T.I.S.P. Community Meeting 2010

Köln, 03./04.11.2010

Mechthild Stöwer
Fraunhofer-Institut Sichere Informationstechnologie - SIT

Workshop A:
Wirtschaftlichkeitsbetrachtungen zu IT-Sicherheitsinvestitionen

Workshop A:
Wirtschaftlichkeitsbetrachtungen zu IT-Sicherheitsinvestitionen
Agenda

- Warum in IT-Sicherheit investieren?
- Beispielrechnungen
- Alternativen?
- Einschätzung der Wirtschaftlichkeitsbetrachtung aus der Sicht der Praxis - Workshopdiskussion

Security Investment - empirisch

Studie der Gartner Group:

Ausgaben für IT-Sicherheit liegen bei durchschnittlich 3-5% des IT-Budges (Großbritannien)

Erfahrungswerte:

- Ca. 5-10% der IT-Projektkosten
- Ca. 14% der IT-Infrastrukturkosten
- Ca. 3-5% des IT-Personals

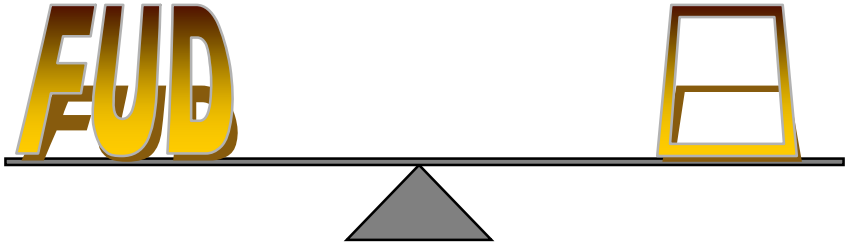
„Gründe“ für IT-Sicherheitsinvestitionen

Triebfeder FUD

(**F**ear, **U**ncertainty and **D**oubt)

Ziellose, unüberlegte Investitionen

- aus Angst, etwas falsch zu machen
- aufgrund von Medien-Hystery



Triebfeder „Me-too“-Effekt

- Sicherheit als Statussymbol
- Orientierung am Sicherheitsniveau der Konkurrenz

Gründe für IT-Sicherheitsinvestitionen

- Gesetze, Vorschriften, branchenspezifische Regelungen
- Risikominimierung
- Effizienzsteigerung
- Neue Chancen: IT-Security als „enabling Technology“

Gesetze, Vorschriften, branchenspezifische Regelungen

- BDSG, AktG, KonTraG, …
- Basel II
- ISO 27000 ff
- CobiT
- Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin): Mindestanforderungen an Risikomanagement (MA Risk) und Kreditgeschäft (MaK)

Betriebswirtschaftliche Seite der IT-Sicherheit

versichern	optimieren	ermöglichen
Minimierung von Risiko	Einsparung durch das IT-Sicherheits-projekt	Unterstützung neuer Prozesse, Erschließung neuer Kunden oder Märkte
RoI (i. d. R) schwer direkt zuzuordnen -> RoSI	RoI (i. d. R) direkt messbar	RoI (i. d. R) nur indirekt messbar
Firewall, Antiviren, usw…	PKI	VPN; „online-banking“

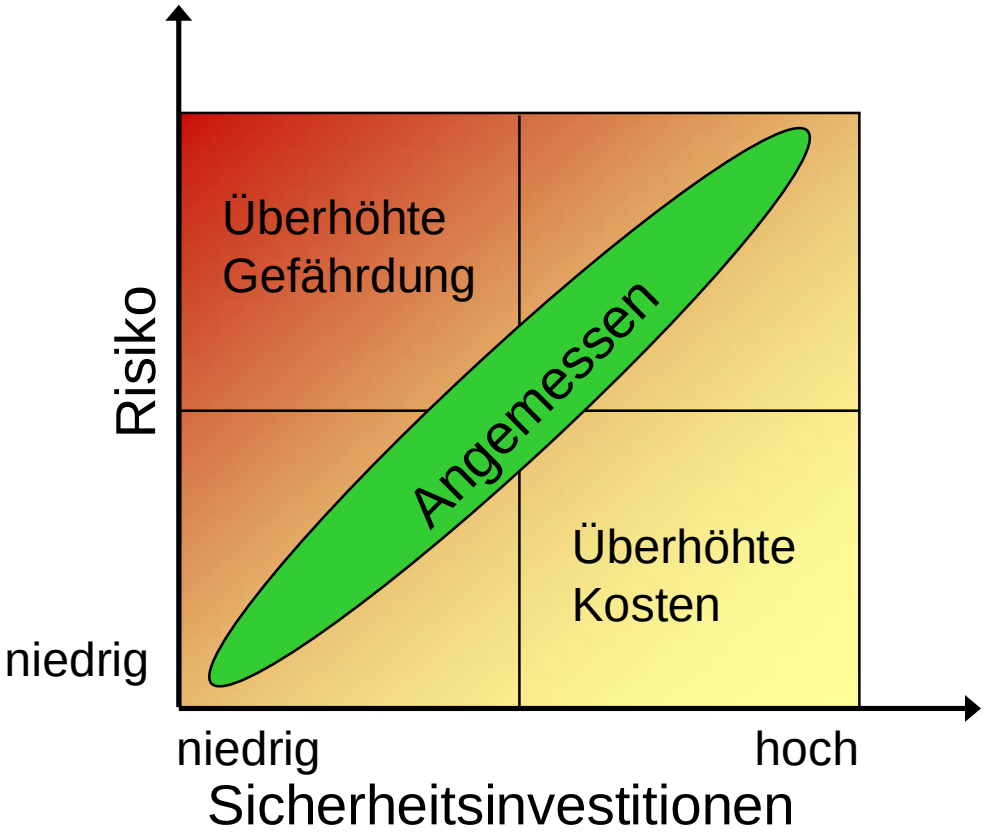
Risikominimierung

„Es gibt keinen positiven Nutzen von Sicherheitsinvestitionen. Investitionen in Informationssicherheit vermeiden lediglich Wertabflüsse. Das ist die Crux der ganzen Sache“

[Christian Dreyer, Finanzanalyst und CFO der schweizerischen Open Systems AG]

Möglichkeit einer Berechnung durch den
Return on Security Investment - RoSI
Einsparungen an Kosten der wahrscheinlichen Schäden, die durch die Investitionen in Maßnahmen erzielt wurden

Betriebswirtschaftliche Seite der IT-Sicherheit



Pareto Prinzip

Pareto-Prinzip (80/20-Regel) gilt auch für Sicherheit:
Werden 20% der möglichen Sicherheitsmaßnahmen richtig eingesetzt, kann 80% Schutz vor potentiellen Risiken erreicht werden

Ist ein Grundschutz erreicht, werden weitere Investitionen in Sicherheit sehr groß und scheinen rein wirtschaftlich betrachtet oft nicht mehr sinnvoll zu sein – auch dann, wenn sie notwendig sind.

Beispiel RoSI

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:

Beispiel RoSI

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 €

Schaden pro Vorfall bei 131.750 Euro

Beispiel RoSI

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 = 80 €)	2.400 €	2.400 €	2.400 €
Ersparnisse durch IT-Sicherheitsinvestition	263.500 €	263.500 €	263.500 €
RoSI	258.403 €	518.606 €	778.809 €

Optimierung von Prozessen und Verfahren

Erschließung von Wirtschaftlichkeitspotentialen durch

- Nutzung neuer Sicherheitsechnologie
- Optimierung von Prozessabläufen durch Integration von IT-Sicherheitsverfahren

Klassische betriebswirtschaftliche Verfahren zur Investitionsrechnung können genutzt werden.

Optimierung von Prozessen und Verfahren Beispiel

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	5.000 €
Kosten für Nutzerunterstützung bei vergessenen Passwörtern = 100 €/Nutzer	200.000 €
Ersparnisse durch IT-Sicherheitsinvestition	175.200 €

IT-Sicherheit als Enabling Technology

Beispiel: Einführung einer PKI als Basis für elektronische Prozesse und Konvergenz von Technologien

RoI - Betrachtungen				
	Jahr 1	Jahr 2	Jahr 3	Jahr 4
Investitionskosten	1.733.000			
laufende Kosten/Jahr	1.128.000	1.128.000	1.128.000	1.128.000
Kostensenkung Help Desk durch smartcard-basiertes Zugangssystem	1.430.000	1.430.000	1.430.000	1.430.000
Kostenreduzierung durch WebZEB	-470.000	504.108	504.108	504.108
RoI	-1.901.000	-1.094.892	-288.784	517.324

Alternativen, Ergänzungen

- Schwachstellenanalysen (Penetrationstests)
- Szenarioanalysen
- Kennzahlen
- …..

Leitfragen zur Strukturierung der Diskussion

- Müssen Investitionen in IT-Sicherheit betriebswirtschaftlich begründet werden?
- Welche Verfahren werden genutzt? – Beispiele?
- Wie werden diese Verfahren bewertet?
- Erfahrung in der Anwendung der Rechenverfahren?
- Gibt es ein systematisch Controlling – Ergebnisse?
- Werden alternative Bewertungsverfahren genutzt? – Erfahrungen?