Fraunhofer
SIT

Werte schützen, Kosten senken, Erträge steigern

Beispiele für die Wirtschaftlichkeit von Informationssicherheit

White Paper

Fraunhofer-Institut für
Sichere Informationstechnologie
Darmstadt, Sankt Augustin

Kontakt:

Mechthild Stöwer

Mechthild.stoewer@sit.fraunhofer.de

Inhaltsverzeichnis

Zusammenfassung

In vielen Seminaren und Veröffentlichungen ist immer wieder die Rede davon, dass Maßnahmen und Verfahren zur Steigerung der IT-Sicherheit sich auch anderweitig positiv in Unternehmen bemerkbar machen. Praktische Beispiele und belastbares Zahlenmaterial für die Wirtschaftlichkeit von IT-Sicherheitsverfahren fehlen jedoch bislang. Dieses Whitepaper beschreibt zunächst die allgemeinen Verfahren zur Erfassung der Wirtschaftlichkeit von IT-Sicherheitstechnik und wendet diese auf vier konkrete Sicherheitsverfahren an, die am Fraunhofer SIT entwickelt/erprobt wurden.

Alle beschriebenen Fallbeispiele zeigen konkrete Mehrwerte von IT-Sicherheitsinvestitionen auf, wobei es drei Gründe für die monetären Vorteile gibt:

1) Vermeidung von Schäden und Folgeschäden

2) Effizienzsteigerung von Prozessen

3) Erschließung von neuen Wertschöpfungsspotentialen

Jedes Fallbeispiel enthält eine konkrete Kosten-/Nutzen-Berechnung. Diese basieren teils auf Erfahrungen, teils auf Modellrechnungen und wurden soweit möglich mit bekannten Beispielen und Zahlen ergänzt.

Die Betrachtung der Beispiele zeigte, dass Unternehmen durch IT-Sicherheitsinvestitionen nicht nur ihre Sicherheitsprozesse optimieren und Kosten reduzieren können, sondern sich mit IT-Sicherheitstechnik auch Prozesse und Leistungsangebote verbessern lassen. Zwar sind mögliche Mehrwerte von IT-Sicherheit aufgrund von komplexen Zusammenhängen und Wechselwirkungen nicht immer leicht vorherzusagen, entsprechende RoSI-Kalkulationsverfahren verschaffen Unternehmen jedoch ausreichend Planungssicherheit.

1 Einführung

Es gibt vier Gründe für die Implementierung von IT-Sicherheitsverfahren in einem Unternehmen:

Zunächst sind es *gesetzliche Verpflichtungen*, zum Beispiel zum Datenschutz oder zur Archivierung, die Unternehmen zwingen, Sicherheitsmaßnahmen zu ergreifen. Überlegungen, ob sich diese Investitionen auch wirtschaftlich lohnen werden, spielen keine Rolle.

Der klassische Investitionsgrund ist jedoch die *Abwendung von Schäden* durch die Implementation von IT-Sicherheitslösungen, deren Identifikation eine Analyse der Bedrohungen und Schwachstellen sowie von Schadensgröße und Eintrittswahrscheinlichkeit zugrunde liegt. Beispiele dafür sind Firewalls und die Verschlüsselung von Kommunikation.

Drittens können Sicherheitsverfahren die *Effizienz bestehender Verfahren steigern*, etwa bei der Nutzung von einfach zu bedienenden Signaturkarten oder Passwortmanagern.

Oft spielen zwei oder gar alle drei dieser Gründe zusammen, etwa bei der Absicherung digitaler Waren durch die Nutzung der Wasserzeichentechnologie: Händler sind gesetzlich verpflichtet, den Schutz der Urheber zu gewährleisten, weiterhin birgt die unkontrollierten Weitergabe von Waren das Risiko von Umsatzeinbußen, und schließlich ist die Wasserzeichentechnologie gegenüber anderen Schutzverfahren besonders effizient.

Ein vierter Grund wird oft übersehen: IT-Sicherheitsverfahren können als Grundlage für neue Anwendungen bis hin zu neuen Geschäftsmodellen dienen. Man nennt das die *„enabling"-Rolle* von IT-Sicherheit. Dafür sind Public-Key-Infrastrukturen ein Beispiel, ohne die etwa Homebanking oder der elektronische Abschluss von Verträgen gar nicht möglich wäre. Gleichzeitig hilft sie die Vertraulichkeit und Authentizität der Kommunikation in einem Betrieb und nach draußen effizienter zu gestalten.

Investitionen aller Art hängen von dem Gewinn ab, den sie dem Unternehmen bringen, sei es als zusätzliche Erlösquelle („enabling"), als Steigerung bestehender Erlöse oder als Reduktion von Kosten. Diese betriebswirtschaftliche Begründung ist gerade für Investitionen in IT-Sicherheit nicht immer leicht zu erbringen. Die Berechnung von Schäden etwa beruht auf einem Blick in eine ungewisse Zukunft und auf variablen Schätzungen ihres Ausmaßes. Diese Schäden haben also eine Chance, gar nicht erst aufzutreten oder so klein zu bleiben, dass sie nicht wehtun. Investitionsbefürworter und -gegner argumentieren daher oft mit jeweils bevorzugten weichen Eintrittsszenarien, statt mit klaren Verlust- und Gewinnmargen.

Die Verletzung von gesetzlichen Pflichten ist besonders schwer zu quantifizieren. Der zugehörige Schaden wird mit dem vagen Begriff

eines möglichen Reputationsverlusts assoziiert, der nur schwer mit Kostenzahlen zu belegen ist. Hier kann man Beispiele zum Vergleich heranziehen, etwa bei den jüngsten Datenskandalen bei Lidl und der Telekom: Was kostet es eine Firma, Wiedergutmachung zu leisten im Vergleich zu den Investitionen in eine – freilich umfassende – IT-Sicherheit, die den Schadensfall von vorne herein verhindert hätte? Auch Bußgelder können hier auf der Schadensseite verbucht werden.

So musste die Postbank AG ein Bußgeld in Höhe von 120.000 Euro zahlen, weil sie freiberuflichen Handelsvertretern für Vertriebszwecke den Zugriff auf die Kontobewegungsdaten der Postbankkunden ermöglicht hat.[1]

Ein weiteres Beispiel ist die Bußgeldzahlung der Drogeriekette Müller in Höhe von 137.500 Euro. Müller hatte seine Mitarbeiter nach den Gründen für den Krankheitsausfall gefragt und dies in den Personalakten vermerkt, obwohl ein Arbeitgeber solche privaten Informationen nur erfragen darf, um sicherzustellen, dass keine Ansteckungsrisiken bestehen, der Arbeitnehmer seinem Arbeitsplatz gewachsen ist, oder zur Beseitigung von Gefahren am Arbeitsplatz.[2]

In diesem Beitrag geht es nun darum, die – zweifellos berechtigten - weichen Investitionsfaktoren für IT-Sicherheit wie allgemeines Sicherheitsgefühl, Wohlverhalten gegenüber Partnern und Kunden oder Gesetzestreue außer Acht zu lassen. Stattdessen konzentriert er sich auf harte Zahlen von Investitionskosten und stellt sie Schadensgrößen und -wahrscheinlichkeiten, sowie Effizienzgewinnen gegenüber.

Nach einer kurzen Vorstellung der Berechnungsmethoden wird das anhand von konkreten IT-Sicherheitsverfahren, deren Umfeld wir besonders gut kennen, da sie aus unserem Hause stammen, in Schätzungen durchgerechnet, die wir zur besseren Verständlichkeit dieses Textes vereinfacht haben. Die Methode ist aber selbstverständlich auf jedes andere Beispiel anwendbar, und sie kann in größere Detailtiefe hinein verfeinert werden.

[1] Pressemitteilung des Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen vom 07.05.2010
[2] RP-Online (Rheinische Post) vom 11.01.2010

2 Verfahren zur Wirtschaftlichkeitsbetrachtung von IT-Sicherheitsinvestitionen

2.1 Zwischen Pragmatismus und analytischer Investitionskostenrechnung

Die übliche Praxis, Investition von einer exakten Kalkulation ihrer Wirtschaftlichkeit abhängig zu machen, scheint vielfach im Bereich der IT-Sicherheit nicht zu gelten. FUD – Fear, Uncertainty and Doubt: In vielen Unternehmen ist dies immer noch die Methode, um Budgets für IT-Sicherheitsinvestitionen aufzustellen. Die ständig sich verschärfende IT-Sicherheitslage, die auch durch seriöse Veröffentlichungen[3] dokumentiert wird, dient dabei den IT-Sicherheitsbeauftragten bei der Diskussion ihrer Budgets als Hintergrund, um wachsende Ausgaben für IT-Sicherheitsmaßnahmen zu rechtfertigen. Sie argumentieren dabei auch mit der zunehmenden Kritikalität der IT-Infrastruktur, die es zu schützen gilt.

Auch andere wenig analytisch geprägte Verfahren dienen der Budgetfindung in vielen Behörden und Unternehmen. Es werden Trends aufgegriffen, Rest-Budgets ohne konkrete Erfordernisse verplant oder nach einem Sicherheitsvorfall außerordentliche Budgets bereitgestellt.

Dass die aus der Betriebswirtschaftslehre bewährten Verfahren zur Investitionsrechnung nicht systematisch auch für den Bereich der IT-Sicherheit genutzt werden, ist nur auf den ersten Blick verwunderlich, denn in vielen Fällen haben IT-Sicherheitsinvestitionen keinen erkennbaren Ertrag. Zudem ist IT-Sicherheit nicht nur ein technisches Anliegen. Um einen angemessen Schutz der IT-Infrastruktur zu erreichen, muss eine ganzheitliche Betrachtung angestellt werden, die sowohl Netze, Anwendungen, IT-Systeme, die zunehmend mobil genutzt werden, aber auch die räumliche Infrastruktur und die agierenden Personen umfasst. Damit sind erhebliche Investitionen verbunden. Die bauliche Absicherung von Serverräumen, die Installation von Überwachungssystemen mit entsprechendem Meldesystem für ein Firmengelände, die Implementierung von Produktschutzmaßnahmen, die Integration von IT-Sicherheitskonzepten in die Softwareentwicklung, die Schulung aller Betriebsangehörigen und kontinuierliche Awarenesskampagnen kosten viel Geld und ihr Erfolg ist nicht immer unmittelbar monetär messbar. Auch, dass es im Unternehmen zu keinem Sicherheitsvorfall gekommen ist, ist kein Beweis für die Wirtschaftlichkeit der vorgenommenen Sicherheitsinvestitionen.

Der Verzicht auf Wirtschaftlichkeitsberechnungen bei der Entscheidung über Investitionen in die IT-Sicherheit wird jedoch angesichts knapper werdender IT-Budgets und umfassender Controllingbemühungen

[3] Die Berichte des Bundesamtes für Sicherheit in der Informationstechnik dokumentieren regelmäßig in Jahres- und Quartalsberichten die IT-Sicherheitslage https://www.bsi.bund.de/DE/Publikationen/Lageberichte/lageberichte_node.html

vielfach nicht mehr akzeptiert. Auch IT-Sicherheitsverantwortliche müssen zunehmend analytisch fundierte Budgets präsentieren. Und so reicht die Diskussion um geeignete Verfahren inzwischen über den akademischen Diskurs hinaus und wird zunehmend für die betriebliche Praxis relevant.

Das vorliegende Papier greift diese Diskussion auf und veranschaulicht exemplarisch, wie sich Investitionsrechenverfahren für IT-Sicherheitsmaßnahmen anwenden lassen. Es stellt anhand von IT-Sicherheitslösungen, die am Fraunhofer-Institut für Sichere Informationstechnologie entwickelt wurden, insbesondere heraus, dass IT-Sicherheit nicht nur hilft, Schäden und damit Kosten zu vermeiden, sondern auch einen positiven Beitrag zu den Erträgen eines Unternehmens leisten kann.

2.2 Ansätze zur Erfassung der Wirtschaftlichkeit von IT-Sicherheitsinvestitionen

Die Investitionskostenrechnung stellt mehrere Ansätze zur Verfügung, die auch für Wirtschaftlichkeitsbetrachtungen für IT-Sicherheitsinvestitionen genutzt werden:

- Beim Verfahren **Total Cost of Ownership – TCO** werden nicht nur die Anschaffungskosten einer Investition berücksichtigt, sondern alle weiteren direkten und indirekten Kosten für Beschaffung, Installation, Wartung, Schulung, kalkulatorische Anteile für Mieten und Energiekosten. Ziel des Verfahrens ist eine möglichst umfassende Sicht auf die Kosten einer Investition. Für eine Wirtschaftlichkeitsbetrachtung ist die Zusammenstellung der Kosten jedoch nur ein Aspekt, zusätzlich ist auch die Ertragsseite zu berücksichtigen. Die Berechnung des TCO ermöglicht es damit zwar, Entscheidungsalternativen unter Kostengesichtspunkten zu bewerten, soll jedoch die Frage beantwortet werden, welche Investition die wirtschaftlichste ist, muss die Nutzenseite zusätzlich analysiert werden können.

- Die Rendite von Investitionen berücksichtigt das Konzept des **Return-on-Investment – RoI**, der sich als Quotient aus Gewinn und Kapitaleinsatz ergibt. Mit Hilfe dieses Wertes kann die Frage beantwortet werden, wann sich eine Investition amortisiert hat, das heißt, wann die Erträge das eingesetzte Investitionskapital überschreiten.

Wenn es um die Schätzung der Wirtschaftlichkeit von IT-Sicherheitsinvestitionen geht, wird das Konzept des **Return on Security Investment – RoSI** genannt. Es verspricht eine budgetmäßige Kontrolle und eine greifbare Nutzenmessung von IT-Sicherheitsinvestitionen. In die Berechnung des RoSI fließen Kosten für Aufwendungen zur

Beseitigung von Schäden durch IT-Sicherheitsvorfälle ein[4]. Der RoSI ist dann positiv, wenn die vermuteten Einsparungen durch das Vermeiden von Schäden größer sind als die Investition in die IT-Sicherheitsmaßnahme.

Vereinfacht dargestellt, wird der RoSI in folgenden drei Schritten berechnet:

1. Identifikation der zu schützenden Informationsgüter und der möglichen Präventivmaßnahmen

2. Bewertung der Informationsgüter und der Risiken, denen diese ausgesetzt sind

3. Bewertung der Investitionen durch die Berechnung des RoSI als Differenz zwischen den Anschaffungs- und Betriebskosten für Sicherheitsmaßnahmen und der Höhe der vermiedenen Schäden

In dieser Risikobetrachtung[5] liegt das Problem dieses Verfahrens. Es ist für einige Bereiche einfach, Schadenshöhe und Eintrittswahrscheinlichkeiten zu bestimmen, weil gute Erfahrungswerte vorliegen. Zuweilen ist es jedoch aufwendig und nicht immer in der nötigen Detailgenauigkeit möglich, verlässliche Werte zu ermitteln.

Eine weitere methodische Hilfe für die Beurteilung der Wirtschaftlichkeit von IT-Investitionen ist das **WiBe**-Verfahren[6], das für die Bundesverwaltung entwickelt wurde. Dieses Verfahren versucht eine umfassendere Wirtschaftlichkeitsbetrachtung zu unterstützen, indem nicht nur monetär greifbare Faktoren einbezogen werden, sondern auch die Dringlichkeit einer Investition, ihre strategische Bedeutung und externe Effekte. Dieses Verfahren ist grundsätzlich auch für IT-Sicherheitsinvestitionen nutzbar.

Die Betriebswirtschaftslehre stellt somit eine Reihe von bewährten Verfahren zur Verfügung, die jedoch häufig qualitative Kosten- oder Nutzenfaktoren nicht angemessen berücksichtigen. Dies tun Methoden, die eine umfassende Kosten-Nutzenbetrachtung einbeziehen. Alle Verfahren sind grundsätzlich auch für IT-Sicherheitsinvestitionen nutzbar, wenn positive Erträge durch die Investition erzielt werden können.

Zielt eine Investition auf die Vermeidung von Schäden, dann müssen Risikobetrachtungen angestellt werden, die häufig sehr schwierig und aufwendig durchzuführen und damit in ihren Ergebnissen sehr angreifbar und für Entscheider wenig überzeugend sind. Ihren positiven

[4] Berechnungsbeispiele finden sich bei Pohlmann, N.; Wirtschaftlichkeitsbetrachtung von IT-Sicherheitsmechanismen, http://www.internet-sicherheit.de/fileadmin/docs/publikationen/Wirtschaftlichkeit_ITsec_06_03_04.pdf
[5] Zu Verfahren zur Analyse von Risiken liefert die European Network and Information Security Agency – ENISA - eine sehr breite Übersicht: http://www.enisa.europa.eu/act/rm
[6] Zur Methodik dieses Verfahren siehe http://www.wibe.de/

Beitrag leisten diese Verfahren jedoch für die Entscheidungsfindung, indem sie die Verantwortlichen dazu zwingen, eine systematische Analyse der Investitionsentscheidung durchzuführen. Hierdurch werden häufig schon Wirtschaftlichkeitspotentiale oder aber auch Schwachstellen erkannt, die Investitionen plausibel machen können.

2.3 Verfahren zur Unterstützung von Wirtschaftlichkeitsberechnungen

Für IT-Sicherheitsinvestition haben sich einige Verfahren bewährt, die Investitionsrechnungen sinnvoll unterstützen können:

- Penetrationstests ermöglichen die Entdeckung und Bewertung von Schwachstellen und können damit Investitionen in IT-Sicherheitssysteme gezielt steuern.

- Mit Hilfe einer Szenarioanalyse können neue Klassen von Sicherheitslücken identifiziert werden. Dieses Verfahren ist jedoch sehr aufwendig und die Ergebnisse sind häufig nicht konkret genug, um sie für die Budgetplanung zu berücksichtigen.

- Zur Abschätzung des Sicherheitsniveaus und der daraus abzuleitenden Budgetplanung können Verfahren zur Nutzung von Kennzahlen verwendet werden. Hier arbeitet das Fraunhofer Institut für Sichere Informationstechnologie an einem methodischen Ansatz und an der Entwicklung eines Softwaretools, um eine umfassende Kontrolle von Sicherheitsmaßnahmen zu ermöglichen. Das Ergebnis dieser Analysen ist für die Planung von Budgets aber auch für die Kontrolle von Investitionsentscheidungen nutzbar.[7]

[7] Informationen zum Projekt „Entwicklung eines kennzahlenbasierten Monitoring und Reporting Systems zur Unterstützung des Information Security Managements – KennSec“ www.sit.fraunhofer.de

3 Wirtschaftlichkeitseffekte von IT-Sicherheitslösungen

3.1 Überblick

Investitionen in IT-Sicherheitsverfahren haben folgende Wirtschaftlichkeitseffekte[8]:

- Sie minimieren Risiken.
  Hierbei werden keine Effizienzsteigerungen erwartet sondern lediglich mögliche Schäden, die ohne eine Sicherheitslösung entstehen können, reduziert.

- Sie steigern die Effizienz von Prozessen,
  indem sie zur wirtschaftlicheren Gestaltung von Abläufen beitragen. In diesem Fall lassen sich echte Einsparungen durch Investitionsrechenverfahren nachweisen.

- Sie ermöglichen neue Chancen.
  Der Einsatz von IT-Sicherheitslösung unterstützt neue Produktionsverfahren, neue Formen der Kundenansprache, neue Leistungsangebote oder erschließt neue Kundengruppen. Auch hier lassen sich positive Erträge berechnen.

Im Folgenden werden für diese Aspekte Verfahren vorgestellt und vom Fraunhofer-Institut für sichere Informationstechnologie entwickelte Verfahren und Technologien als Beispiele angeführt. Sie zeigen, dass Investitionen in IT-Sicherheit zum wirtschaftlichen Erfolg von Unternehmen beitragen.

3.2 Minimierung von Risiken durch IT-Sicherheitsinvestitionen

3.2.1 Verfahren zur Bewertung dieser Investitionen

Die Analyse und die Steuerung von Risiken sind zentrale Aufgaben aller IT-Sicherheitsverantwortlichen. Gesetzliche Vorschriften (wie AktG, GmbHG, KonTraG) oder aber branchenspezifische Regelungen (wie die von der Bundesanstalt für die Finanzdienstleistungsaufsicht – BaFin - formulierten Mindestanforderungen an das Risikomanagement der Banken – MaRisk) verlangen von den Unternehmen eine angemessene Steuerung ihrer operationellen Risiken, zu denen auch die Risiken aus dem Betrieb von IT-Systemen gehören. So verlangt die BaFin für das Risikomanagement von IT-Systemen: „Die IT-Systeme (Hardware- und Software-Komponenten) und die zugehörigen IT-Prozesse müssen die Integrität, die Verfügbarkeit, die Authentizität sowie die Vertraulichkeit

[8] Siehe hierzu auch Gadatsch, A., Uebelacker, H.; Wirtschaftlichkeitsbetrachtungen für IT-Security-Projekte in Mörike, M., Teufel, S. (Hrsg.); Kosten & Nutzen von IT-Sicherheit, Heidelberg 2006

der Daten sicherstellen. Für diese Zwecke ist bei der Ausgestaltung der IT-Systeme und der zugehörigen IT-Prozesse grundsätzlich auf gängige Standards abzustellen. Ihre Eignung ist regelmäßig von den fachlich und technisch zuständigen Mitarbeitern zu überprüfen." [9]

Hierbei wird explizit auf die Implementierung von Standards etwa zum IT-Sicherheitsmanagement hingewiesen. Dies bedeutet, dass unabhängig von detaillierten Wirtschaftlichkeitsbetrachtungen, die Nutzung von Standardverfahren, etwa nach ISO 27001 oder IT-Grundschutz entsprechend der Vorgaben des Bundesamtes für Sicherheit in der Informationstechnik (BSI), für ein Unternehmen erforderlich sein kann und Auditierungsprozeduren durchgeführt werden müssen.

Häufig werden in gesetzlichen Vorgaben jedoch nur Anforderungen genannt und auf zu ergreifende geeignete organisatorische oder technische Maßnahmen verwiesen. Welche Lösung den Anforderungen entspricht, ist der Beurteilung der Entscheider im Unternehmen oder der Behörde überlassen. In diesem Fall müssen Risiken und die Nutzen verschiedener Lösungsalternativen in der Regel nach wirtschaftlichen Gesichtspunkten abgewogen werden.

3.2.2 Risikominimierung durch Investitionen zum Schutz von Datenbeständen

Um die Wirtschaftlichkeit von Investitionen in IT-Sicherheit zu analysieren, deren Ziel eine Reduktion von Risiken ist, wird der Return on Security Investment – RoSI – berechnet. Hierbei wird eingeschätzt, ob die Aufwendungen für eine Sicherheitsmaßnahme in einem angemessen Verhältnis zur Risikoreduktion durch diese Maßnahme stehen. Das folgende Beispiel, das Kosten für den Verlust von Daten aufgreift, illustriert diese Vorgehensweise:

Ein großer Versicherungsmakler mit 30 Außendienstmitarbeitern, die durchschnittlich Informationen über 5.000 Kunden auf ihren Laptops nutzen, sieht durch die Regelungen der Novellierung des Bundesdatenschutzgesetzes (BDSG) vom 1.9.2009 gestiegene Risiken für die Tätigkeit. Insbesondere die Benachrichtigungspflicht für den Fall, dass personenbezogene Daten Dritten unrechtmäßig zur Kenntnis gelangt sind, könnte erhebliche Kosten für das Unternehmen verursachen, denn pro Jahr gehen 2 Laptops mit Kundendaten verloren.

Als Kostenfaktoren im Falle einer Benachrichtigung von 5.000 Kunden beim Verlust eines Laptops sind zu nennen:

[9] http://www.bafin.de/cln_161/nn_722754/SharedDocs/Veroeffentlichungen/DE/Service/Rundschreiben/2009/rs__0903__marisk__va.html#doc1412762bodyText13

Kostenart	Betrag/Jahr
Verwaltungsaufwand zur Erzeugung des Benachrichtigungsschreibens	5 €/Schreiben = 25.000 €
Porto	2.750 €
Kosten für zusätzliche Kräfte zur Verstärkung der Hotline, da 20 % aller Betroffenen Informationen einfordern: 2 Personen für 2 Wochen nach einem Vorfall, 1.000 €/Woche/Kraft	4.000 €
Umsatzeinbußen, da 2 % der Versicherungsnehmer nach diesem Vorfall ihre Versicherungen kündigen werden (durchschnittlicher Umsatz/Kunde = 1.000 €/Jahr	100.000 €

Damit liegt der Schaden pro Vorfall bei 131.750 Euro. In dieser Rechnung sind Risiken, die schwer zu quantifizieren sind, noch nicht berücksichtigt, etwa Reputationsschäden, Schäden durch die Nutzung des Kundenstamms durch Dritte, Schadensersatzforderungen von Kunden oder die Höhe möglicher Geldbußen durch Verletzung von Pflichten nach dem Bundesdatenschutgesetz (BDSG). Die möglichen Schäden können folglich noch deutlich über den hier aufgeführten liegen und erhebliche wirtschaftliche Auswirkungen für das Unternehmen und ihre Geschäftsführungen (auch diese tragen hohe persönliche Haftungsrisiken!) haben. Verletzungen des BDSG etwa können nach §43 mit einer Geldbuße bis 300.000 € (oder sogar darüber hinaus) geahndet werden.

Die Firma sucht nun zunächst ein Werkzeug zur Nutzung sicherer Passwörter. Bei der Auswahl dieser Hilfsmittel zur Verwaltung von Authentikationsdaten sind jedoch wiederum notwendige Sicherheitseigenschaften der Werkzeuge zu berücksichtigen, denn durch die Konzentration von sensiblen Authentikationsdaten in Verwaltungsprogrammen werden diese zu einem attraktiven Angriffsziel für Hacker. Die Sicherheit der Authentikationsdaten ist eine notwendige Voraussetzung für die Sicherheit vieler weiterer IT-Sicherheitssysteme. Ist diese Voraussetzung nicht mehr erfüllt, dann sind weitere und ggf. teure IT-Sicherheitssysteme nutzlos. Somit helfen solche Lösungen zwar, die Kosten für Helpdesk und Produktivitätsausfall zu reduzieren, sie garantieren jedoch keine Reduktion der Kosten, die im Zusammenhang mit IT-Sicherheitsvorfällen entstehen. Deshalb ist es unbedingt notwendig, dass die Verwaltungsprogramme bekannte Angriffe und weit verbreitete Angriffe abwehren. Dadurch dass die konventionellen Produkte zur Verwaltung von Authentikationsdaten allesamt auf passwort-basierte Verschlüsselung setzen, können diese meistens mit Wörterbuchangriffen erfolgreich angegriffen werden.

Die von Fraunhofer Institut für Sicher Informationstechnologie SIT entwickelte Software MobileSitter[10] ist die einzige am Markt verfügbare Lösung, die ihren Benutzern Resistenz gegen Wörterbuchangriffe bietet und somit hilft, obige Risiken zu vermeiden. MobileSitter erlaubt die Verwaltung von Authentikationsdaten auf Mobilgeräten, so dass ein Benutzer seine Passwörter stets verfügbar hat. Somit ergeben sich Kosteneinsparungen im Bereich Produktivität und Helpdesk als auch im Bereich der Konsequenzen von IT-Sicherheitsrisiken. Mit der vergleichbar geringen Investition in eine sichere Verwaltung von Authentikationsdaten als Basissicherung können sowohl Unternehmen als auch Privatpersonen Risiken und größere potenzielle Schäden vermeiden.

Diese Lösung soll durch eine Festplattenverschlüsselung ergänzt werden, um sicherzustellen, dass die Kundendaten auch im Fall des Verlusts eines Laptops vor dem Zugriff Dritter geschützt sind.

Die Wirtschaftlichkeitsberechnung unter Nutzung des RoSI Schemas zeigt, dass die geplante Investition zu einer deutlichen Risikominderung führt, die den Aufwand für die Einführung und Administration der Software wirtschaftlich lohnend macht:

Kalkulation: Festplattenverschlüsselung plus Tool für Handling sicherer Passwörter			
Zeitspanne	Jahr 1	Jahr 2	Jahr 3
Kosten MobileSitter: Lizenz 9,90 €/Laptop/Jahr	297 €	297 €	297 €
Kosten Festplattenverschlüsselung Lizenz 80 €/Laptop einmalig, 25 % für Updates in den Folgejahren	2.400 €	600 €	600 €
Kosten Administration der Lösung (pro Laptop 2 Admin Std/Jahr = 160 €)	4.800 €	4.800 €€	4.800 €€
Ersparnisse durch IT-Sicherheitsinvestition	263.500 €	263.500 €	263.500 €
RoSI	256.003 €	512.006 €	775.506 €

Welche Kosten durch Datenpannen verursachen werden können, zeigen auch folgende Beispiele:

Der Verlust einer Bandsicherung im Jahr 2009 betraf 51.000 Daten britischer Kunden (und mehr als 1 Mio. Datensätze afrikanischer

[10] MobileSitter ist ein Tool zum Managen von Passwörtern. Es unterstützt Benutzer ihre Geheimkombinationen —egal ob Passwort, PIN oder TAN— auf dem eigenen Mobiltelefon zu managen. Informationen: www.mobilesitter.com

Kunden) des Versicherungskonzerns Zurich Financial Services (ZFS)[11]. Dadurch entstanden dem Konzern nicht nur Kosten für die Benachrichtigung ihrer Kunden und weitere Verwaltungsaufwendungen sondern die britische Finanzaufsichtsbehörde FSA verhängte auch eine Strafe von 2,3 Mio. Pfund (2,75 Mio. Euro)[12].

Der Deutschen Bank wurde Ende 2002 durch die US-Börsenaufsicht SEC eine Strafzahlung in Höhe von 1,65 Millionen US-Dollar auferlegt. Hintergrund: Anlageberater des Unternehmens hatten (entgegen den unternehmenseigenen Vorgaben) E-Mails nur so unzureichend gespeichert, dass dadurch Ermittlungsverfahren zu bestimmten umstrittenen Anlageempfehlungen erschwert bzw. vereitelt worden sind.[13]

Dass besondere Schutzmaßnahmen erforderlich sind, um die Datenbestände und das Know-How eines Unternehmens zu sichern, weist die Studie der KMPG zur Computerkriminalität nach. Gute Schutzkonzepte, ihre Anwendung und Kontrolle können betriebliche Verluste in Millionenhöhe vermeiden.[14].

3.3 Effizienzsteigerung durch Nutzung innovativer Technologien und Verfahren der IT-Sicherheit

3.3.1 Return-on-Investment - Betrachtungen für IT-Sicherheitsinvestitionen

In der Optimierung von Prozessabläufen und Verfahren stecken hohe Wirtschaftlichkeitspotentiale, die durch die Implementierung von Sicherheitslösungen realisiert werden können. Für die Wirtschaftlichkeitsberechnungen werden klassische Investitionsrechenverfahren genutzt, wie sie etwa zur Bestimmung des Return-on-Investment (RoI) angewandt werden.

Häufig reicht jedoch auch schon ein Vergleich der Aufwendungen eines bestehenden Verfahrens mit einer optimierten Lösung, um den Nachweis der Wirtschaftlichkeit einer Investition zu erbringen.

Im Folgenden wird anhand einiger Beispiele für IT-Sicherheitsinvestitionen aus unterschiedlichen Anwendungsgebieten gezeigt, wie die Einführung innovativer IT-Sicherheitstechnologien die Effizienz von Prozessen erhöhen kann.

[11] http://www.handelszeitung.ch/artikel/Unternehmen-AWP_ZFS-mit-Datenpanne-in-Suedafrika_625524.html
[12] http://www.wirtschaftsblatt.at/home/boerse/binternational/435264/index.do
[13] E-Mail Archivierung und ihre rechtlichen Grundlagen - zur Schaffung eines rechtlichen Problembewusstseins (2. Teil der neuen Serie der IT-Recht Kanzlei zur E-Mailarchivierung und IT-Richtlinie) von RA Max-Lion Keller, LL.M. (IT-Recht) und Patrick Prestel, 27.05.2010, IT-Recht Kanzlei München
[14] http://www.kpmg.de/Presse/21498.htm

3.3.2 Beispiele für Effizienzsteigerungen

3.3.2.1 Beispiel 1: Benutzerorientierte Lösungen für das Passwort-Problem

Der sichere Umgang von Benutzern mit Authentifizierungsdaten wie Passwörtern und PINs ist eine notwendige Bedingung für IT-Sicherheit, sowohl im professionellen als auch im privaten Umfeld. Leider überfordern die Vielfalt der von einem Benutzer benötigten Passwörter und die Sicherheitsanforderungen an diese Passwörter nicht nur IT-unerfahrene Benutzer. Benutzer benötigen Hilfsmittel, um mit ihrem alltäglichen Passwortdilemma klar zu kommen. Diese Hilfsmittel erhöhen nicht nur die Sicherheit, sondern stellen auch eine deutliche Steigerung der Effizienz im Zugang zu IT-Anwendungen dar, wie folgendes Beispiel unter Nutzung des vom Fraunhofer SIT entwickelten Systems MobileSitter zeigt, eine – wie bereits in Kapitel 3.2.2 beschriebene – leistungsstarke Lösung zum Passwortmanagement.

Vergessene Passwörter implizieren in Unternehmen hohe Kosten für Helpdesk und Produktivitätsausfall. Laut Informationen von Scriptlogic ist bei einem vergessenen Passwort mit einem Produktivitätsausfall von durchschnittlich 20 Minuten zu rechnen.[15] Nach Angaben von Psylock fallen je vergessenem Passwort Kosten zwischen 25 Euro und 45 Euro an, was sich in einem Unternehmen je Benutzer auf jährliche Kosten zwischen 110 Euro und 190 Euro aufsummiert.[16]

Kalkulation: Nutzung des MobilSitters als Tool zum Handling sicherer Passwörter	
Unternehmen mit 2000 Mitarbeitern	
Kosten MobileSitter: Lizenz 9,90 €/Jahr	19.800 €
Kosten für Nutzerunterstützung: 5 AdminTage/Jahr – interner Tagessatz 640 €	3.200 €
Kosten für Nutzerunterstützung bei vergessenen Passwörtern = 100 €/Nutzer	200.000 €
Ersparnisse durch IT-Sicherheitsinvestition	166.200 €

[15] Scriptlogic: The True Cost of Password Management. 2008, http://www.scriptlogic.com/landing/roi/helpdesk-authority/ScriptLogic-The-True-Cost-of-Password-Management.pdf

[16] Psylock / D. Bartmann: Tippverhaltensbiometrie Psylock, 2008

3.3.2.2 Beispiel 2: Sicherheitslösung für innovatives Gebäudemanagement

Die Optimierung von Geschäftsprozessen ist eine der Hauptanstrengung im Tagesgeschäft von Unternehmen. Effiziente Prozesse steigern die Produktivität und schützen das Kerngeschäftsmodell vor äußeren Einflüssen. Oftmals werden IT- und Informationssicherheit dabei als limitierende Faktoren beim Erreichen dieses Ziels wahrgenommen.

Fraunhofer SIT hat eine Sicherheitslösung entwickelt, die die Integration von Komponenten aus verschiedenen Bereichen wie z.B. Facilitymanagement, Gebäudesteuerung und Büroanwendungen zulässt. Dieser Ansatz bietet eine innovative Basis für bereichsübergreifende Prozessoptimierungen mit dem Effekt der Erhöhung des Sicherheitsniveaus.[17]

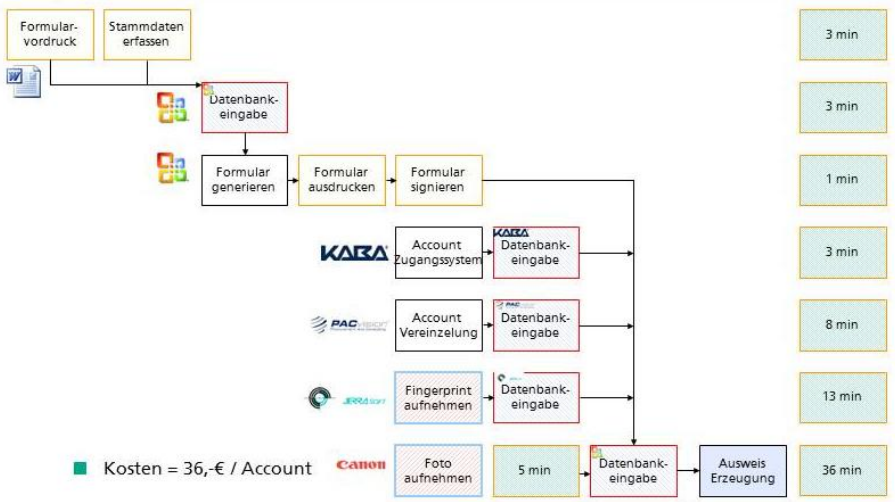
Zum Beispiel kann die Implementierung des Zugangsprinzips „eine Person eine Karte/Schlüssel nicht nur vermeiden, dass verschiedene Systeme zur Kontrolle des Zugangs zu Gebäuden - aber auch zu digitalen Systemen in Gebäuden - dezentral organisiert werden müssen. Die Integration der Systeme durch facilityboss bündelt deren Funktionen und stellt diese mit einem systemüberspannenden Sicherheitskonzept dem Endnutzer auf einer integrierten Weboberfläche als Dienst zur Verfügung. Für den Anwender verbessern sich Komfort, Sicherheit und Qualität der Informationen.

Mit der Nutzung von facilityboss ist es möglich

- IT-Systeme zu bündeln und webbasiert zu realisieren,
- Den Zugang zu digitalen aber auch physikalischen Ressourcen über eine Karte/Token zu ermöglichen,
- ggf. Zertifikate zur sicheren Identifizierung zu genutzen,
- durchgängige Security Policy zu etablieren.

Wie unter Einsatz von facilityboss Effizienzpotentiale erschlossen werden, zeigt das Beispiel eines optimierten Accounting-Prozesses durch die Integration aller Komponenten. Ohne facilityboss ergeben sich folgende Abläufe und Zeiten:

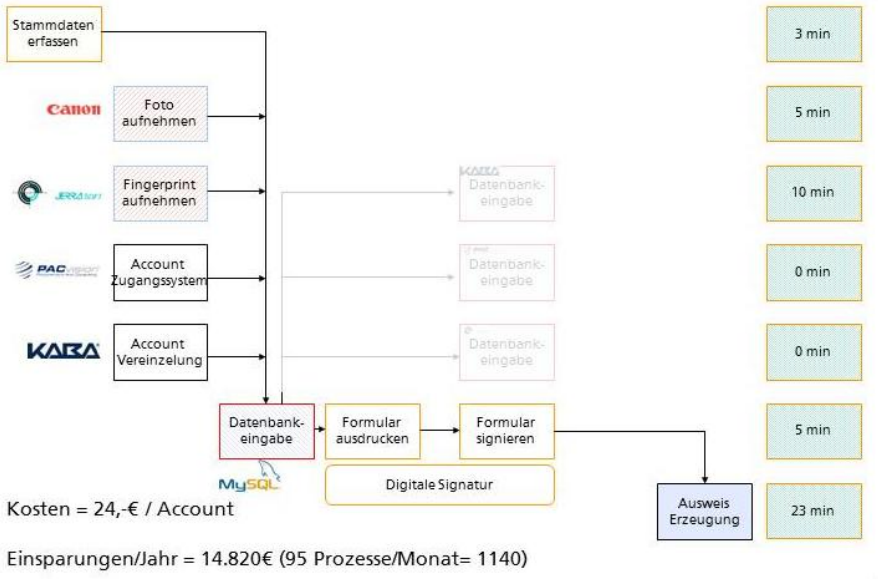
[17] Mehr Informationen zu facilityboss: http://www.facilityboss.biz/



Ohne Nutzung von facilityboss fallen 36 Euro für einen Account an.

Facilityboss leistet durch seine Integrationsschicht, dass auf die Redundanz von systemeigenen Datenbanken verzichtet werden kann. Diese laufen als Backupsysteme im Hintergrund weiter, werden für den Accountingprozess aber nicht direkt benötigt. Die Integration der Komponenten optimiert den Prozess, da alle personenbezogenen Daten nun von facilityboss erhoben und dann an die Systeme weitergeleitet werden. Doppeleinträge werden vermieden, Datenbankinkonsistenzen aufgelöst und das Controlling & Reporting vereinfacht.

Bei Nutzung von facilytyboss gestalten sich der Prozess und die benötigten Zeiten wie folgt:



Hier haben sich die Kosten für einen Account auf 24 Euro verringert. Die Zusammenstellung der Verfahrenskosten ergibt ein Optimierungspotential unter Nutzung von facilityboss von 14.976 Euro pro Jahr und einen Amortisationszeitraum für die Investition von 3,34 Jahren.

Optimierung eines Accounting Prozesses in einem offenen Rechenzentrum

Durchgerechnetes Beispiel eines optimierten Accounting Prozesses:
Integrieren folgender Komponente:
1. Personenstammdatenbank
2. Zugangskontrollsystem (Karte)
3. Vereinzelungsanlage
4. Fingerprintsystem
5. Foto

	Verfahren ohne facilityboss	**Verfahren mit facilityboss**
Zeitaufwand Erstellung Account	36 €	24 €
Kosten/Woche (24 Account/Woche)	864 €	576 €
Ersparnis/Woche		288 €
Optimierungspotential/Jahr		**14.976 €**
Investition (25k Kern, 25k Integration)		**50.000 €**
Amortisation nach Jahren		**3,34**

3.3.2.3 Beispiel 3: Lösung zur Nutzung digitaler Wasserzeichen

Am Fraunhofer-SIT wurde ein Verfahren für Container-Wasserzeichen entwickelt[18]. Hiermit lassen sich große Datenmengen kostengünstig und ohne merkliche Zeitverzögerung mit Wasserzeicheninformationen markieren. So können zum Beispiel nach dem Kauf in einem Online-Shop während des Downloads Informationen wie die Rechnungsnummer unsichtbar, unhörbar und untrennbar eingebettet werden. Mit diesem Verfahren ergeben sich gegenüber herkömmlichen Verfahren zur individuellen Markierung digitaler Medien erhebliche Einsparungen, wie das Beispiel zeigt:

[18] Informationen zu diesem Verfahren:
http://www.sit.fraunhofer.de/Images/merit_container_de_en_tcm105-92888.pdf

Beispiel: Kleiner Onlineshop mit nur jeweils einem aktiven Kunden	
Serverkosten Euro/ Monat	150 €
Markierungsaufkommen/ Spielminuten pro Minute	100
Standardwasserzeichen/ Spielminuten pro Minute	20
Serveranzahl	5
Kosten	750 €
Containerwasserzeichen/ Spielminuten pro Minute	3.000
Serveranzahl	1
Kosten	150 €
Einsparung:	**600 €**

Beispiel: Großer Onlineshop mit bis zu 100 aktiven Kunden	
Serverkosten Euro/ Monat	150 €
Markierungsaufkommen/ Spielminuten pro Minute	10.000
Standardwasserzeichen/ Spielminuten pro Minute	20
Serveranzahl	500
Kosten	75.000 €
Containerwasserzeichen/ Spielminuten pro Minute	3.000
Serveranzahl	25
Kosten	3.750 €
Einsparung:	**71.250 €**

3.3.2.4 Beispiel 4: ArchiSoft – Langzeitbeweiswerterhaltung digital signierter Dokumente

Elektronische Geschäftsprozesse in Wirtschaft und Verwaltung brauchen sichere und dauerhafte elektronische Signaturen für Dokumente – nur so wird eine papierlose und dennoch revisionssichere Abwicklung erst möglich.

Zum Teil sind extrem lange Aufbewahrungspflichten solcher Dokumente vom Gesetzgeber vorgeschrieben, zum Beispiel 30 Jahre im Gesundheitswesen. Das gilt auch für die elektronischen Signaturen – diese aber können veralten, »verblassen«, weil sie eventuell mit Verfahren erzeugt wurden, die aufgrund des technischen Fortschritts nicht mehr sicher genug sind. In einem Streitfall kann dies dazu führen, dass die Signatur vor Gericht ihren kryptographischen Beweiswert verliert. Mit »ArchiSoft« jedoch behalten Signaturen und damit Dokumente ihren Wert und können in Streitfällen weiter zuverlässig vor Gericht eingesetzt werden.

Das vom Fraunhofer-Institut SIT entwickelte Softwarepaket ArchiSoft aktualisiert Signaturen bei Bedarf, bevor sie veralten. Besonders kostengünstig wird es durch die Einbindung in vorhandene Dokumentenmanagement-Systeme (DMS): Es bündelt vorhandene Dokumente samt ihren Signaturen zu einem Baum und teilt ihnen gemeinsam eine neue, schwerer als bisher zu brechende Signatur zu, statt

jedes einzeln zu signieren.[19] Das Verfahren ist sehr kosteneffizient, verglichen mit der Zeitstempelung jedes einzelnen Dokuments. Als Beispiel betrachte man ein Dokumentenvolumen von 1000 Dokumenten pro Tag bei Zeitstempelkosten von 1ct pro Zeitstempel:

Ohne ArchiSoft betragen die Kosten bei 250 Arbeitstagen pro Jahr:

250 Tage * 10000 Dokumente * 1ct = 25.000 Euro

Mit ArchiSoft betragen die Kosten:

250 Tage * 1ct = 2,50 Euro

Die Kosten, die ArchiSoft für Zeitstempel erfordert sind somit praktisch zu vernachlässigen. Die Kosten für den ArchiSoft-Server amortisieren sich innerhalb weniger Monate.

3.4 Neue Chancen durch den Einsatz von IT-Sicherheitsverfahren und Technologien

3.4.1 IT-Sicherheit für neue Prozesse und Leistungsangebote

IT-Sicherheitsverfahren sind häufig die Grundvoraussetzung für die Implementierung neuer Prozesse und Verfahren. Ein Return-on-Investment ist hier indirekt dadurch messbar, dass die Ertragskraft des Unternehmens deutlich gestärkt wird, indem neue Leistungsangebote für Kunden realisiert oder aber auch interne Abläufe neu gestaltet werden können.

IT-Sicherheitstechniken in diesem Kontext sind Basistechnologien wie Firewallsysteme oder andere Security-Bausteine, ohne die keine internet-basierten Anwendungen möglich sind. So waren PIN-TAN-Verfahren Innovationen, die etwa Banken ganz neue Leistungsangebote ermöglichten.

3.4.2 Enablingprojekte zur Erschließung von Wirtschaftlichkeitspotentialen

3.4.2.1 Beispiel 1: Implementierung einer PKI zur sicheren Kommunikation

Die Implementierung einer Public-Key-Infrastruktur ist eine Investition, die einen hohen Aufwand erfordert. Gleichzeitig bietet sie als Basisinfrastruktur viele Nutzungsoptionen und vereinfacht den Zugriff auf IT-Ressourcen erheblich. Sie leistet damit einen großen Beitrag zur Usabilitiy von IT-Sicherheitsfunktionen.

[19] Mehr zur ArchiSoft Lösung und zum Verfahren:
http://www.sit.fraunhofer.de/forschungsbereich/tad/archisoft.jsp

Dass sich eine Einführung einer PKI auch rechnet, zeigt das Beispiel der Fraunhofer-Gesellschaft, die eine auf Chipkarten (Fraunhofer-Smartcard) basierende PKI für alle Fraunhofer-Mitarbeiter, mit vielfältigen Einsatzmöglichkeiten und umfassenden Service-Angeboten betreibt.

Die Fraunhofer Service CA, die von den Fraunhofer-Instituten SIT und IOSB betrieben wird, ist für die Zertifizierung von Systemen und Diensten der Fraunhofer-Gesellschaft verantwortlich, und stellt darüber hinaus einen eigenen Dienst für externe Partner zur Verfügung (»PKI-Contacts«), um diesen einen einfachen Weg zur verschlüsselten Kommunikation mit Fraunhofer-Mitarbeitern zu ermöglichen.

Eine Übersicht über die Kosten gibt folgende Zusammenstellung:

Investitionen			
Investitionskosten pro AP	Menge	Projektpreis in Euro	Gesamtprojekt-preis in Euro
Kosten pro Leser inkl. Smartcard	17.000	20	340.000
Lizenz für die Software inkl. Erstausstattung mit Zertifikaten	17.000	50	850.000
Summe		**70**	**1.190.000**
Investitionskosten Sonstiges			
Bauliche Maßnahmen zum Aufbau zweier redundanter Trustcenter	2	50.000	100.000
Kosten für redundante Serverinfrastruktur	2	30.000	60.000
CA Lizenzen	3	5.000	15.000
Weitere Softwarelizenzen + Softwareentwicklungskosten	2	300.000	600.000
Hardware Security Modul	2	7.000	14.000
RA Smartcard Drucker inkl. Laminiereinheiten	4	8.500	34.000
Summe			**823.000**
Gesamtinvestition	**2.013.000**		

Betriebskosten			
Personalaufwand Betrieb in Personenmonate	€/Monat	PM	
laufenden Zertifikatsproduktion	7.400	36	266.400 €
Aufrechterhaltung des Betriebs (SW-Updates, Backups etc.)	7.400	24	177.600 €
User-Support- und Helpdesk	8.250	40	330.000 €
Summe		**100**	**774.000 €**
Sonstiger Aufwand Betrieb			
Wartung- und Anpassung Software			100.000 €
Lizenz- und Supportvertragskosten			130.000 €
Ersatzkarten			45.000 €
Erweiterungen/Ersatz Serverinfrastruktur			40.000 €
Verbrauchsmaterial (Toner, Papier, etc)			15.000 €
Porto + Verpackung			15.000 €
Reisekosten			9.000 €
Summe			**354.000** €
Gesamtbetriebskosten/ Jahr	**1.128.000** €		

Diesen Kosten stehen Erträge Kosteneinsparungen durch Prozessoptimierung gegenüber:

So sind **Ersparnisse für ein vereinfachtes Passwort-Handling** in einem deutlich reduzierten Aufwand des Helpdesks sichtbar. Wenn die oben angeführten Kosten für vergessenes Passwort unterstellt werden, spart die Fraunhofer Gesellschaft allein 1.87 Mio. Euro pro Jahr durch die Einführung der Smartcard (bei zum Zeitpunkt des Projektstarts 17.000 Mitarbeitern und Kosten für vergessenen Passwörter von 110 Euro/Mitarbeiter, s.o.). Damit wird bereits ab dem dritten Jahr ein positiver RoI erzielt.

RoI – Betrachtungen (jeweils Euro – Werte)				
	Jahr 1	Jahr 2	Jahr 3	Jahr 4
Investitionskosten	2.013.000			
laufende Kosten/Jahr	1.128.000	1.128.000	1.128.000	1.128.000
Kostensenkung Help Desk durch smartcard-basiertes Zugangssystem	1.870.000	1.870.000	1.870.000	1.870.000
RoI	-1.271.000	-529.000	213.000	955.000

Hier zu kommen deutliche Einsparungen durch die Karte, die nun das einzige Zugangsinstrument für alle Anwendungen und die Infrastruktur ist (etwa für Gebäude, Aufzüge, Kostenabrechnung in der Betriebskantine etc.).

Eine Public-Key-Infrastruktur macht jedoch nicht nur Authentifizierungsprozesse effizienter, sondern sie fungiert als Basistechnologie für die Neugestaltung von betrieblichen Prozessen. Hier liegt ein großes Effizienzpotential in der Möglichkeit, papiergebundene Verfahren elektronisch abwickeln zu können.

Es gibt Verfahren, die eine persönliche Unterschrift tragen müssen. Dazu gehören in der Fraunhofer Gesellschaft die Beantragung von Urlaub und das Ausfüllen der Zeiterfassungsbögen. Diese Verfahren können bei der Nutzung einer PKI nun medienbruchfrei elektronisch durchgeführt werden.

Die Einführung des webbasierten Zeiterfassungsbogens (WebZEB), der monatlich von allen Mitarbeitern erstellt werden muss, erspart der Fraunhofer Gesellschaft ca. 500.000 Euro pro Jahr. Dieser Ersparnis stehen einmalige Entwicklungskosten von 470.000 Euro und jährlichen Betriebskosten von 243.000 Euro für diese Anwendung gegenüber:

Kostenreduktion durch die Einführung von WebZEB in der Fraunhofer Gesellschaft	Jahr 1	Jahr 2	Jahr 3	Jahr 3
Entwicklungskosten	470.000			
Betriebskosten		243.500	243.500	243.500
Kosten	470.000	243.500	243.500	243.500
Ersparnis in den Instituten: 2 Tage/Monat/Institut durch den Verzicht auf die zentrale Erfassung der Papierbögen durch die Personalsachbearbeitung: 2 Tage bei 60 Instituten und einem internen Tagessatz von 500 €:		720.000	720.000	720.000
Ersparnis in der Zentralverwaltung durch den Verzicht auf eine zentrale Erfassung: 20 PT/Jahr (interner Tagessatz 500 €)		10.000	10.000	10.000
Papierkosten (Annahme: 80% aller MA drucken eine zusätzliche Kopie ihres Bogens, Papierkosten 2 cent/Blatt)		7.344	7.344	7.344
Raumkosten (Verzicht auf Archiv=20qm bei 10€ Miete/qm)		2.400	2.400	2.400
Ersparnis	-470.000	496.244	496.244	496.244

Wenn nun den Kosten der PKI (neben den Ersparnissen beim Help Desk durch ein einfacheres Zugangssystem zu IT-Anwendungen) auch noch die Ersparnisse durch die Einführung des papierlosen WebZEB Prozesses gegenübergestellt werden, ergibt sich bereits im 3. Jahr ein Return on Invest (RoI):

RoI - Betrachtungen				
	Jahr 1	Jahr 2	Jahr 3	Jahr 4
Investitionskosten	2.013.000			
laufende Kosten/Jahr	1.128.000	1.128.000	1.128.000	1.128.000
Kostensenkung Help Desk durch smartcard-basiertes Zugangssystem	1.870.000	1.870.000	1.870.000	1.870.000
Kostenreduzierung durch WebZEB	-470.000	496.244	496.244	496.244
RoI	-1.741.000	-502.756	735.488	1.973.732

Der RoI wird bei Betrachtung weiterer Anwendungen noch deutlich höher ausfallen. So wird neben der WebZEB Lösung auch der Prozess der Beantragung und Genehmigung von Urlaub in der Fraunhofer-Gesellschaft nach Einführung der PKI online abgewickelt. Auch dies erspart gegenüber der papiergebunden Version jedes Jahr mehrere hunderttausend Euro.

Weiterhin werden Personalvorgänge nun per E-Mail und elektronischem Dokumentenaustausch durchgeführt. Eine erhebliche Beschleunigung dieser Prozesse, die häufig zeitkritisch sind und für die enge Fristen eingehalten werden müssen, ist die Folge.

Dieses Beispiel zeigt, dass auch eine aufwendige IT-Sicherheitsinvestition – wie die Einführung einer Public-Key-Infrastruktur – schnell einen Return-on-Investment erwirtschaften kann.

3.4.2.2 Beispiel 2: Erschließung von Wachstumspotentialen durch Nutzung innovativer Wasserzeichentechnologien

Das folgende Beispiel illustriert, dass nicht nur interne Prozesse unter Nutzung innovativer Sicherheitslösungen wirtschaftlicher gestaltet, sondern auch neue Märkte erschlossen werden können.

Die Medienindustrie, insbesondere die Musikindustrie, hat lange Zeit durch die Verwendung von proprietären Digital Rights Management-Lösungen ihren Kundenkreis beschränkt. Denn durch solche DRM - Lösungen sind Kunden an Betriebssysteme oder Abspielgeräte gebunden, die die entsprechenden DRM-Formate unterstützen. Kunden, die ein anderes Betriebssystem verwenden, können nicht erreicht werden.

Digitale Wasserzeichen bieten hier einen anderen Ansatz: Die Verfahren betten Informationen untrennbar und transparent in die Medien ein, die verkauft werden. So wird eine Nachverfolgung von Rechteverstößen ermöglicht. Das Medienformat kann aber generisch und somit auf beliebigen Betriebssystemen und Geräten anspielbar sein. Beispiele sind hier mp3 - Musikstücke oder MPEG-2-Videos.

So können durch die Implementierung von Wasserzeichenlösungen Kunden in Märkten gewonnen werden, in denen die Rechteinhaber einen Schutz ihrer Werke fordern, entsprechende Lösungen bislang aber fehlen. Ein Beispiel wäre das folgende Szenario, in dem ein Anbieter 10.000 Kunden hat, die über ein DRM System an Windows gebunden sind. Wenn er davon ausgeht, dass er dadurch 10 % Kunden nicht erreicht, die Linux verwenden, kann er bei einem durchschnittlichen Umsatz von 100 Euro pro Kunden ein Wachstum von 100.000 Euro erzielen.

Potential	
Anzahl Kunden	10.000
Umsatz pro Kunde	100 €
Profil potentieller Kundenstamm/ genutzte Betriebssysteme	
Erwarteter Anteil Linux-Nutzer in Prozent	10
Wachstumspotential durch Nutzung von Wasserzeichen	100.000 €

4 Fazit und Ausblick

Unter dem gestiegenen Kostenbewusstsein müssen auch IT-Sicherheitsverantwortliche stärker als je zuvor ihre Budgets rechtfertigen. So wird die Zahl der Unternehmen, die nicht angeben können, wie viel sie für IT-Sicherheit ausgeben, in Zukunft abnehmen. Aktuell weist die KES-Studie 2010 einen Anteil von immerhin 30 % der Großunternehmen aber nur 12 % der KMUs aus, die über ermittelte Werte für ihre IT-Sicherheitsaufwendungen verfügen. Nur 8 % der befragten Unternehmen verfügen über ein IT-Sicherheitsbudget.[20] Der Trend, Budgets zuzuweisen und nachzuverfolgen, den große Unternehmen vorgeben, wird auch für mittelständische Unternehmen verstärkt umgesetzt werden. Investitionen in IT-Sicherheit müssen ihre Wirtschaftlichkeit nachweisen.

Die dargestellten Beispiele haben gezeigt, dass dies durchaus möglich ist:

- IT-Sicherheitsverfahren reduzieren operationelle Risiken. Dabei sind für viele Investition nicht einmal umfassende Risikobetrachtungen erforderlich. Häufig lassen sich die Schadenshöhe durch einen Sicherheitsvorfall und die Eintrittswahrscheinlichkeiten ganz pragmatisch bestimmen. Hier fällt es dann auch nicht schwer, wirtschaftliche Effekte durch eine Investition nachzuweisen.

  Jedoch auch für Investitionen mit sehr komplexen Auswirkungen und aufwendigeren Risikobetrachtungen sollte nicht auf eine ökonomische Analyse verzichtet werden. Hierfür stehen komplexe stochastische Verfahren zur Verfügung. R.Rumpel und R. Glanze etwa beschreiben Beispiele zur Bewertung von Bündeln von Investitionsalternativen und zur differenzierten Betrachtung von Ersparnissen durch IT-Sicherheitsinvestitionen.[21] Denn selbst wenn die Ergebnisse diskutabel sind, werden Investitionsalternativen systematisch betrachtet und bewertet und IT-Sicherheitsrisiken transparenter. Die Entscheidung ist in jedem Fall fundierter.

- Durch IT-Sicherheitsinvestitionen lassen sich deutliche Einsparpotentiale durch Optimierung von Sicherheitsprozessen erzielen. Wie die angeführten Beispiele zeigen, lassen sie sich durch die Nutzung klassischer Investitionsrechenverfahren, mit der Lösungsalternativen bewertet werden, auf ihre Ertragsrelevanz hin analysieren.

- Zudem bieten IT-Sicherheitsverfahren vielfältige Chancen als Enabling - Technology zur Prozessoptimierung und Erschließung

[20] Lagebricht zur IT-Sicherheit, Kes – Die Zeitschrift für Informationssicherheit, Nr. 4, August 2010, S. 34
[21] Rumpel, Rainer, Glanze, Richard, Verfahren zur Wirtschaftlichkeitsanalyse von IT-Sicherheitsinvestitionen, http://www.e-journal-of-pbr.info/downloads/wirtschaftlichkeititsecurityrumpelglanze.pdf

neuer Märkte, so dass selbst aufwendige IT-Sicherheitslösungen wirtschaftlich sinnvoll sein können.

Auch wenn der Aspekt der Risikominimierung bei IT-Sicherheitsinvestitionen immer stark im Blickpunkt der Betrachtung stehen wird, wird in Zukunft der wertschöpfende Aspekt von Sicherheitsverfahren und -technologien an Bedeutung gewinnen und ihr Beitrag zum wirtschaftlichen Erfolg eines Unternehmens zunehmend wichtiger werden.

5 Das Fraunhofer – Institut für Sichere Informationstechnologie

Das Fraunhofer-Institut für Sichere Informationstechnologie (SIT) entwickelt Konzepte zur Gestaltung sicherer IT-Strukturen und Soft- und Hardware zur Absicherung von Informationen, Geräten, Diensten und Netzen. Als Spezialist für IT-Sicherheit entwickelt das SIT unmittelbar einsetzbare Lösungen, die vollständig auf die Bedürfnisse der Auftraggeber ausgerichtet sind. Zu den Arbeitsgebieten zählen unter anderem Aufbau sicherer Organisationsstrukturen und Prozessabläufe, Publik Key Infrastrukturen, Biometrie, Internetsicherheit, Identitätsmanagement und die Sicherheit von elektronischen Ausweisen als auch Mobilfunk, Sensornetze, eingebettete Systeme, Gebäudesysteme.

Wirtschaftliche Aspekte spielen bei den Projekten des Instituts immer eine große Rolle, denn ohne den Nachweis, dass neue Verfahren eine Effizienzsteigerung bewirken, wird keine Akzeptanz erzielt. Die Forscher des Fraunhofer SIT orientieren sich in ihren Entwicklungsarbeiten an der Leitlinie, theoretische Erkenntnisse in praxistaugliche Lösungen umzusetzen. Sie werden aber auch explizit in Projekten tätig, bei denen es um Risikobewertungen oder aber Kosten-Nutzen-Betrachtungen für existierende Verfahren oder Investitionsentscheidungen geht. Hierfür verfügen sie über breites Methoden-Know-How, das sie in Beratungsprojekte bei Behörden und Unternehmen einbringen und so dazu beitragen, dass die dort genutzten Verfahren nicht nur sicher sondern auch wirtschaftlich sind.

6 Weiterführende Literatur

Gadatsch, A., Uebelacker, H.; Wirtschaftlichkeitsbetrachtungen für IT-Security-Projekte in Mörike, M., Teufel, S. (Hrsg.); Kosten & Nutzen von IT-Sicherheit, Heidelberg 2006

Gadatsch, A., Mayer, E.; Masterkurs IT-Controlling, Wiesbaden 2006

Rumpel, R., Glanze, R., Verfahren zur Wirtschaftlichkeitsanalyse von IT-Sicherheitsinvestitionen, http://www.e-journal-of-pbr.info/downloads/wirtschaftlichkeititsecurityrumpelglanze.pdf