die globale wirtschaftliche Ausdehnung kann mit der Hilfe von IT-Systemen einfach ermöglicht werden, z.B. durch die Nutzung des Internets, Angebote übers Web international verfügbar machen, E-Mail als Kommunikationsmedium nutzen oder Videokonferenzen nutzen, um mit internationalen Geschäftspartnern Absprachen zu treffen.

Was für sämtliche Geschäftsbereiche eines Unternehmens gilt, gilt auch für den Einsatz von IT-Systemen: sie müssen wirtschaftlich sein. Diese Wirtschaftlichkeit kann durch unterschiedliche Wirtschaftlichkeitsprinzipien erreicht werden:

Das **Minimierungsprinzip** hat als Schwerpunkt, dass bei einem gesetzten Ziel minimaler Aufwand betrieben werden soll. Wenn das Ziel ein bestimmter Gewinn ist, müssen bei gleichem Umsatz die Kosten gesenkt werden. Somit soll das Ziel Gewinn (Profit) durch den minimalen Mittelverbrauch (Kosten/Input) erreicht werden.

Das **Maximierungsprinzip** bedeutet, dass mit gegebenen Mitteln ein maximales Ziel erreicht werden soll. Der Gewinn ist dabei eine individuell wählbare Zielvorstellung und soll mit den gegebenen Mitteln maximiert werden. Die Mittel (Kosten/Input) sind also vorgegeben, der Umsatz (Output) ist jedoch ein Ziel, das bezüglich des Profits optimiert werden soll.

Das **generelle Extremumprinzip** ist so zu verstehen, dass Mitteleinsatz und Ergebnis so aufeinander abgestimmt sind, dass der durch sie definierte Prozess, gemessen an problemindividuellen Kriterien, optimal wird. Hierbei strebt keine Größe nach einem bestimmten Ergebnis oder Ziel, sondern Kosten und Umsatz stehen in einer variablen Wechselwirkung zu einander. Um den Prozess des Wirtschaftens zu optimieren, müssen Arbeitsschritte einer ständigen Qualitätskontrolle unterliegen.

Diese unterschiedlichen Wirtschaftlichkeitsprinzipien 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

Total Cost of Ownership bedeutet die Kosten für Anschaffung, Schulung, Installation, Betrieb, Wartung und Ersatz von IT-Systemen und IT-Sicherheitsmaßnahmen zu errechnen. Diese entspricht der Kapitalwert-Methode, d.h. was kostet ein Investment in der Summe aller Aspekte, die berücksichtigt werden müssen? Dieser Wert kann mit den Kosten, die z.B. durch einen erfolgten oder geschätzten Schaden und dessen sofortige, mittelfristige und langfristige finanziellen Auswirkungen, verglichen werden.

Nach Nutzenaspekten: ROI = Return on Investments

Hier wird der 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 durch den mit der Investition erwirtschafteten Ertrag gedeckt? Je schneller eine Deckung erzielt wird, umso schneller kann ein Gewinn, z.B. durch das Investment von IT-Sicherheitsmaßnahmen, generiert werden.

IT-Sicherheit

Im Folgenden werden einige Begriffe definiert, die helfen unterschiedliche Sichtweisen auf die IT-Sicherheit besser zu verstehen.

Schutzbedarf von IT-Systemen

Der Schutzbedarf wird in IT-Werten bemessen. Die Höhe des IT-Wertes zeigt dessen Bedeutung für den Eigentümer und hilft Sicherheitsmaßnahmen ökonomisch und zielgerichtet einzusetzen. Zu den IT-Werten gehören u.a. die Daten (Entwicklungsdaten, Vertriebsdaten, Logistikdaten, usw.), IT-Systeme (Hardware) und IT-Anwendungen (Software). Um den Schutzbedarf von IT-Werten einheitlich festzustellen, wird ein festgelegter Maßstab benötigt, der bzgl. der Grundwerte Vertraulichkeit, Integrität und Verfügbarkeit festlegt, wann der Schutzbedarf als „niedrig bis mittel“, „hoch“ oder „sehr hoch“ anzusehen ist. Wenn dann der Schutzbedarf der IT-Applikationen und Daten gemäß des Schutzbedarfsmaßstabes festgestellt ist, lässt sich der Schutzbedarf für die IT-Systeme einfach ableiten (siehe BSI IT-Grundschutzhandbuch: www.bsi.de).

Wie sicher ist „sicher“?

Bei so vielen Risiken und Gefahren in der IT-Welt, stellt sich unweigerlich die Frage, wie wirksam IT-Sicherheitsmaßnahmen überhaupt sein können. Ein grundsätzlich wichtiges Kriterium für die Beurteilung von IT-Sicherheitsmaßnahmen ist die Frage danach, ob die IT-Sicherheitsmaßnahmen auch tatsächlich in der Lage sind, den realen Angriffen entgegen zu wirken. Dabei kann die Stärke der eingesetzten IT-Sicherheitsmaßnahmen unterschiedlich bewertet werden. Meist werden hier für die Bewertungen der Wirksamkeit „hoch“, „mittel“ und „niedrig“ verwendet. Wichtige Kriterien für die Bewertung der Stärke der Wirksamkeit sind dabei Fachkenntnisse, Ressourcen und Gelegenheit der potentiellen Angreifer. Unter Fachkenntnisse fasst man alle Kriterien zusammen, die das Anwendungs-KnowHow des Angreifers beschreiben. Handelt es sich um einen Laien, einen versierten Benutzer (eine kenntnisreiche Person) oder gar einen Experten? Ressourcen sind die für einen erfolgreichen Angriff erforderlichen Mittel. Dabei unterscheidet man die Komponenten Zeit und Ausstattung – die Zeit, die zur Durchführung des Angriffs benötigt wird und die erforderliche Ausstattung in Form von Hardware, Werkzeugen und Software. So entstehen Bewertungsbandbreiten von „Sonderausstattung - innerhalb von Monaten“ bis hin zu „Ohne Ausstattung – innerhalb von Minuten“. Das Bewertungskriterium „Gelegenheit“ beschreibt im Gegensatz zu den anderen Punkten die eher schwer kontrollierbaren Gegebenheiten wie Zufall, geheime Absprachen und Entdeckung. Darunter fällt die eher zufällige Zusammenarbeit mit einem Anwender genauso, wie Absprachen mit dem eigentlich als vertrauenswürdig eingestuften Systemverwalter. Daraus ergeben sich Sicherheitsbewertungen, die der jeweiligen Situation entsprechend greifen können. So kann eine IT-Sicherheitsmaßnahme, die innerhalb von Minuten von einem Laien alleine überwunden werden kann, wohl nicht einmal mehr als „niedrig“ bezüglich der Wirksamkeit eingestuft werden. Jedoch könnte man eine IT-Sicherheitsmaßnahme, die nur mittels Sonderausstattung und in monatelanger Expertenarbeit in die Knie gezwungen werden kann, bezüglich der Wirksamkeit als „hoch“ einstufen. Ein weiteres Kriterium zur Beurteilung einer IT.Sicherheitsmaßnahme ist die Korrektheit. Mit dem Faktor Korrektheit soll überprüft und beurteilt werden, ob die IT-

Sicherheitsmaßnahmen korrekt implementiert sind und wie groß das Vertrauen in die Implementierung der Lösungen ist. Grundsätzlich kann also gesagt werden, dass IT-Sicherheitsmaßnahmen nur als wirklich sicher eingestuft werden können, wenn Wirksamkeit, Stärke und Korrektheit zu gleichen Teilen in angemessener Qualität vorherrschen.

Verwundbarkeit

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!

IT-Sicherheitsrisiken und -investment

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

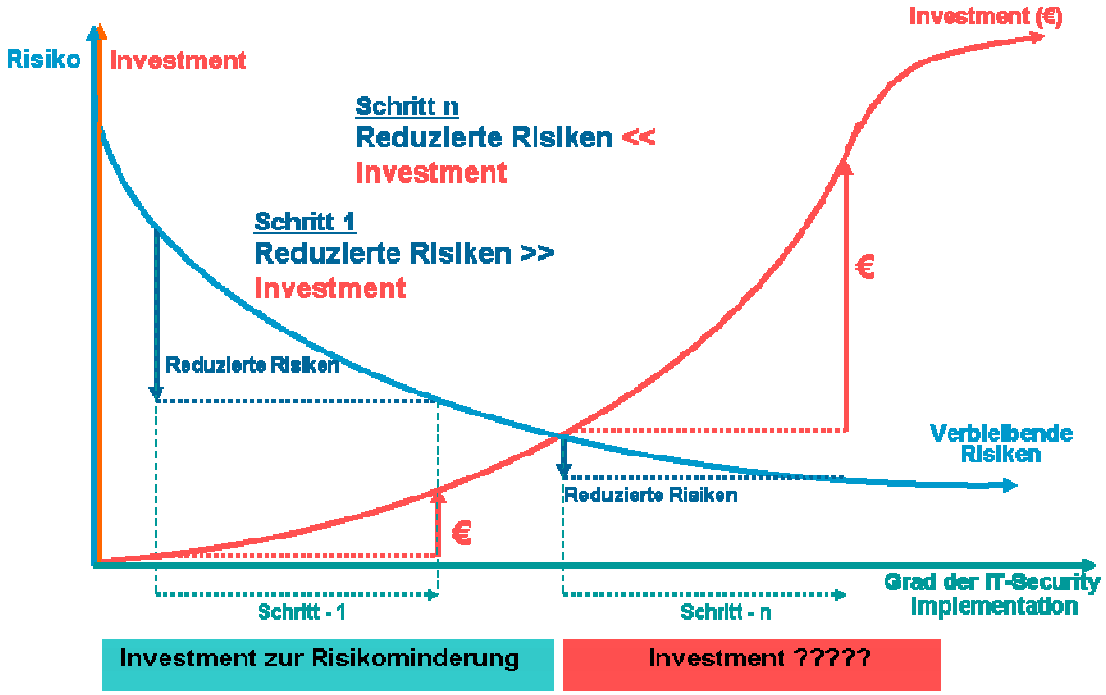

Abb. 1: IT-Sicherheitsrisiken und -investment

Abb. 1 zeigt, dass in einem ersten Schritt mit einem kleinen Investment eine große Risikominimierung erzielt werden kann (Reduzierte Risiken >> Investment). Wird aber immer weiter in IT-Sicherheitsmaßnahmen investiert, dreht sich das Verhältnis. Mit einem hohen Investment in weiteren Schritten kann nur noch eine kleine Risikominimierung mit IT-Sicherheitsmaßnahmen erreicht werden (Reduzierte Risiken << Investment).

Aus dieser praktischen Erfahrung 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 hoch 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 oder übertriebenes Sicherheitsgefühl.

Return on Security Investment RoSI - Nutzenaspekt

Im Folgenden soll eine Return on Security Investment (RoSI) Berechnung vorgestellt werden, mit der ein Nutzenaspekt von IT-Sicherheitsmaßnahmen dargestellt werden kann.

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

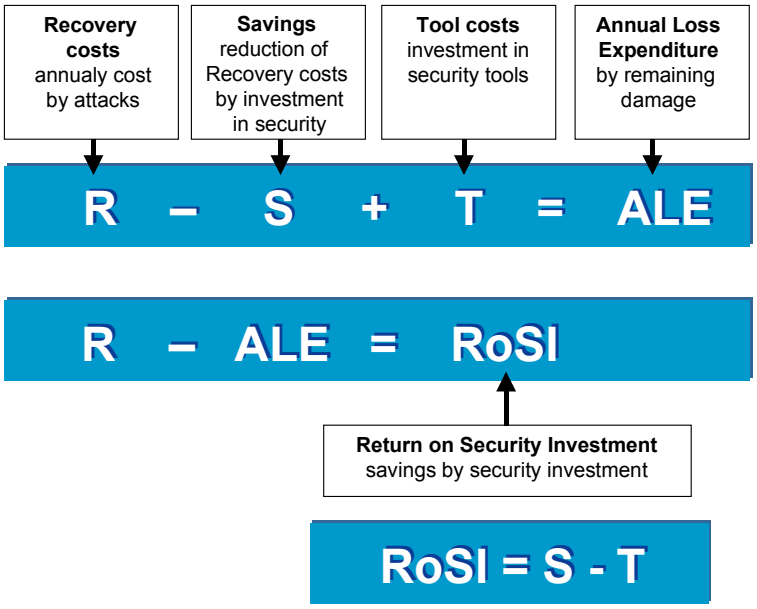

Abb. 2: Return on Security Investment

Beschreibung der Abkürzungen:

Recovery Costs - R (Kosten der wahrscheinlichen Schäden)
Diese Kosten beschreiben alle Aufwendungen, die notwendig sind, um nach einem aufgetretenen Schaden den ursprünglichen Zustand wieder herzustellen. Sie werden in die Gesamtkosten der geschäftlichen Tätigkeiten mit einbezogen. Die Recovery Costs hängen von dem tatsächlichen Eintritt von Schäden ab, müssen aber aus Erfahrungswerten für die Zukunft abgeschätzt werden.
Hinweis:
In den Recovery Costs 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)
Hierbei handelt es sich um die Kosten, die durch die Einführung von IT- Sicherheitsmechanismen (Tools) gespart werden, weil sie mit einer sehr hohen Wahrscheinlichkeit einen Angriff erfolgreich verhindern haben. Auch diese Kosten müssen abgeschätzt werden.

Tool Costs - T (Kosten für IT-Sicherheitsmaßnahmen)
Dies sind die vollständigen Kosten (Total Cost of Ownership - TCO) für die IT-Sicherheitsmaßnahmen, die potentielle Angriffe mit einer hohen Wahrscheinlichkeit verhindern sollen.

Annual Loss Expenditure - ALE (verbleibende Kosten)
Das sind die verbleibenden Kosten (Schaden) nach einem Investment in IT-Sicherheitsmaßnahmen.

Return on Security Investment - RoSI (gesparte Kosten, erzielter Profit)
Einsparungen der Recovery Cost (Schäden), die durch das Investment in IT-Sicherheitsmaßnahmen erzielt wurden.

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

Formel: R - (R - S + T) = RoSI = S - T

Beispielberechung RoSI: Notebookverluste

In diesem Beispiel soll anhand der Verluste von Notebooks und die Investition in eine passende IT-Sicherheitsmaßnahme, die die Daten auf den Notebooks schützt, exemplarisch eine Berechnung des Return on Security Investment (RoSI) 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 für Notebooks im Unternehmen hat, weiß wie viele 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, so zeigt sich, 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 den wichtigsten Entwicklern verwendet werden, die mit ihrem Notebook auf Reisen gehen oder von zu Hause aus 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 Issues and Trends, ...) über die Schäden von verlorenen Notebooks analysieren, kommen wir zu dem Ergebnis, dass im Schnitt der **Schaden pro gestohlenem 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 3.000,--).

IT-Sicherheitsmaßnahme zum Schutz der Informationen, die auf einem Notebook gespeichert sind.

Um die Kosten abzuschätzen, die notwendig sind um 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 diese IT-Sicherheitsmaßnahme 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 z.B. durch den Ausbau der Festplatte an die Daten gelangen. 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 einschließlich der installierten Software (2.000 bis 3.000 €) und die Wiederbeschaffung und Fertigstellung eines neuen Notebooks begrenzt.

Die Anschaffung einer solchen IT-Sicherheitsmaßnahme kostet ca. € 110,--, d.h. im Schnitt ca. 4% des Anschaffungspreises eines Notebooks.

Berechnung der Return on Security Investment (RoSI)

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

Annahmen:

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

Tool Costs - 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 1: Return on Security Investment RoSI - Berechnung: 1. Beispiel

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

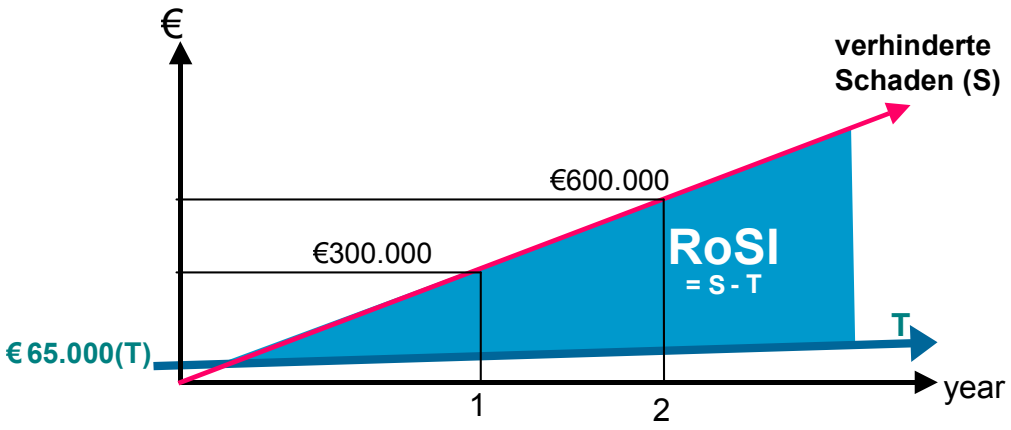

Abb. 3: Return on Security Investment

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.

Beispiel mit anderen Annahmen:

In diesem Beispiel werden die Annahmen für den Schaden und die Eintrittswahrscheinlichkeit anders angenommen.

Annahmen:

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

Tool Costs - 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 2: 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 Jahren selber Zahlen über die Kosten, die durch Schäden bei Virenbefall aufgetreten sind, zur Verfügung.

ID-Management, SingleSineOn (SSO) oder Authentikation mit biometrischen Verfahren
Hier kann der Einspareffekt durch Helpdesk-Kosten sehr gut nachgewiesen werden (100 bis 200 €/Jahr pro Benutzer).

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 versendete normale Papierrechnung mit handgeschriebener Unterschrift, kann eine elektronische Rechnung mit digitaler Signatur, z.B. per E-Mail bereits für € 0,40 versendet werden.

Herausforderungen bei der RoSI-Berechnung

Die RoSi-Berechnung kann, anders als im Notebook-Beispiel, ein sehr komplexer Prozess sein. Die Komplexität bei vielen Berechnungen kommt durch die Abschätzung des direkten und indirekten Schadens eines möglichen erfolgreichen Angriffes und die Beurteilung der Reduzierung des Schadens durch eine spezielle IT-Sicherheitsmaßnahme, die dagegen wirkt zustande. Weitere, schwer kalkulierbare Aspekte sind zum einem die Beurteilung des direkten Zusammenhangs zwischen einem konkreten Angriff und einem speziellen Schaden und zum anderen die Abschätzung zwischen einem Angriff und der unmittelbaren Wirkung einer IT-Sicherheitsmaßnahme. Hier müssen in der Praxis die Kosten für die IT-Sicherheitmaßnahmen oft auf verschiedene Schadensfälle, die möglicherweise durch unterschiedliche Angriffe verursacht wurden, anteilig berechnet werden.

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

Wenn wir in der Lage sind, Schäden nicht nur zu qualifizieren, sondern auch zu quantifizieren, dann können wir, wie aufgezeigt wurde, ein Return of Security Investment (RoSI) berechnen und oft auch in der Praxis erzielen. Der Einsatz von IT-Sicherheitsmaßnahmen kann also weit mehr von Nutzen sein und sollte nicht nur als kostspieliger Nebeneffekt betrachtet werden oder aus Angst vor Haftung oder Gesetzen in Betracht gezogen werden.

Um diesen Aspekt erfüllen zu können, müssen wir anfangen, die Angriffe und die resultierenden Schäden so gut wie möglich zu dokumentieren, damit wir die tatsächlichen Kosten der Schäden benennen können. Dazu benötigen wir in Zukunft geeignete Hilfsmittel, die die Kosten von erfolgreichen Angriffen festhalten.

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

Literatur

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

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