Fachhochschule Gelsenkirchen

Securitykosten ermitteln:
→ Gibt es einen RoSI?

Prof. Dr. Norbert Pohlmann

Institut für Internet-Sicherheit
Fachhochschule Gelsenkirchen
http://www.internet-sicherheit.de

if(is) institut für internet-sicherheit.

Inhalt

- Einführung
- IT-Sicherheitsrisiko und -Investment
- Kosten-Nutzen-Betrachtung im Hinblick auf das zu tragende Risiko
- Return on Security Investment RoSI
- Zusammenfassung

Inhalt

institut für internet-sicherheit.

- **Einführung**

- IT-Sicherheitsrisiko und -Investment
- Kosten-Nutzen-Betrachtung im Hinblick auf das zu tragende Risiko
- Return on Security Investment RoSI
- Zusammenfassung

Einführung
→ Was sind die Aufgabe eines IT-Systems?

- **Geschäftsprozesse zu verbessern**, damit die Ziele einer geschäftlichen Tätigkeit besser erreicht werden können.

- Beispiele sind z.B.:
  - Aufgaben vereinfachen oder beschleunigen
  - Abläufe störungsfreier oder flexibler gestalten
  - Mitarbeiter von Routineaufgaben entlasten
  - Mitarbeiter bei komplexen Aufgaben unterstützen
  - Globale wirtschaftliche Ausdehnung einfach ermöglichen

Einleitung
→ Ziel einer geschäftlichen Tätigkeit

- **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!

Einleitung
→ Wirtschaftlichkeit: Kostenaspekte

- **Total Cost of Ownership**
  - Kosten für Anschaffung, Schulung, Installation, Betrieb, Wartung und Ersatz von IT-Systemen und IT-Sicherheitsmaßnahmen
    - **Entspricht der Kapitalwert-Methode**
  - Was kostet ein Investment in der Summe alle 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.

Einleitung
→ Wirtschaftlichkeit: Nutzenaspekte

- **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 Anschaffung für die Investition wird durch den mit der Investition erwirtschafteten Ertrag gedeckt.

- Je schneller eine Deckung erzielt wird, um so schneller kann ein Profit, z.B. durch das Investment von IT-Sicherheitsmaßnahmen, generiert werden.

Einleitung
→ Return on Investment - RoI

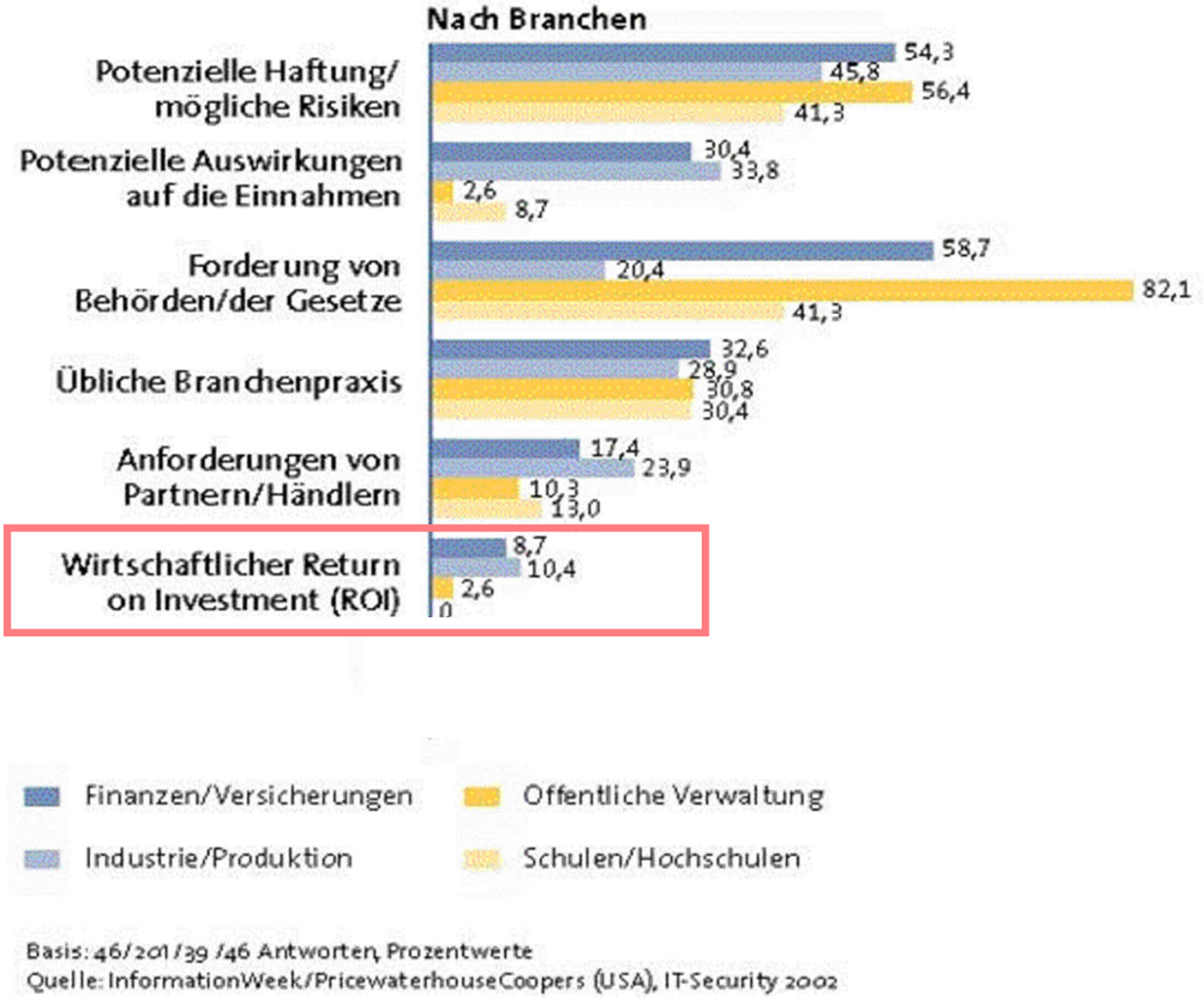
- 82 % der IT-Entscheidungen basieren auf **RoI** Analysen (Information Week, 10/2002)

- CEO und CFO wollen einen Nachweis des **RoI** bevor investiert wird

- Problem bei IT-Sicherheit:
  Quantitativer Nachweis von Schäden ist sehr schwierig!

  (Mittelbare und unmittelbare finanzielle Schäden; Renommeeverlust, Vertrauensverlust, ...)

Einleitung
→ Gründe: Investment in IT-Sicherheit

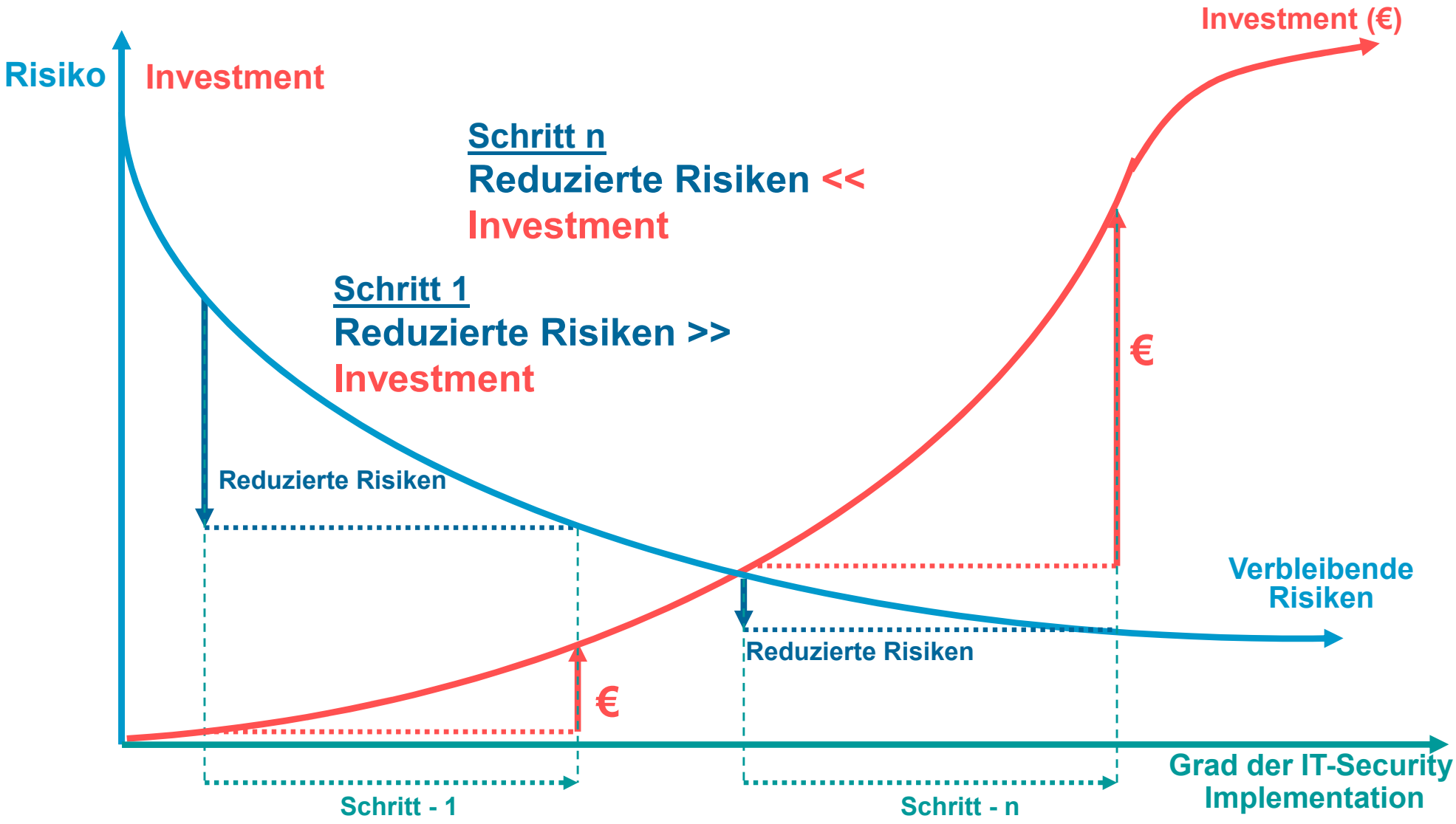


http://www.informationweek.de/index.php3?/topthemen/021822.htm

Inhalt

- Einführung
- **IT-Sicherheitsrisiko und -Investment**
- Kosten-Nutzen-Betrachtung im Hinblick auf das zu tragende Risiko
- Return on Security Investment RoSI
- Zusammenfassung

IT-Sicherheitsrisiko und -Investment



Investment zur Risikominderung

Investment ?????

Investment zur Risikominimierung → Grundschutz

institut für internet-sicherheit.

Pareto-Prinzip (80:20 Regel)

20% der möglichen IT-Sicherheitsmechanismen richtig eingesetzt liefern

80% Schutz vor potentiellen Bedrohungen

- Das bedeutet, dass mit dem **Einsatz der richtigen IT-Sicherheitsmaßnahmen** mit einem relativ geringen Aufwand, ein **vernünftiger Grundschutz** für IT-Systeme **hergestellt werden kann**.

Investment zur Risikominimierung → Spezieller Schutz

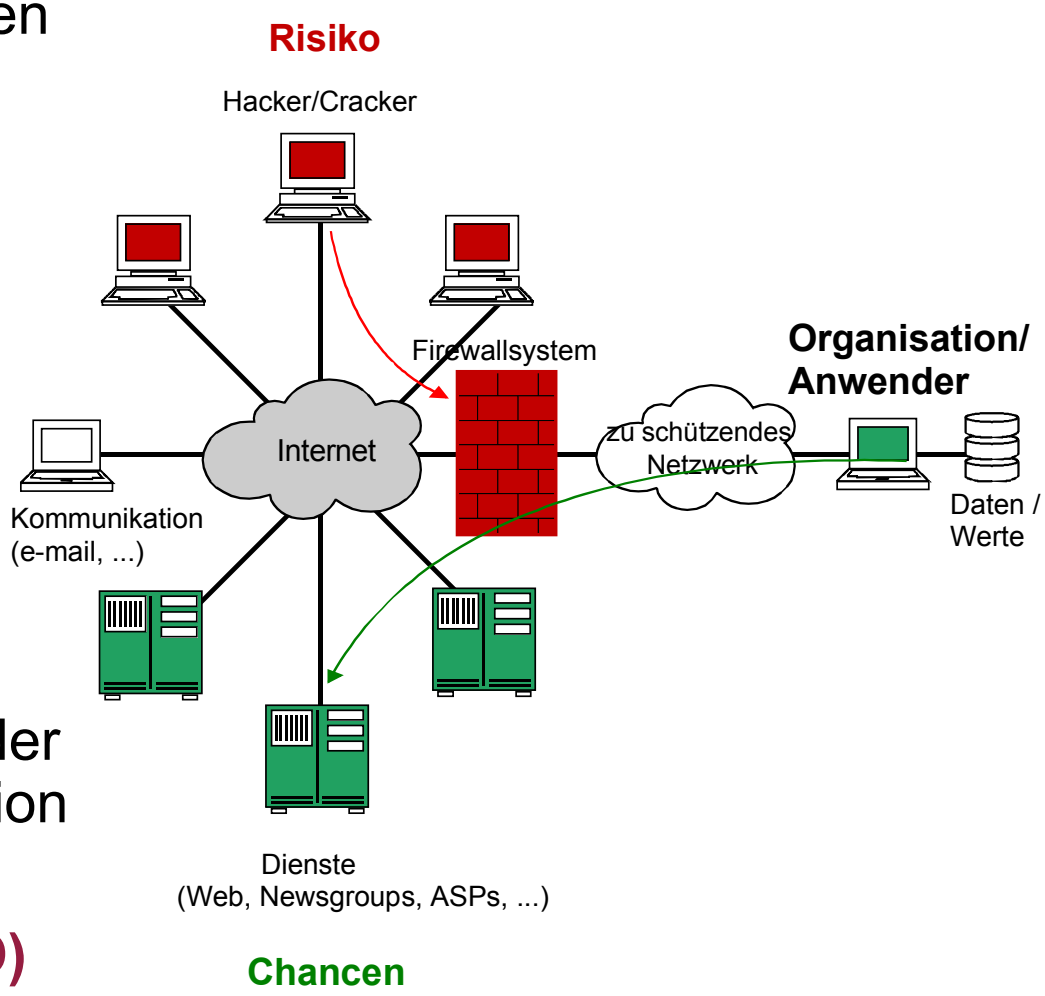
- Wenn ein Grundschutz bereits implementiert ist, wird notwendiges weiteres Investment in Sicherheit sehr groß und ist **„wirtschaftlich“** isoliert betrachtet, i.d.R. **nicht mehr sinnvoll**.
- Es kann aber andere Gründe außer der Wirtschaftlichkeit geben, ein solches Investment dennoch durchzuführen.
  - Ist im Gesamtzusammenhang besonders wichtig
    - kritische Infrastruktur
    - besonders sensibler Bereich
  - Gesetzliche Notwendigkeiten
  - Im militärischen Bereich, zum Schutz der Gesellschaft
  - Wenn es um die Sicherheit von Menschen geht
  - Angst
  - Übertriebenes Sicherheitsgefühl

Inhalt

- Einführung
- IT-Sicherheitsrisiko und -Investment
- **Kosten-Nutzen-Betrachtung im Hinblick auf das zu tragende Risiko**
- Return on Security Investment RoSI
- Zusammenfassung

Kosten-Nutzen-Betrachtung (Risiko)
→ TCO: Beispiel Firewall

- Aufwendungen der Anschaffungskosten für ein Firewall-System
  - **EUR 38.750 und EUR 236.250**
- Kosten für die Aufrechterhaltung des Betriebs für ein Firewall-System
  - **EUR 76.500 im Jahr**
- Diese Zahlen hängen sehr stark von der Struktur und der Größe der Organisation ab.
- Produktkosten: **(12 bis 30 % der TCO)** EUR 5.000 bis 75.000



Kosten-Nutzen-Betrachtung (Risiko)
→ Ausgangssituation und Angriff

- **Angenommener Profit einer Bank:** EUR 25.000.000/Jahr

- **Kosten eines Firewall-Systems (TCO)**
  - Anschaffungskosten: EUR 250.000 (1 % vom Profit)
  - Betriebskosten: EUR 80.000/Jahr

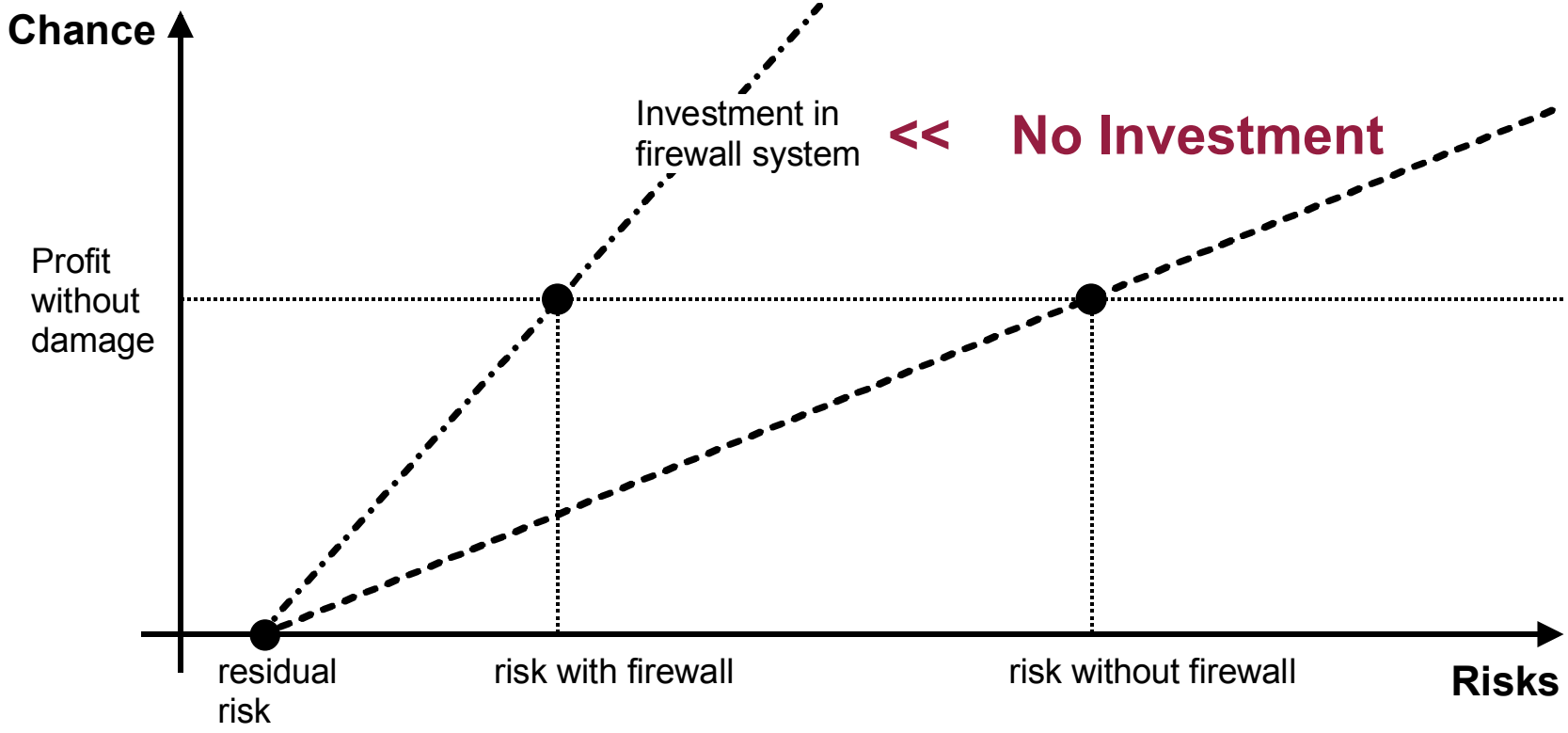
- **Beschreibung eines möglichen Angriffs**
  - Hacker entwenden Namen und Kontostände der 500 wichtigsten Kunden
  - Diese veröffentlichen die Hacker dann im Internet

Kosten-Nutzen-Betrachtung (Risiko) → möglicher Schaden

- **Möglicher Schaden durch diesen Angriff**
  - sofort: EUR 12.500.000 (50 % vom Gewinn)
  - mittelfristig: EUR 2.500.000/Jahr

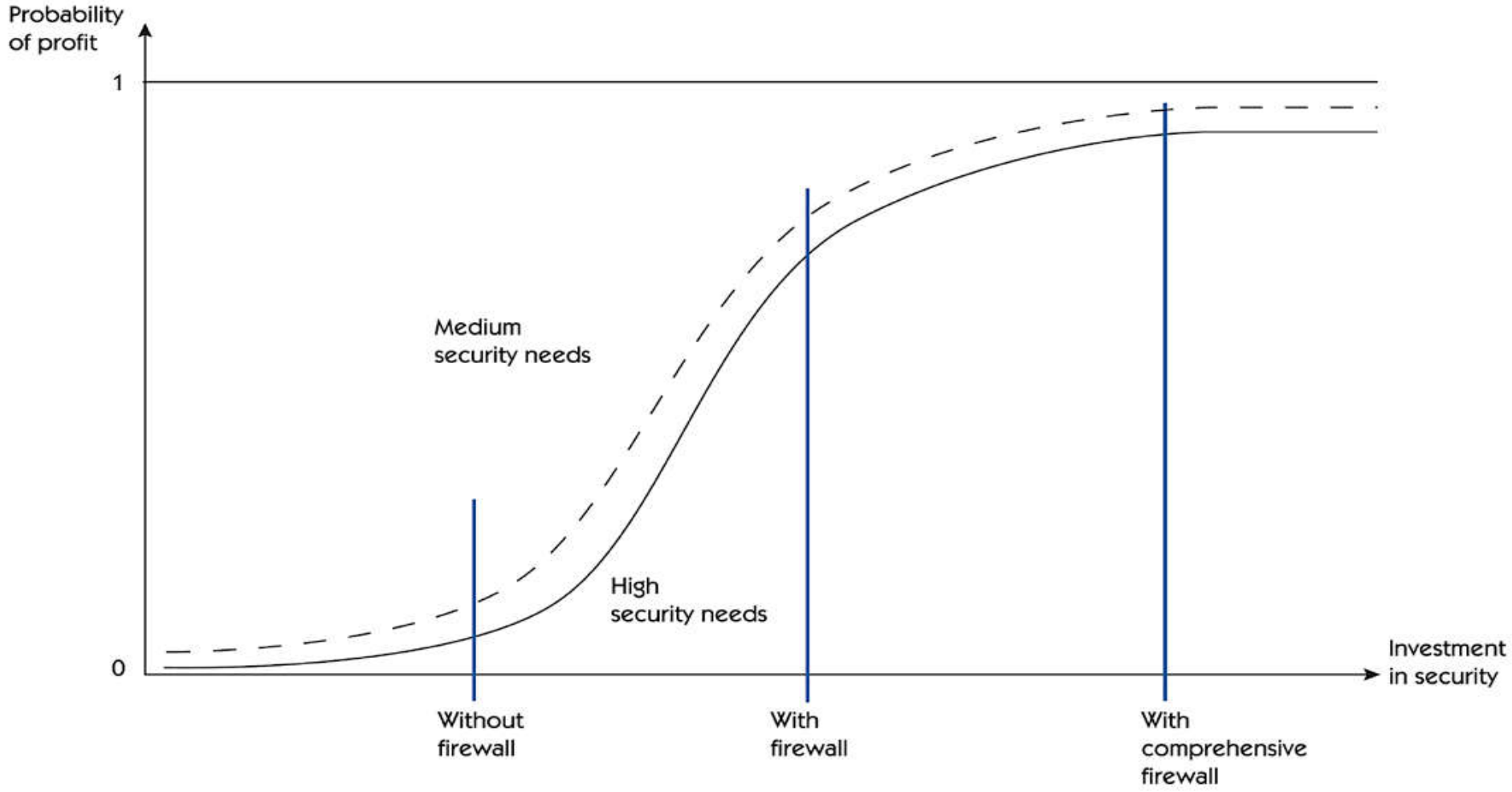
- **Zusammenfassung:**
  - Unter der Annahme, dass der Schaden mit Hilfe eines Firewall-Systems verhindert wird und der Schaden nicht auftritt, hat sich die Investition in ein Firewall-System sehr gelohnt !
  - Es sind nur **1 % vom Gewinn** notwendig, um einen sehr hohen Schaden zu vermeiden.
  - **Wirtschaftlich sehr sinnvoll!**
  - Diese ist **keine RoI Berechnung**

Kosten-Nutzen-Betrachtung (Risiko)
→ Kein Investment kann teuer sein!



- Falls ***kein*** Firewall-System eingesetzt wurde, muss nach dem Schadensfall auf jeden Fall ein Firewall-System eingerichtet werden, da mit einem ersten Schadensfall das Risiko eines zweiten sehr viel höher ist !
- In den meisten Fällen steigen die IT-Sicherheitsaufgaben nach einem größere Vorfall (survey released in March 2002 by IDC , Mass.)

Kosten-Nutzen-Betrachtung (Risiko) → Zusammenhang

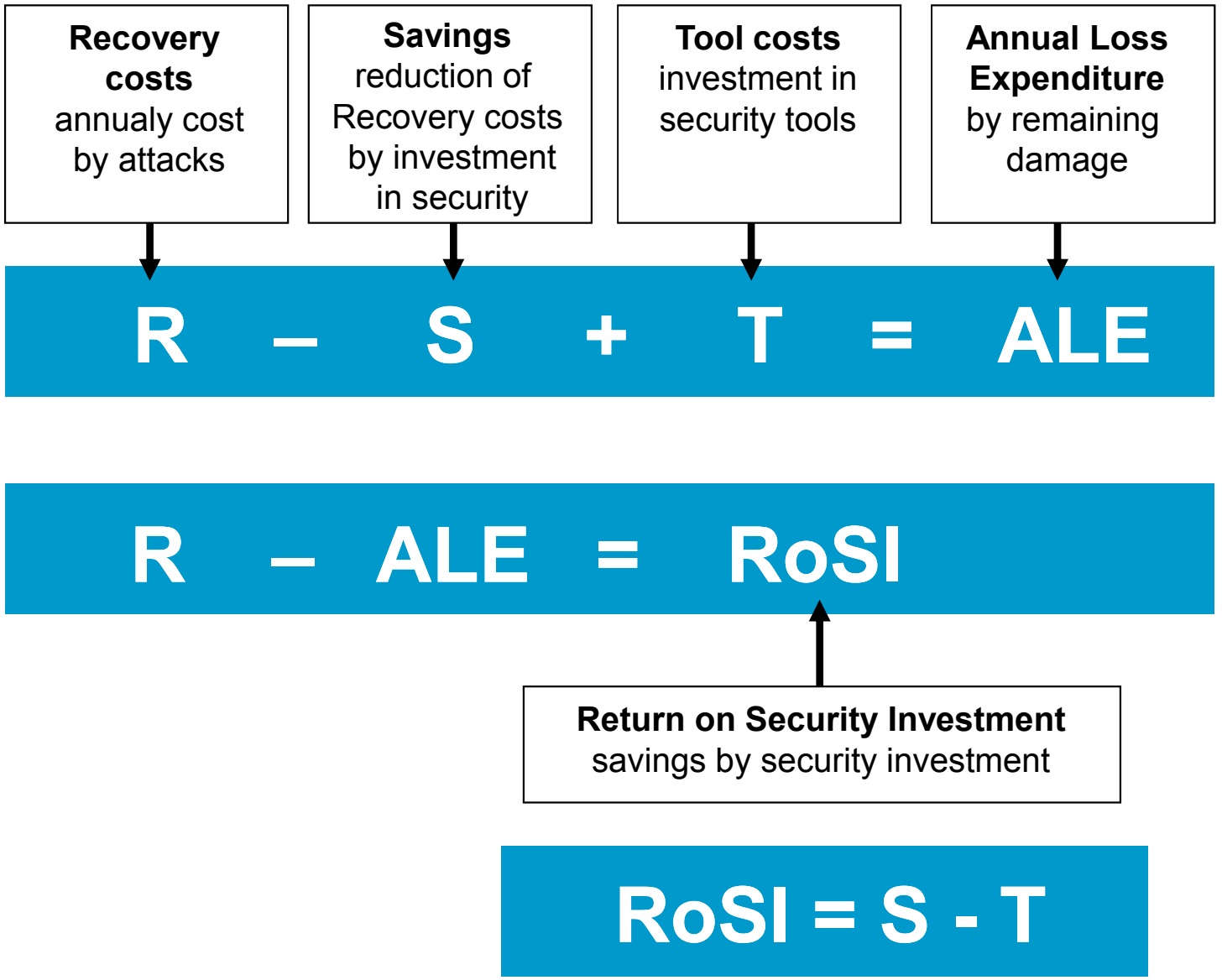


- Wahrscheinlichkeit, einen bestimmten Profit erreichen zu können, ohne dass ein Schaden durch einen erfolgreichen Angriff auftritt!

Inhalt

- Einführung
- IT-Sicherheitsrisiko und -Investment
- Kosten-Nutzen-Betrachtung im Hinblick auf das zu tragende Risiko
- **Return on Security Investment RoSI**
- Zusammenfassung

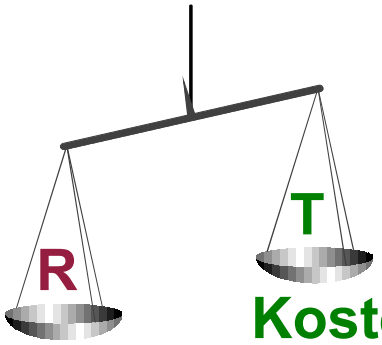
Return on Security Investment – RoSI
→ Übersicht



Source: University of Idaho, CIO 5/2002

Return on Security Investment – RoSI → Beispiel: Notebookverluste

- In diesem Beispiel soll anhand der Verluste von Notebooks exemplarisch eine **Return on Security Investment (RoSI)** durchgeführt werden.
- **Ablauf:**
  - Festlegung der Wahrscheinlichkeit des Verlustes eines Notebooks.
  - Festlegung des Schadens (R), wenn die Daten, die auf einem Notebook gespeichert sind, von Dritten missbräuchlich verwendet werden.
  - TCO für die Anschaffung eines Sicherheitssystems (T) für die Sicherung der Daten auf dem Notebook.
  - **RoSI - Berechnung**



Kosten eines Schadens

Kosten für eine Sicherheitssystems

RoSI-Beispiel: Notebookverluste
→ Wahrscheinlichkeit des Verlustes?

institut für internet-sicherheit.

- Jeder der die Verantwortung von Notebooks im Unternehmen hat, müsste wissen wieviele Notebooks jährlich aus nachvollziehbaren und nicht nachvollziehbaren Gründen verschwinden!

Durchschnitt:
gestohlene Notebooks
6%

- **Einschätzung (Erfahrungen anderer)**
  - 5% of the company's laptops were stolen over the past year.
    Head of the MIS Department at the Advisory Board Company
    www.compuclamp.com/Computer%20Theft.htm
  - ...as many as one in every 14 laptops sold in the US was stolen last year. Newsweek , 05/2002, www.compuclamp.com/Computer%20Theft.htm
  - One in every 14 laptops is stolen (= 7%)
    World Security Corporation, 2002
  - 1 in 10 notebooks are stolen
    Tech Republic survey, www.microsaver.com/tips/tip_1028.html
  - Annual notebook theft rate rising to 5% and more through 2002 Gartner Group, www.ebiz.co.za/L_SCRIPTS/article.asp?pklArticleID=1380&pklIssueID=245

RoSI-Beispiel: Notebookverluste
→ Wie hoch ist der Schaden?

institut für internet-sicherheit.

- Dies kann der Besitzer des Notebooks am besten bemessen.
- Problem: der Schaden ist oft nicht genau zu analysieren, sondern durch Reduktion des Umsatzes und des Gewinns nur schwer zu beziffern.
- **Einschätzung (Erfahrungen anderer)**

Annahme
Wert der Daten
€10.000

  - Average losses top $40,000 per Computer Stolen
    Over four years, the average reported loss related to notebook computer theft topped $40,000, and the highest reported single loss — $1.2 million.

    FBI/Computer Security Institute Survey, Computer Security Issues and Trends
    Computer Security Institute, June 2000

  - The average financial loss resulting from a laptop theft grew by 44% from 2000 to 2001 ($62.000)
    → Only a small percentage of the sum actually relates to the hardware costs

    Source: 2001 and 2002 Computer Security Institute/FBI Computer Crime & Security Survey

  - Im November 1996 wurde ein Notebook von Visa International gestohlen. Darauf befanden sich über 314.000 Kreditkartennummern. Kosten für den Austausch pro Kreditkarte ca. 23 Euro. Insgesamt also ca. **7 Millionen Euro Schaden**.

    Deutsche Ausgabe PKI, e-security implementieren, Nash, Duane, Joseph, Brink, mitp-Verlag, Bonn: 2002.

Notebook Verschlüsselung
→ 1. Berechnung

- Notebook Verschlüsselung für 500 Nutzer:
  - Einmalige Lizenzkosten: → € 55.000 (1 Lizenz = €110)
  - Jährliche Kosten: → 1. Jahr € 10.000, dann € 5.000/Jahr
  - Vermiedener Schaden: → € 300.000 (= 30 Notebooks * €10.000)
    (= Reduced costs per year)

Annahme
Wert der Daten
€10.000

Durchschnitt:
gestohlene Notebooks
6%

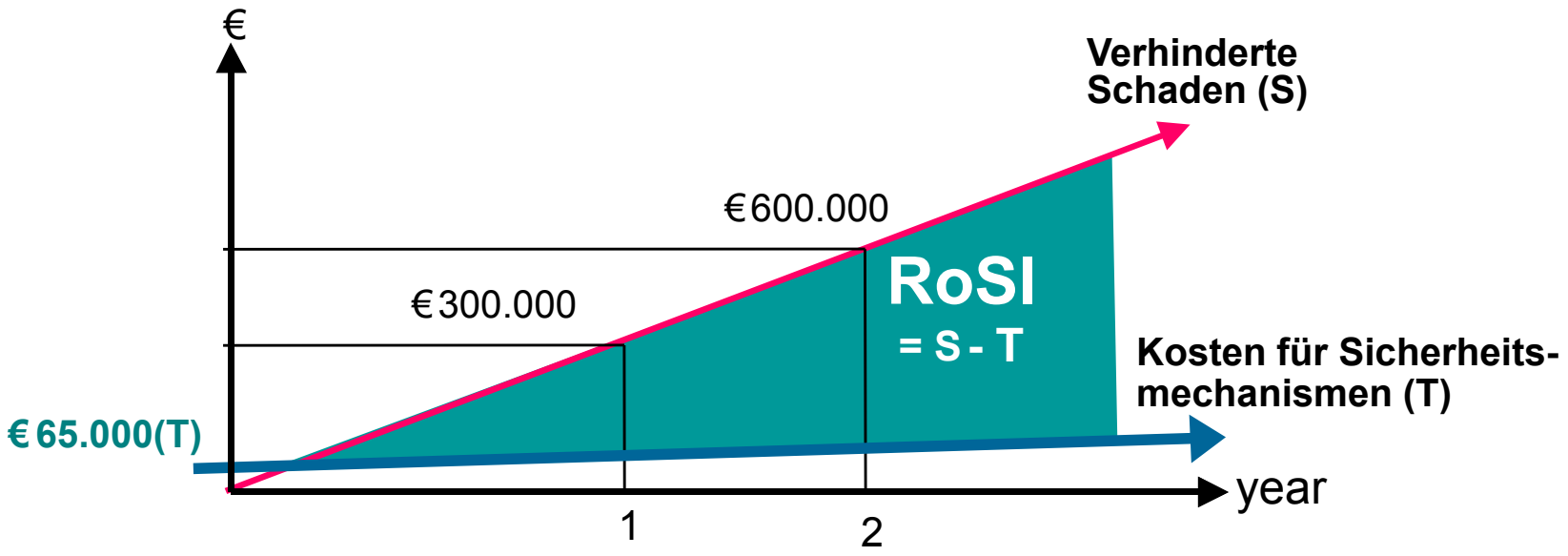
Calculation					In total
Time span	1st year	2nd year	3rd year	4th year	4 years
Initial costs	**€ 55.000**	**--**	**--**	**--**	**€ 55.000**
Implementation/ Roll-out, Admin	**€ 10.000**	**€ 5.000**	**€ 5.000**	**€ 5.000**	**€ 25.000**
Reduced costs??	**--**	**--**	**--**	**--**	**--**
Value of no losses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

Notebook Verschlüsselung (RoSI)

Beispiel: Firma mit 500 Notebooks

- **Schaden** = Wert der Daten auf jedem Notebook = **€ 10.000**
- **Wahrscheinlichkeit** eines Notebook Diebstahl/Jahr = 6%

→500 Notebooks x 6% Wahrscheinlichkeit eines Notebook Diebstahl = **30**



Das Investment (T) ist kleiner als der verhinderte Schaden (S)

Notebook Verschlüsselung
→ 2. Berechnung

institut für internet-sicherheit.

- Notebook Verschlüsselung für 500 Nutzer:
  - Einmalige Lizenzkosten: → € 55.000 (1 Lizenz = €110)
  - Jährliche Kosten: → 1. Jahr € 10.000, dann € 5.000/Jahr
  - Vermiedener Schaden → € 75.000 (= 15 Notebooks * € 5.000)
    (= Reduced costs per year)

Annahme
Wert der Daten
€5.000

Durchschnitt:
gestohlene Notebooks
3%

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**

Notebook Verschlüsselung
→ 3. Berechnung

- Notebook Verschlüsselung für 500 Nutzer:
  - Einmalige Lizenzkosten: → € 55.000 (1 Lizenz = €110)
  - Jährliche Kosten: → 1. Jahr € 10.000, dann € 5.000/Jahr
  - Vermiedener Schaden → € 25.000 (= 5 Notebooks * €5.000)
    (= Reduced costs per year)

Annahme
Wert der Daten
€5.000

Durchschnitt:
gestohlene Notebooks
1%

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	**€ 25.000**	**€ 25.000**	**€ 25.000**	**€ 25.000**	**€ 100.000**
ROI 1st year	**€-40.000**				
ROI 2nd year		**€-20.000**			
ROI 3rd year			**€0**		
ROI 4th year				**€ 20.000**	**€ 20.000**

RoSI-Berechnung
→ weitere einfache Beispiele

- 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 (S), die durch Schäden bei Virenbefall aufgetreten sind, zur Verfügung.
  - **ID-Managemen: SingleSignOn (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 normale Papierrechnung mit handgeschriebener Unterschrift versendet, oder € 0,40 für eine elektronische Rechnung mit digitaler Signatur, z.B. per E-Mail versendet.

RoSI-Berechnung
→ Herausforderungen

- Die RoSi-Berechnung kann ein sehr komplexer Prozess
  - Berechnung/Abschätzung des Schadens
  - Berechnung/Abschätzung der Reduzierung des Schadens durch Sicherheitsmechanismen
  - Komplexe Zusammenhänge zwischen Bedrohung und Schaden
  - Komplexe Zusammenhänge zwischen Bedrohung und Wirkung von Sicherheitsmechanismen
  - usw.

Inhalt

- Einführung
- IT-Sicherheitsrisiko und -Investment
- Kosten-Nutzen-Betrachtung im Hinblick auf das zu tragende Risiko
- Return on Security Investment RoSI
- **Zusammenfassung**

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.
- Es gibt Maßnahmen zur IT-Sicherheit, die 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 ein Return of Security Investment – RoSI durchführen!
- Um diesen Aspekt erfüllen zu können, müssen wir anfangen, die Angriffe und die ***resultierenden Schäden so gut wir möglich zu dokumentieren***. Dazu müssen in Zukunft geeignete Hilfsmittel zur Verfügung gestellt werden.

Zusammenfassung

- 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.

Fachhochschule Gelsenkirchen

Securitykosten ermitteln:
→ Gibt es einen RoSI?

Vielen Dank für Ihre Aufmerksamkeit
Fragen ?

Prof. Dr. Norbert Pohlmann

Institut für Internet-Sicherheit
Fachhochschule Gelsenkirchen
http://www.internet-sicherheit.de