T.I.S.P.
TeleTrusT Information Security Professional

TeleTrusT
Pioneers in IT security.

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
Ergebnisse

Ergebnisse – grundsätzliche Einschätzung

- Investitionen in IT-Sicherheit müssen begründet werden, aber nicht immer sind aufwendige Nachweise erforderlich. Hier spielt die Art des Unternehmens eine Rolle: im Bankenbereich werden Maßnahmen eher akzeptiert, Mittelstand scheint oft schwierig.
- Die „allgemeine“ Diskussion über das Thema beeinflusst die Budgets. Z.Zt. scheint die Bereitschaft vorhanden zu sein, auch aufwendigere Investitionen zu tätigen.
- Wann müssen die Investitionen begründet werden:

  Budgets für die „regulären“ IT-Sicherheitsaufgaben sind vorhanden, hier muss nicht aufwendig die Wirtschaftlichkeit nachgewiesen werden, bei Projekten muss ein Sonderbudget jedoch begründet werden
- Umfang des IT Sicherheitsbudgets 10 – 15% der IT Budgets
- Abgrenzung der Aufwendungen für IT-Sicherheit häufig schwierig, weil Anteil für Kunden nicht immer sichtbar.
- Bedrohungsanalysen als Motivation für Investment

Ergebnisse

Gründe für IT Sicherheitsinvestitionen:

- Gesetzliche Vorgaben, Regelungen (Basel III, MaRisk)
- Risikominimierung
- Effizienzsteigerung
- IT-Security als enabling Technology
- Starkes Argument: IT-Security optimiert Prozesse!
- Für die Analyse und Bewertung: Mix aus allem sinnvoll

Risikominimierung

Wie kann man Risiken bewerten?

- Risikomanagement wird in Unternehmen etabliert (seit ca. 7-8 Jahren)
- Versicherungen haben Daten zu Risiken, diese sollten für das Risk Management genutzt werden.
- Szenarien erstellen und analysieren!
- In Banken werden Rückstellungen gebildet, daher erfolgt eine sorgfältige Analyse.

Beispiel Risikominimierung - 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

Analysebeispiel:
Einschätzung Wirtschaftlichkeit Awareness Kampagne

Kosten:

1 Personenjahr (80.000 Euro)

80.000 Euro Standort 1

20.000 Euro Standort 2

Einschätzung Wirtschaftlichkeit Awareness Kampagne

Assets:

- exklusive Zeitungsnachricht
- Gut verfügbare Arbeitsumgebung

Gefährdungen:

- Verlust Vertraulichkeit (exklusiver Artikel wir ausspioniert und erscheint in Konkurrenzzeitungen)
- Mangelnde Verfügbarkeit (Journalisten können – zeitweise – nicht arbeiten, Zeitung erscheint verspätet)
- Integrität: manipulierte Artikel

Schadenseinschätzung Malware auf Rechnern

Folge: IT-Infrastruktur steht nicht oder nur eingeschränkt zur Verfügung:
Journalisten können nicht arbeiten

Maßnahmen zur Wiederherstellung der Verfügbarkeit:

6 Tage externe Support zur Beseitung der Schäden: 6.000 €

Schadenseinschätzung Malware auf Rechnern

Umsatzeinbußen:

- Reguläre Auflage 500.000 (KStA, Express), Preis 1 €
- 1 Tag erscheint nur eine Notausgabe: 150.000 Exemplare
- Einbuße 400.000 € durch höhere Erstellungskosten und geringere Auflage

Schadensersatzleistung für manipulierten Artikel: 50.000€

Verlust Anzeigenkunden: 50.000 €

Schadenseinschätzung Malware auf Rechnern

Zusammenstellung:

- 6.000 Externer Support
- 400.000 Umsatzeinbußen
- 50.000 Schadensersatz
- 50.000 Verlust Anzeigenkunden

Schadenshöhe: 506.000€

Eintrittswahrscheinlichkeit: alle 3 Jahre

Jährliche Verlusterwartung: 168.700 €

Nutzen der Wirtschaftlickeitsbetrachtungen

- Systematische Analyse der Investition führt zu sorgfältiger Planung und einem effizienteren Design einer IT-Sicherheitsmaßnahme
- Unterstützt die Kommunikation und Aktzeptanz beim Management aber auch bei den Mitarbeitern