IT-Sicherheit – Kosten vs. Nutzen

Prof. Dr. Hannes Federrath

Sicherheit in Verteilten Systemen (SVS)

http://svs.informatik.uni-hamburg.de

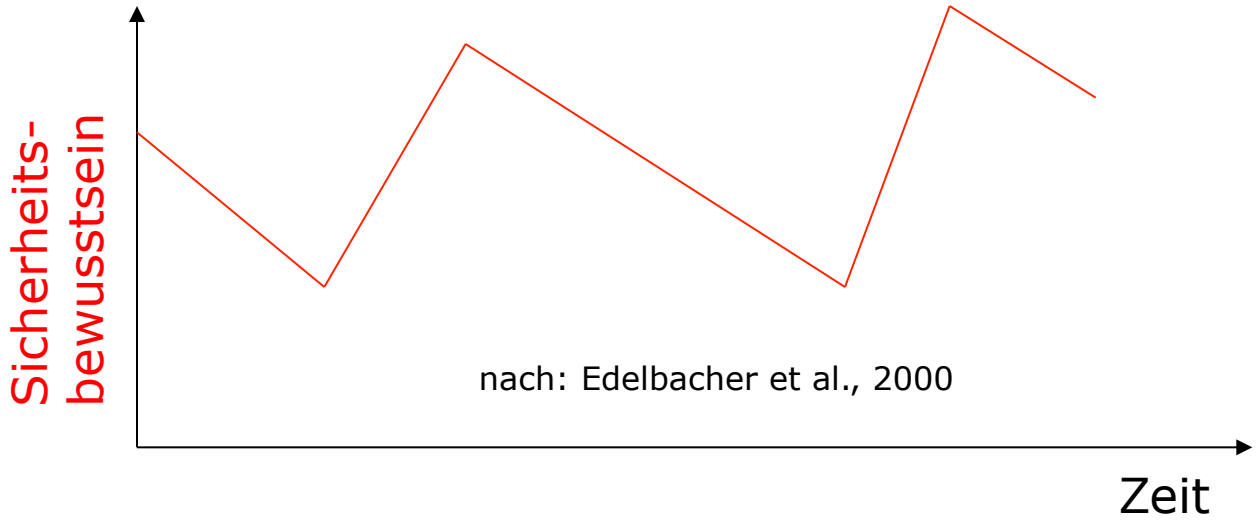
Universität Hamburg
DER FORSCHUNG | DER LEHRE | DER BILDUNG

20. Berliner Anwenderforum E-Government, Berlin, 20. Februar 2014

Wieviel soll in IT-Sicherheit investiert werden?

Nichts (zusätzlich)

- Sicherheit ist eine Sekundärfunktion.
- »Kein System ist einfach nur sicher.«
- Sicherheit dient der Unterstützung und Erhaltung eines Primärziels.



Zu hohe oder zu niedrige Ausgaben?

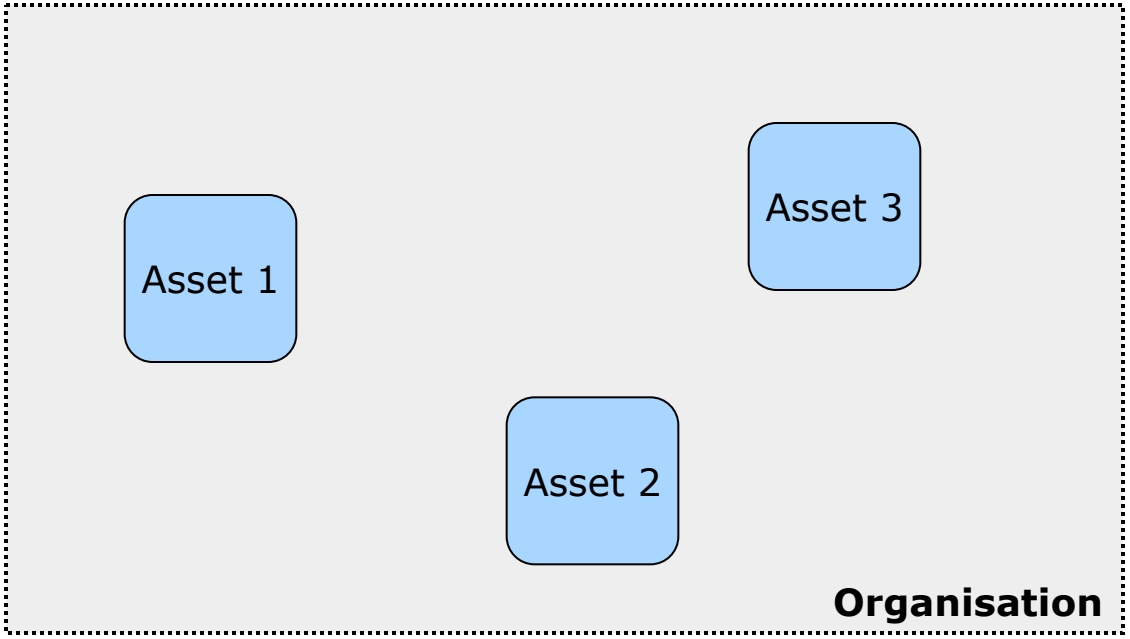
»…mangelnde Investition in IT-Sicherheit…«
BSI Lagebericht 2007

vs.

»The greatest IT risk facing most companies is more prosaic than a catastrophe. It is, simply, overspending.«
Nicholas G. Carr

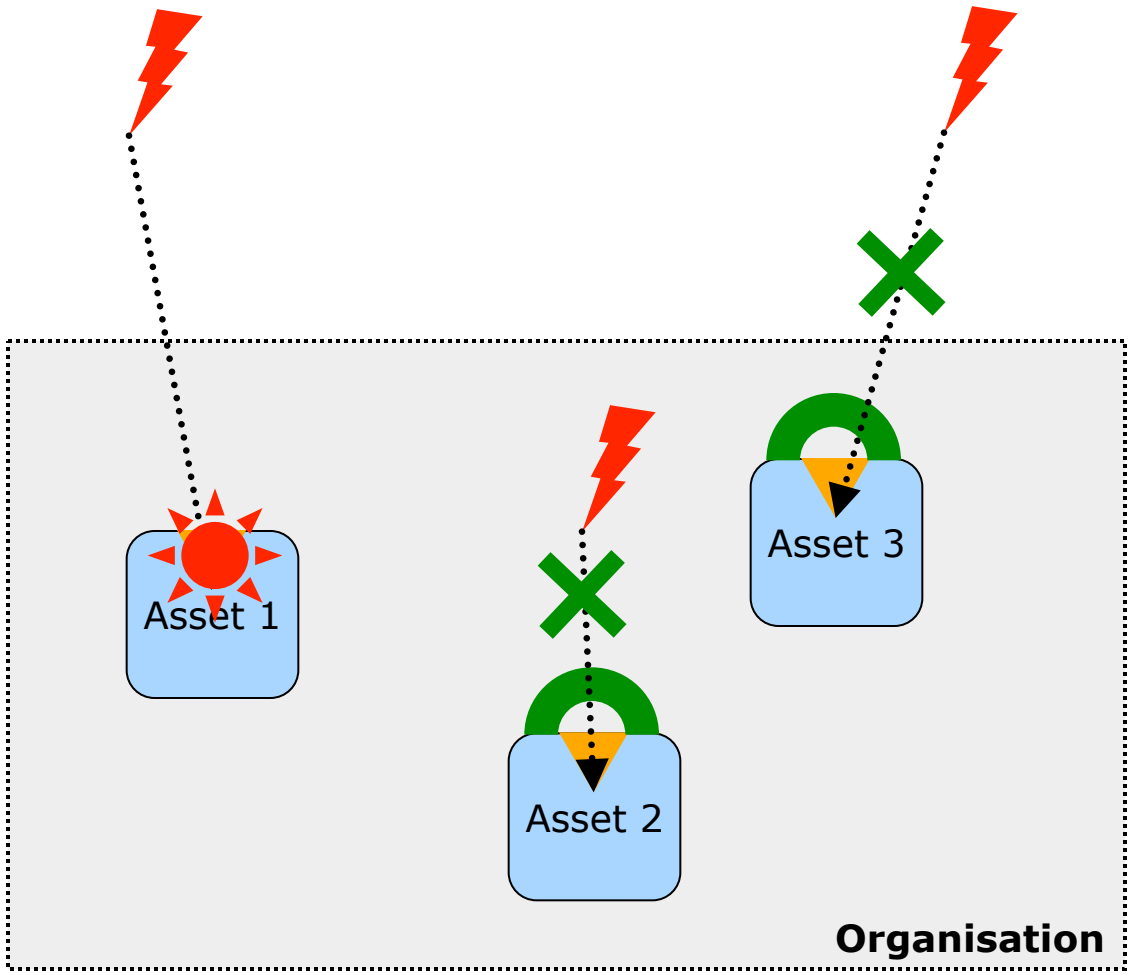
Warum braucht man IT-Sicherheit?

- Gründe, IT-Sicherheitsmanagement zu betreiben
  - Schutz von Unternehmenswerten (Assets)
  - Anforderung von Handelspartnern
  - IT-Compliance



Schutzziele
- Vertraulichkeit
- Verfügbarkeit
- Integrität

Von der Bedrohung zum Sicherheitsvorfall



Bedrohungen, z.B.
- Viren, Würmer
- DoS
- Hacking
- Spionage
- Social Engineering

Verwundbarkeiten, z.B.
- Konfigurationsfehler
- Buffer Overflows

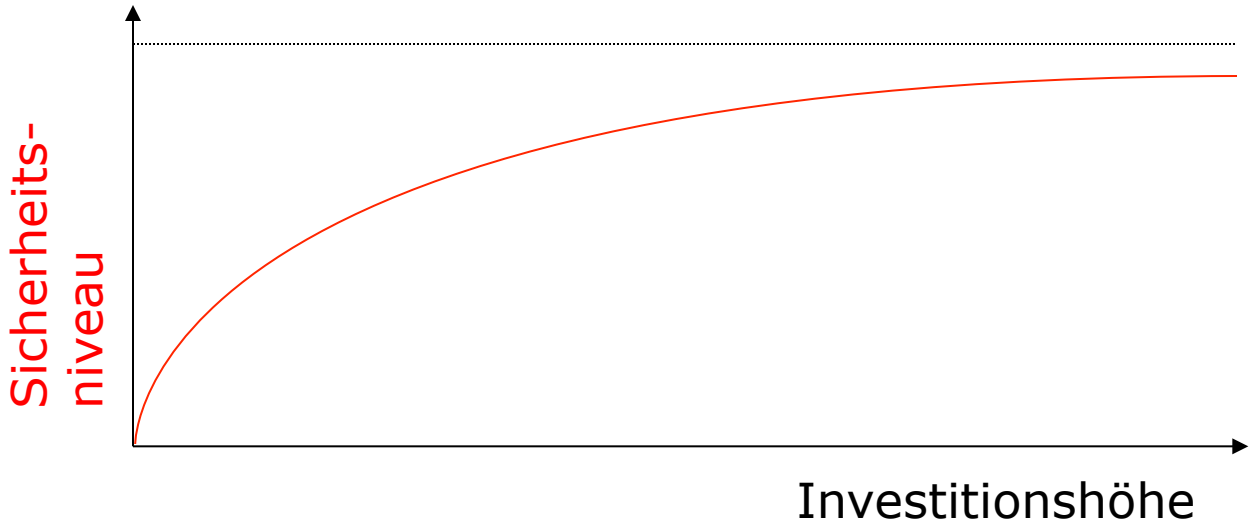
Schutzziele
- Vertraulichkeit
- Verfügbarkeit
- Integrität

Maßnahmen
- Präventiv
- Detektiv
- Reaktiv

Wieviel soll in IT-Sicherheit investiert werden?

So viel wie man braucht, um total sicher zu sein

- Kritik:
  - 100 %-ige Sicherheit ist nicht erreichbar



Wieviel soll in IT-Sicherheit investiert werden?

So viel wie das Budget hergibt

- Kritik
  - Budget nicht rational begründbar
- Anschlussfrage:
  - Wie groß muss das Budget gewählt werden?

Unterschiedliche Zielsetzungen

- Ziel Unternehmensleitung
  - Ausgaben gering halten
  - Kosten einsparen
  - Nur Projekte mit sichtbarem Nutzen realisieren

- Ziel Sicherheitsverantwortliche
  - Möglichst hohes Sicherheitsniveau schaffen
  - Budget erhöhen

- Was können Sie tun um Ihr Budget zu erhöhen?
  - Schüren Sie Angst!
  - Sammeln und drucken Sie Log-Files.
  - Verwenden Sie Abkürzungen und Fachbegriffe.
  - Zitieren Sie Studien von Sicherheitsfirmen und Beratungsunternehmen.

FUD-Strategie — Fear, Uncertainty, Doubt

Wieviel muss wirklich investiert werden?

vs.

Furcht, Ungewissheit, Zweifel

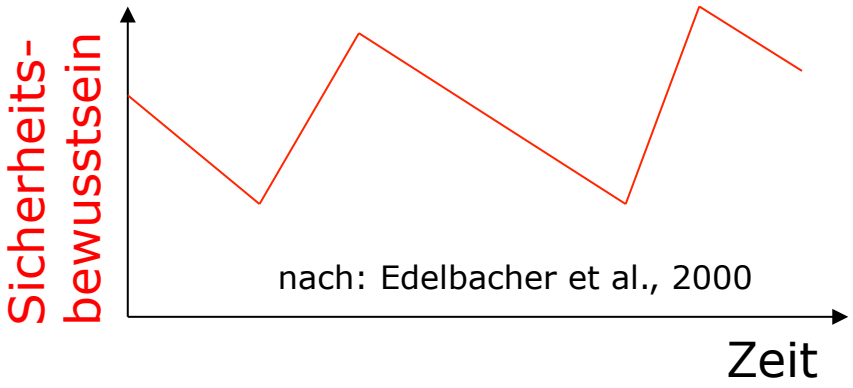


Bild: Bob Eggleton
Quelle: http://lair2000.net/Mermaids_Retreat/Research/Kraken.html

Computer Crime and Security Surveys

- Herausgegeben vom U.S. Computer Security Institute CSI
  - http://www.gocsi.com/
  - bekannteste Langzeit-Umfrage zu IT-Sicherheitsvorfällen
- Stichprobe
  - über 500 IT-Sicherheitsspezialisten aus verschiedenen Branchen

Computer Crime and Security Surveys

- Hauptergebnisse (2003)
  - Schäden in Unternehmen
    - Hauptschäden entstehen durch Datendiebstahl
    - Zweite Stelle: Schäden durch Denial-of-Servcie-Angriffe
  - Angriffsarten
    - 82 Prozent Virenangriffe
    - 80 Prozent Datenmissbrauch durch Insider
  - Reaktion auf Angriffe
    - 93 Prozent schließen Sicherheitslöcher
    - 50 Prozent verheimlichen Sicherheitslöcher
    - 30 Prozent verfolgen Angreifer (law enforcement)

Computer Crime and Security Surveys

- Hauptergebnisse 2007
  - Anstieg der Verluste durch Sicherheitsprobleme von 168.000 Dollar (2006) auf 350.000 Dollar (2007)
    - höchster Wert seit 2004
    - 18 Prozent der Befragten waren Opfer eines gezielten Angriffs
  - Hauptursache von Verlusten
    - in den vergangenen sieben Jahren: Viren (Schadsoftware)
    - nun an erster Stelle: »Financial fraud«
  - Insider-Angriffe
    - 59 Prozent der Fälle: unerlaubte Netznutzung
    - 52 Prozent der Fälle: Verseuchung mit Viren

Computer Crime and Security Surveys

- Hauptergebnisse 2010/11
  - Malware als verbreitetste Angriffsform
    - 67 Prozent der Teilnehmer berichten darüber
  - Anzahl der »Financial fraud« Vorfälle gegenüber der Vorjahre gesunken auf 8,7 Prozent
  - Gezielte Angriffe nehmen weiter zu
    - Bei etwa der Hälfte der Teilnehmer trat mindestens ein Informationssicherheitsvorfall auf
    - 46 Prozent dieser Teilnehmer berichten von mindestens einem gezielten Angriff
  - Erhöhte Sensibilität in Sicherheitsfragen
    - Immer weniger Teilnehmer sind bereit, genaue Daten über monetäre Verluste preiszugeben

Gründe für mangelnde Informationssicherheit

Es fehlt an Geld	55 %
Es fehlt an Bewusstsein bei den Mitarbeitern	52 %
Es fehlt an Bewusstsein und Unterstützung im Topmanagement	45 %
Es fehlt an Bewusstsein und Unterstützung beim mittleren Management	37 %
Es fehlen verfügbare und kompetente Mitarbeiter	32 %
Es fehlt an Möglichkeiten zur Durchsetzung sicherheitsrelevanter Maßnahmen	31 %
Es fehlen die strategischen Grundlagen/Gesamtkonzepte	29 %
Die Kontrolle und Einhaltung ist unzureichend	27 %
Anwendungen sind nicht für Informationssicherheitsmaßnahmen vorbereitet	25 %
Die vorhandenen Konzepte werden nicht umgesetzt	22 %
Es fehlen realisierbare (Teil)-Konzepte	19 %

Basis: 158 Antworten

Quelle: <kes>/Microsoft-Sicherheitsstudie 2006
aus: ZIEL:SICHER 01/2007, Microsoft 2007, S. 6

Welchen Einfluss haben Sicherheitsvorfälle auf das Image?

- Garg, Curtis, Halper, 2003:
  - Messung des Börsenwerts eines Unternehmens
  - Beeinflussung durch einen Vorfall am Tag t ist an t+1 und t+2 in einigen Fällen (signifikant) nachweisbar

Company	Announcement	Date of announcement	*t* (%)	*t*+1 (%)	*t*+2 (%)
Denial of service					
Yahoo	Denial of service attack beginning at 12:15 p.m. EST	2/7/00	–3.4	–2.8	–2.7
eBay	Denial of service attack beginning at 6:00 p.m. EST	2/8/00	–3.7	–4.8	–10.1
Microsoft	Denial of service attack beginning at 9:00 p.m. on 2/8/00	2/9/00	–3.1	–1.5	–0.1
Amazon	Denial of service attack beginning at 8:00 p.m. EST	2/9/00	–0.5	–10.5	–4.4
Time Warner (CNN)	Denial of service attack beginning at 7:00 p.m. EST	2/9/00	2.1	1.6	1.8
E*Trade	Denial of service attack beginning at 4:00 a.m. EST	2/9/00	–2.0	–5.1	–4.7
ZDNel	Denial of service attack beginning at 4:00 a.m.	2/9/00	2.6	–3.2	–3.3
Excite@Home	Denial of service attack	2/10/00	–3.3	–3.2	–5.9
National discount brokers	denial of service attack	2/24/00	4.1	–1.8	–9.4
Microsoft	Denial of service attack over two days for MSN, MSNBC and Microsoft.com	1/25/01	–0.9	3.0	3.0
			–0.8	–2.9	–3.6
Theft of credit card information					
eUniverse (CD Universe)	On-line theft of credit card information for 300,500 customers	1/10/00	–18.0	–20.7	–24.6
First data (Western Union)	On-line theft of credit card information for 15,000 customers	9/8/00	–5.7	0.2	–0.8
Egghead.com	On-lline theft of credit card information for 3.3 million customers	12/18/00	–12.3	–15.5	–36.1
Playboy	On-line theft of credit card information	11/21/01	–1.1	–0.1	2.2
			–9.3	–9.0	–14.9

Company	Announcement	Date of announcement	*t* (%)	*t*+1 (%)	*t*+2 (%)
Denial of service					
Yahoo	Denial of service attack beginning at 12:15 p.m. EST	2/7/00	–3.4	–2.8	–2.7
eBay	Denial of service attack beginning at 6:00 p.m. EST	2/8/00	–3.7	–4.8	–10.1
Microsoft	Denial of service attack beginning at 9:00 p.m. on 2/8/00	2/9/00	–3.1	–1.5	–0.1
Amazon	Denial of service attack beginning at 8:00 p.m. EST	2/9/00	–0.5	–10.5	–4.4
Time Warner (CNN)	Denial of service attack beginning at 7:00 p.m. EST	2/9/00	2.1	1.6	1.8
E*Trade	Denial of service attack beginning at 4:00 a.m. EST	2/9/00	–2.0	–5.1	–4.7
ZDNet	Denial of service attack beginning at 4:00 a.m.	2/9/00	2.6	–3.2	–3.3
Excite@Home	Denial of service attack	2/10/00	–3.3	–3.2	–5.9
National discount brokers	denial of service attack	2/24/00	4.1	–1.8	–9.4
Microsoft	Denial of service attack over two days for MSN, MSNBC and Microsoft.com	1/25/01	–0.9	3.0	3.0
			–0.8	–2.9	–3.6
Theft of credit card information					
eUniverse (CD Universe)	On-line theft of credit card information for 300,500 customers	1/10/00	–18.0	–20.7	–24.6
First data (Western Union)	On-line theft of credit card information for 15,000 customers	9/8/00	–5.7	0.2	–0.8
Egghead.com	On-lline theft of credit card information for 3.3 million customers	12/18/00	–12.3	–15.5	–36.1
Playboy	On-line theft of credit card information	11/21/01	–1.1	–0.1	2.2
			–9.3	–9.0	–14.9
Web-site defacement					
Staples	Web site defacement and diversion of on-line traffic	10/11/99	0.3	4.6	0.9
RSA Security	Web site defacement	2/14/00	–9.5	–20.6	–17.2
Nike	Web site defacement and diversion of on-line traffic	6/21/00	–0.3	0.1	6.0
Diageo (Burger King)	Web site defaced	3/2/01	1.9	2.5	–1.0
British Telecom	Web site defaced	4/2/01	–2.3	–1.5	5.4
HSBC	Web site defaced	9/21/00	–1.6	–1.2	–0.6
			–2.0	–2.7	–1.1
Theft of customer information					
Microsoft	Hotmail defaced for two hours and hackers access accounts	8/30/99	1.4	2.1	0.7
Travelocity	On-line theft of personal information for 45,000 customers	1/23/01	–2.3	–3.7	2.3
Midwest Express	Hackers access customer information	4/26/02	4.32		
Midwest Express	Hackers access customer information	4/26/02			

Garg, Curtis, Halper, 2003

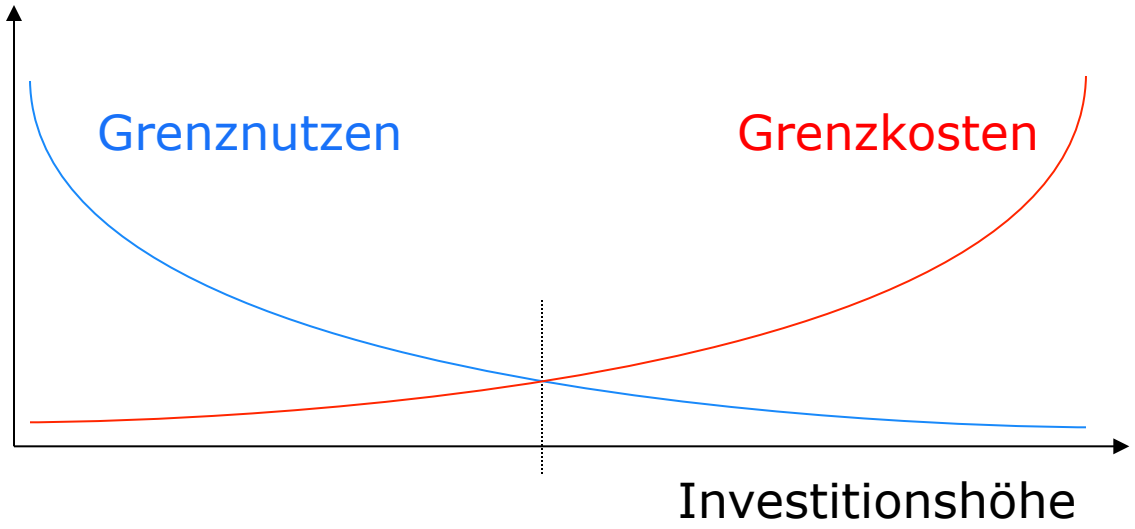
Motivation hinter Angriffen im Wandel der Zeit

- Hackerethik – Chaos Computer Club
  - Zugang zu Computern und allem, was einem zeigen kann, wie diese Welt funktioniert, sollte unbegrenzt und vollständig sein.
  - Alle Informationen müssen frei sein.
  - Misstraue Autoritäten – fördere Dezentralisierung.
  - Beurteile einen Hacker nach dem, was er tut und nicht nach üblichen Kriterien wie Aussehen, Alter, Rasse, Geschlecht oder gesellschaftlicher Stellung.
  - Man kann mit einem Computer Kunst und Schönheit schaffen.
  - Computer können dein Leben zum Besseren verändern.

Wieviel soll in IT-Sicherheit investiert werden?

So viel wie im Schnittpunkt von Grenzkosten und Grenznutzen an der Abszisse abzulesen ist.

- Kritik
  - Viel hilft nicht unbedingt viel, es kommt auch darauf an, wie das Geld ausgegeben wird



Wieviel soll in IT-Sicherheit investiert werden?

So viel wie im Schnittpunkt von Grenzkosten und Grenznutzen an der Abszisse abzulesen ist.

- Kritik
  - Viel hilft nicht unbedingt viel, es kommt auch darauf an, wie das Geld ausgegeben wird

- Effektivität
  - = die richtigen Maßnahmen ergreifen
  - Weniger ist manchmal mehr.
- Probleme
  - Funktionen sind schwierig zu ermitteln
  - Funktionen sind nicht stetig, häufig sind Sicherheitsmaßnahmen binäre Entscheidungen

Return on Security Investment (ROSI)

- Frage
  - »Waren die Maßnahmen effektiv und effizient? Wie sicher ist die Organisation?«

- ROSI
  - basiert auf dem ALE-Konzept (Annual Loss Expenditure) aus den 70er Jahren
  - soll Analogie zum klassischen Return on Investment herstellen
  - verschiedene Darstellungsformen und Weiterentwicklungen

ROSI – Return on Security Investment – »Ersparnis« durch Abwenden der wahrscheinlichen Schäden abzügl. der Kosten der Sicherheitsmaßnahmen

Return on Security Investment (ROSI)

R Recovery Costs – Kosten der wahrsch. Schäden
S Savings – Reduzierung der K. der wahrsch. S.
T Total Costs – Kosten der Maßnahmen
ALE Annual Loss Expenditure – verbl. Schadenskosten nach Vorfall

$$ALE = R - S + T$$

$$ROSI = R - ALE$$

$$ROSI = S - T$$

ROSI – Return on Security Investment – »Ersparnis« durch Abwenden der wahrscheinlichen Schäden abzügl. der Kosten der Sicherheitsmaßnahmen

nach: Pohlmann 2006

Return on Security Investment (ROSI)

- Beispiel
  - Webservice
    - Savings – Reduz. d. Kosten d. wahrsch. Schäden
      S = 100.000 EUR p.a. (Kunden- und Imageverlust)
    - Total Costs – Kosten der Maßnahmen
      T = 5.000 EUR p.a. (Zertifikat, Firewall, Updates etc.)

ROSI = S – T = 95.000 EUR p.a.

ROSI – Return on Security Investment – »Ersparnis« durch Abwenden der wahrscheinlichen Schäden abzügl. der Kosten der Sicherheitsmaßnahmen

nach: Pohlmann 2006

Return on Security Investment (ROSI)

- Kritik am ROSI
  - Kosten und Nutzen schwer ermittelbar → Unterschiede zu klassischen Investitionsprojekten
  - Es geht nicht nur um operative Entscheidungen: Sicherheitsmanagement beginnt auf der strategischen Ebene

- Worin liegt der Nutzen?
  - Erfüllung gesetzlicher Anforderungen, Generierung zusätzlicher Einnahmen, Effizienzgewinne, Reduktion von Risiken

- Wie setzen sich die Kosten zusammen?
  - Ausgaben für Anschaffung, Einführung, laufenden Betrieb, Kosten durch Änderung betriebl. Abläufe

Risikomanagement-Ansatz auf operativer Ebene erforderlich

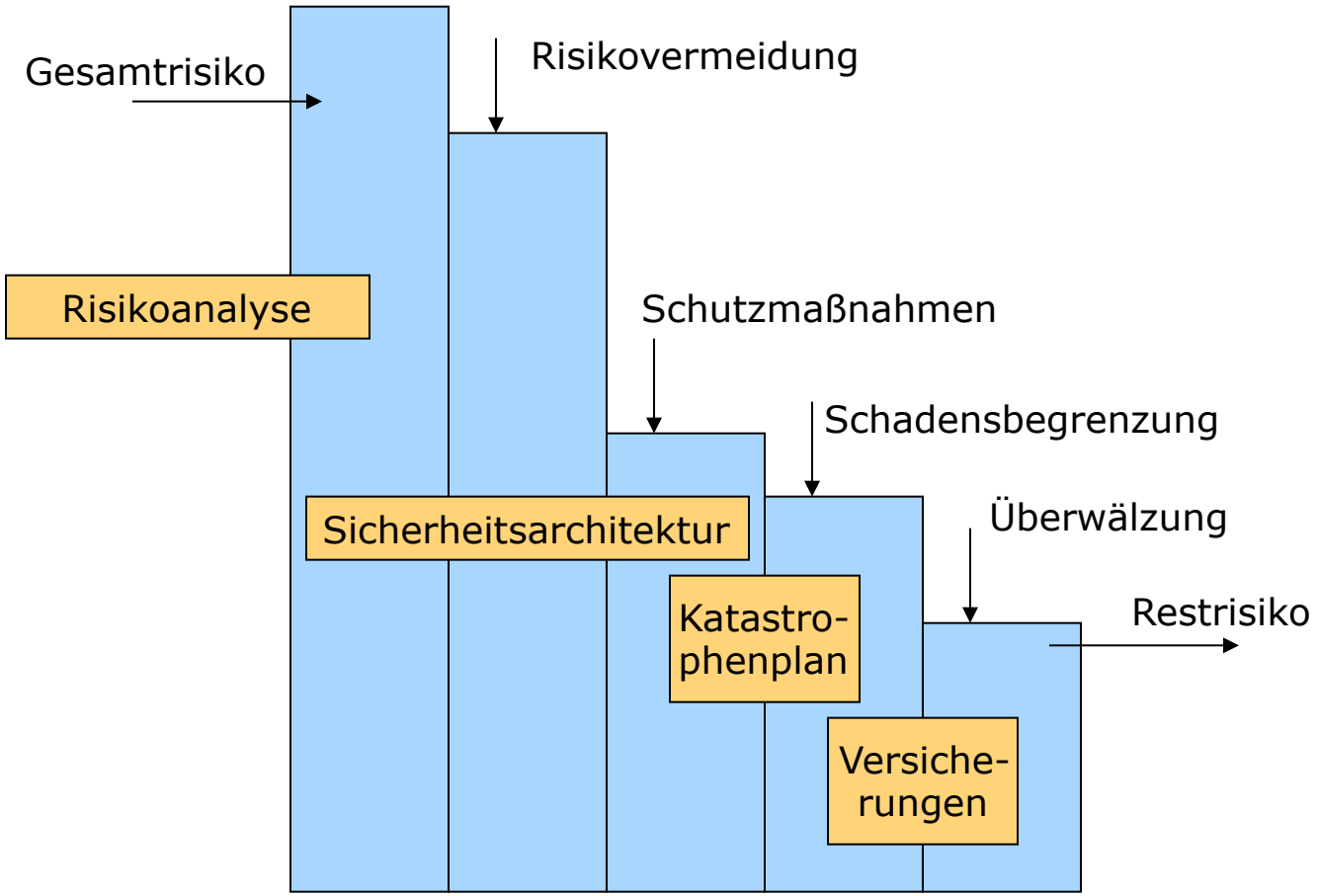
Sicherheitsmanagement beginnt auf der Strategieebene

	Business Engineering	Sicherheitsmanagement
Strategieebene/ Sicherheitspolitik	Festlegung der Unternehmens-aufgaben; Strategische Planung	Definition strategischer Ziele, Grundsätze und Richtlinien; Formulierung der Unterneh-mensziele aus Sicherheitssicht
Prozessebene/ Sicherheitskonzept	Gestaltung der Abläufe in Form von Prozessen	Übersetzung der Politik in Maßnahmen; Risikoanalyse
Systemebene/ Mechanismen	Unterstützung der Prozesse durch den Einsatz von Systemen; Analyse und Spezifikation der Anwendungssysteme	Detaillierung der Maßnahmen durch konkrete Mechanismen

Sicherheitsmanagement beginnt auf der Strategieebene

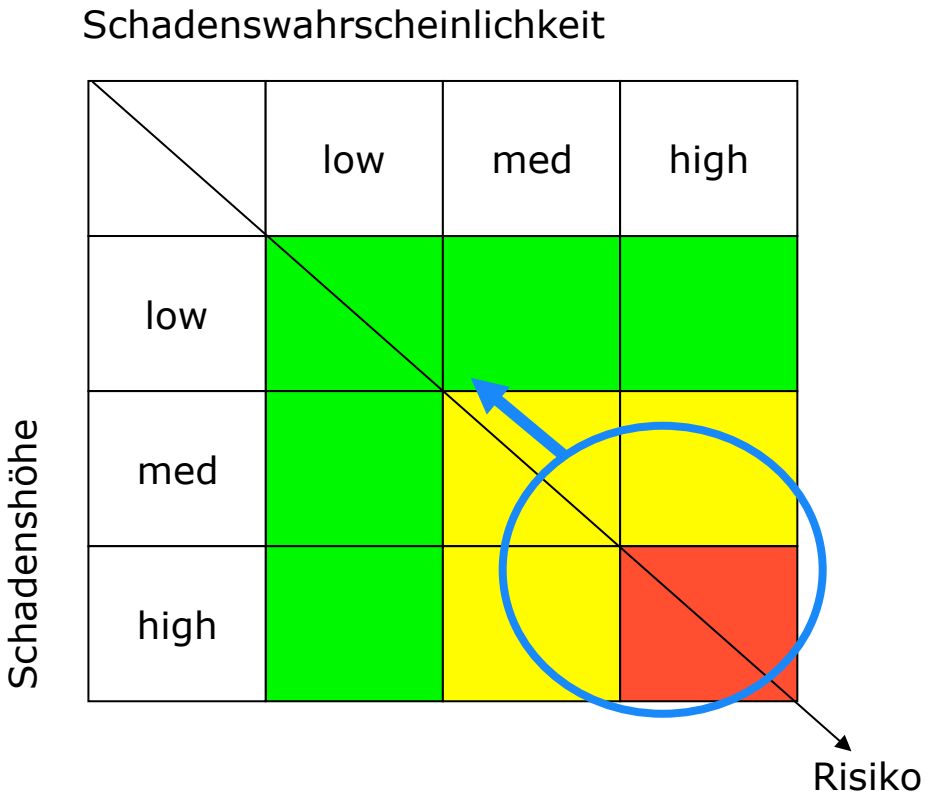
- Aussagen für die strategische Ebene
  - Wer nur auf vorgefertigte Lösungen setzt, verliert auf lange Sicht wertvolles Know How.
  - Heterogene IT-Landschaften schützen vor Kumulrisiken.
  - IT-Sicherheit ist mehr als nur Technik.
  - Sicherheit sollte von Beginn an integraler Bestandteil der Prozesse werden und nicht hinterher hinzugebastelt werden.
  - Die Sicherheit sollte im Einklang mit anderen Disziplinen entwickelt werden, z.B. Synergien mit dem Business Engineering nutzen.

Risiko-Management für IT-Systeme

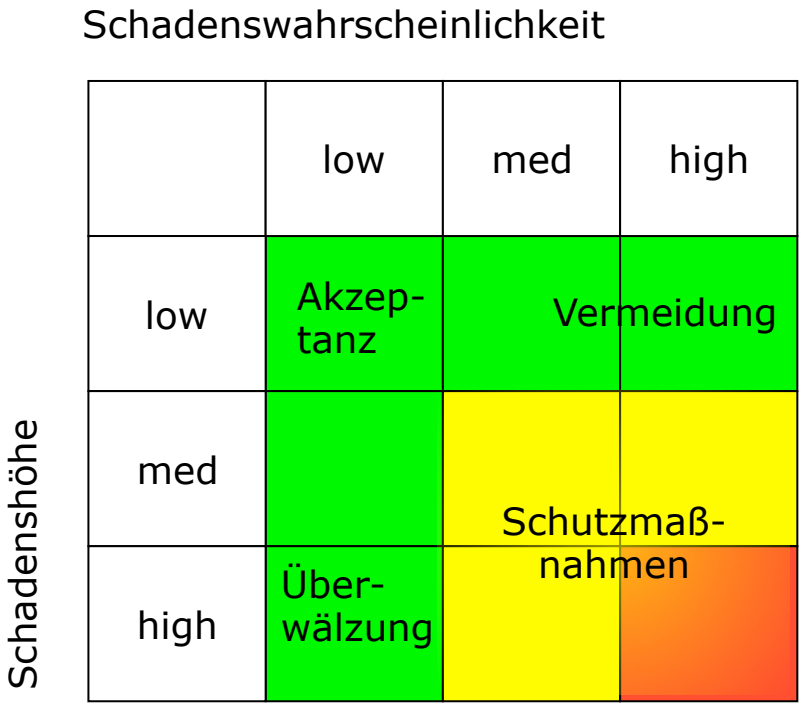


nach: Schaumüller-Bichl

Risiko-Management für IT-Systeme



Typische Positionen für Vermeidung, Akzeptanz und Überwälzung:



Operative Ebene – Betrachtung im Risikomanagement Kreislauf

Checklisten
Workshops
Experten
Histor. Daten

Identifikation

Basisansatz
Kategorien
Quantitative
Verfahren

Bewertung

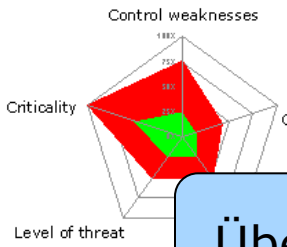
Best Practice
Scoring
Quant.
Verfahren

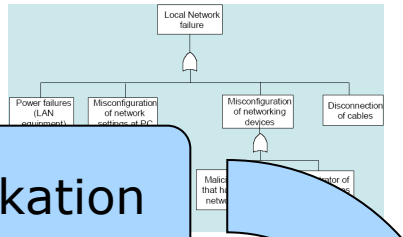
Steuerung

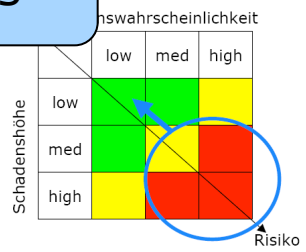
Checklisten
Scorecards
Kennzahlen

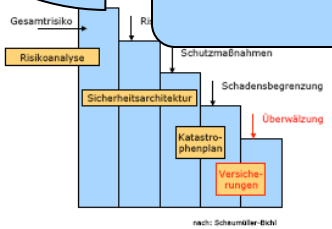
Überwachung

Risiko =
Eintrittswahrschein-
lichkeit · Schadenshöhe









Universität Hamburg
Fachbereich Informatik
Arbeitsbereich SVS
Prof. Dr. Hannes Federrath
Vogt-Kölln-Straße 30
D-22527 Hamburg

E-Mail federrath@informatik.uni-hamburg.de

Telefon +49 40 42883 2358

http://svs.informatik.uni-hamburg.de

Universität Hamburg
DER FORSCHUNG | DER LEHRE | DER BILDUNG