IT-Security – ein Überblick

Prof. Dr. Hannes Federrath
Sicherheit in verteilten Systemen (SVS)
http://svs.informatik.uni-hamburg.de

Universität Hamburg
DER FORSCHUNG | DER LEHRE | DER BILDUNG

VOQUZ Expertentag »IT Sicherheit in unsicheren Zeiten«
Hamburg, 17. November 2015

Der Arbeitsbereich Sicherheit in Verteilten Systemen (SVS)

- Unsere Forschungsthemen (Auswahl)
  - Informationssicherheitmanagement, IT-Grundschutz, ISO 27001
  - Privacy im Internet, Schutz vor Beobachtung, IT-Forensik
  - Sichere und datenschutzfreundliche Vernetzung von Fahrzeugen
  - Sicherheit und Datenschutz in mobilen Systemen

- Beiträge und (interdisziplinäre) Ergebnisse
  - Begleitung von Gesetzgebungsverfahren aus technischer Sicht
  - Erforschung des Spannungsfeldes von Freiheit und Sicherheit
  - Technische Lösungen zum Grundrechtsschutz
  - Informatik als gesellschaftliche Aufgabe

- Weitere Informationen
  - https://svs.informatik.uni-hamburg.de

Agenda

- Von der Bedrohung zum Sicherheitsvorfall
- Risikomanagement Kreislauf
- Vorgehensmodell Informationssicherheitsmanagement
- Querbezüge von Datensicherheit und Datenschutz
- Technische Maßnahmen zum Schutz von Vertraulichkeit, Integrität und Verfügbarkeit
- Schlussbemerkungen

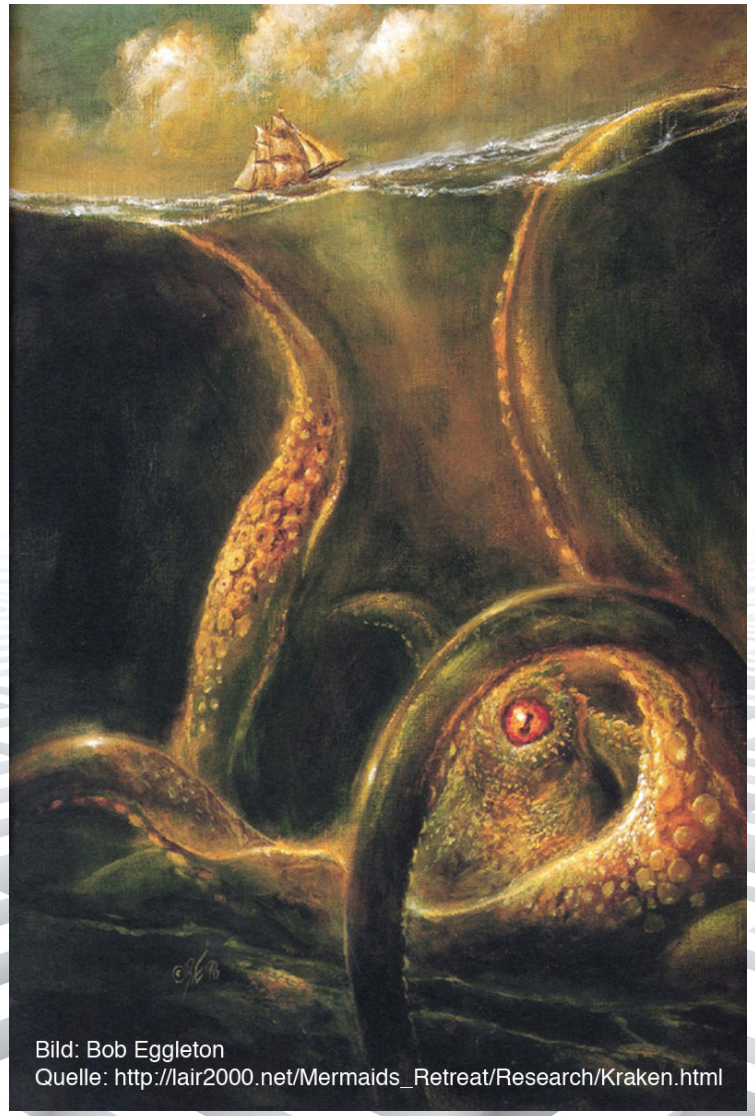


Bild: Bob Eggleton
Quelle: http://lair2000.net/Mermaids_Retreat/Research/Kraken.html

FUD-Strategie — Fear, Uncertainty, Doubt

Wieviel muss wirklich in Sicherheit investiert werden?

vs.

Furcht, Ungewissheit, Zweifel

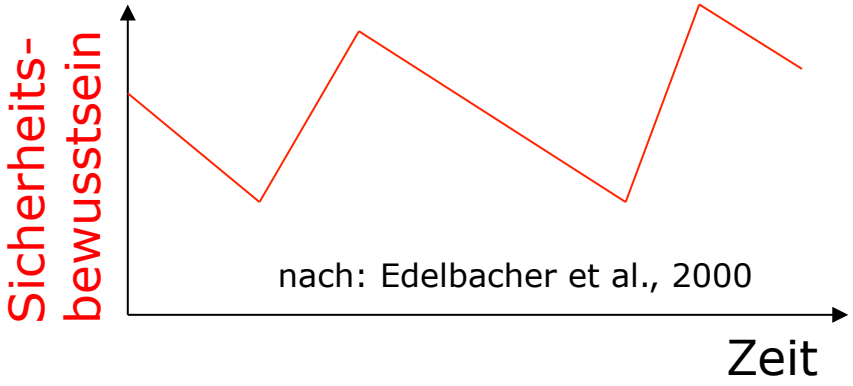


Bild: Bob Eggleton
Quelle: http://lair2000.net/Mermaids_Retreat/Research/Kraken.html

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

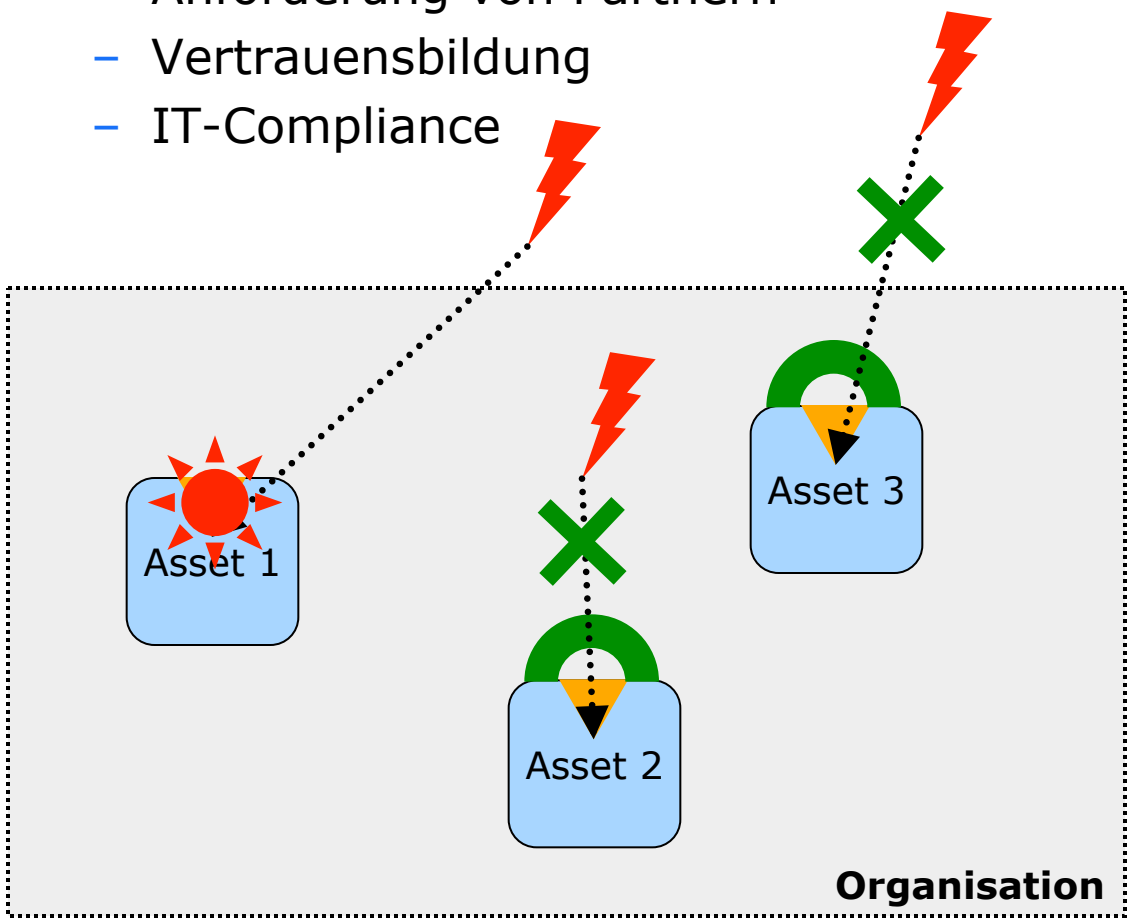
Company	Announcement	Date of announcement	*t* (%)	*t*+1 (%)	*t*+2 (%)
Denial of service					
Yahoo	Denial of service attack beginning at 12:15 p.m. EST	2/7/00	–3.4	–2.8	–2.7
eBay	Denial of service attack beginning at 6:00 p.m. EST	2/8/00	–3.7	–4.8	–10.1
Microsoft	Denial of service attack beginning at 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
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
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

Von der Bedrohung zum Sicherheitsvorfall

- Warum IT-Sicherheitsmanagement?
  - Schutz von Unternehmenswerten (Assets)
  - Anforderung von Partnern
  - Vertrauensbildung
  - IT-Compliance



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

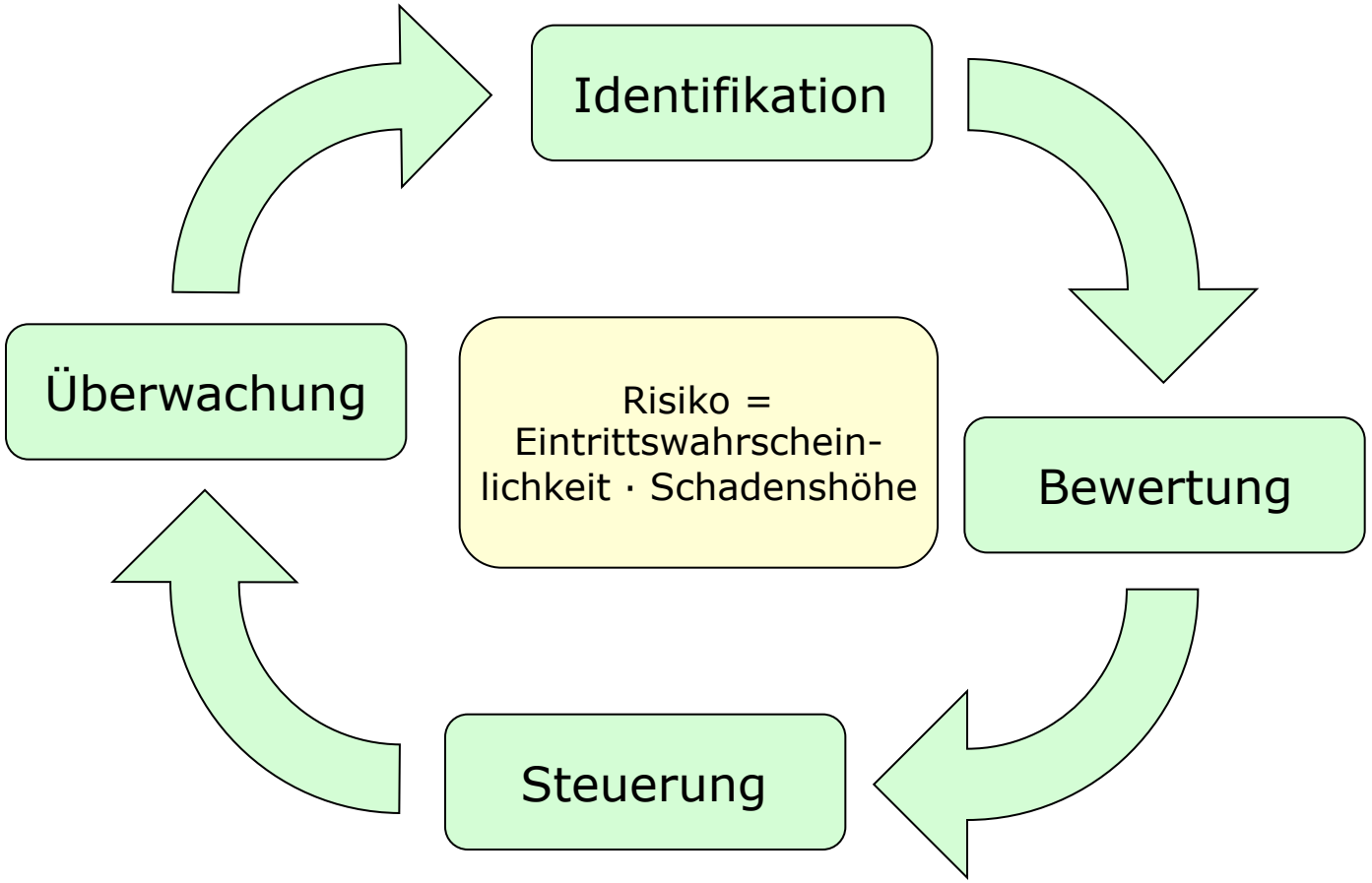
Verwundbarkeiten, z.B.
- Konfigurationsfehler
- Buffer Overflows

Schutzziele
- Vertraulichkeit
- Integrität
- Verfügbarkeit

Maßnahmen
- Präventiv
- Detektiv
- Reaktiv

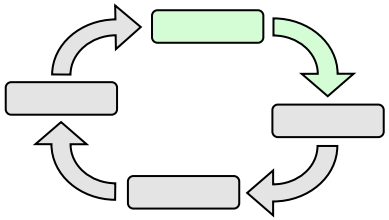
vgl. Nowey, 2011

Risikomanagement Kreislauf

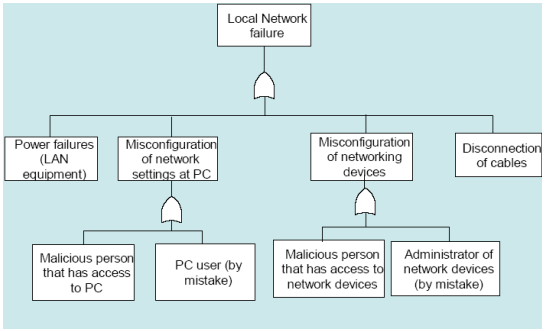


Identifikation von Bedrohungen

- Frage
  - »Welche Bedrohungen sind für das jeweilige Schutzobjekt relevant?«



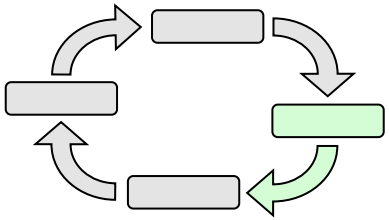
- Methoden & Werkzeuge
  - OCTAVE-Methodik, CORAS-Framework
  - Checklisten
  - Workshops
  - Fehlerbäume, Attack-Trees
  - Szenarioanalysen



- Herausforderungen
  - Vollständige Erfassung aller Bedrohungen

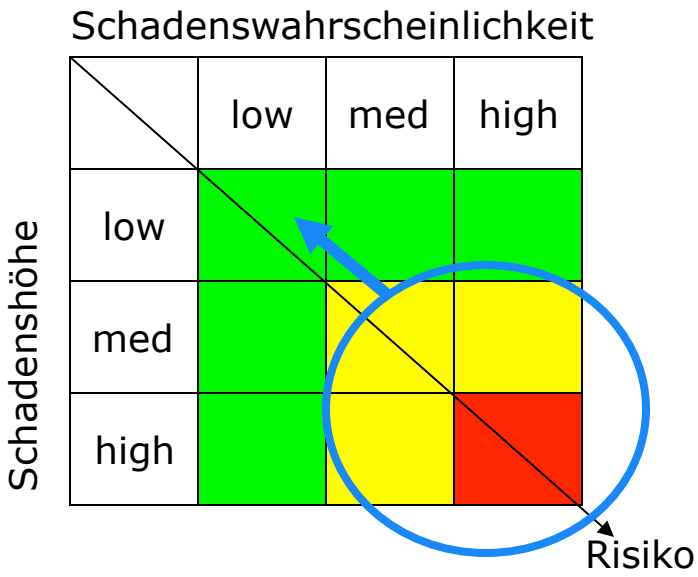
Bewertung von Risiken

- Frage
  - »Wie groß sind Eintrittswahrscheinlichkeit und Schadenshöhe eines potentiellen Schadensereignisses?«



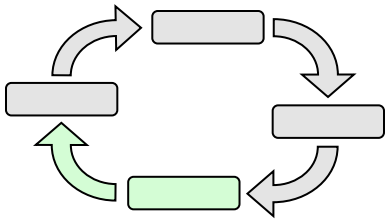
- Methoden & Werkzeuge
  - Qualitative Bewertung
  - Quantitative Bewertung
  - Spieltheorie
  - Maximalwirkungsanalyse

- Herausforderungen
  - Abhängigkeit von den Assets
  - Strategische Angreifer
  - Korrelationen
  - Quantifizierbarkeit



Steuerung der Risiken

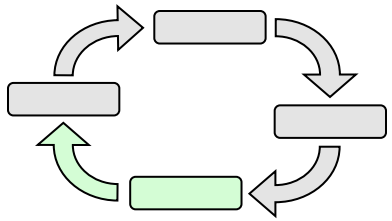
- Frage
  - »Welche Risiken sollen wie behandelt werden?«

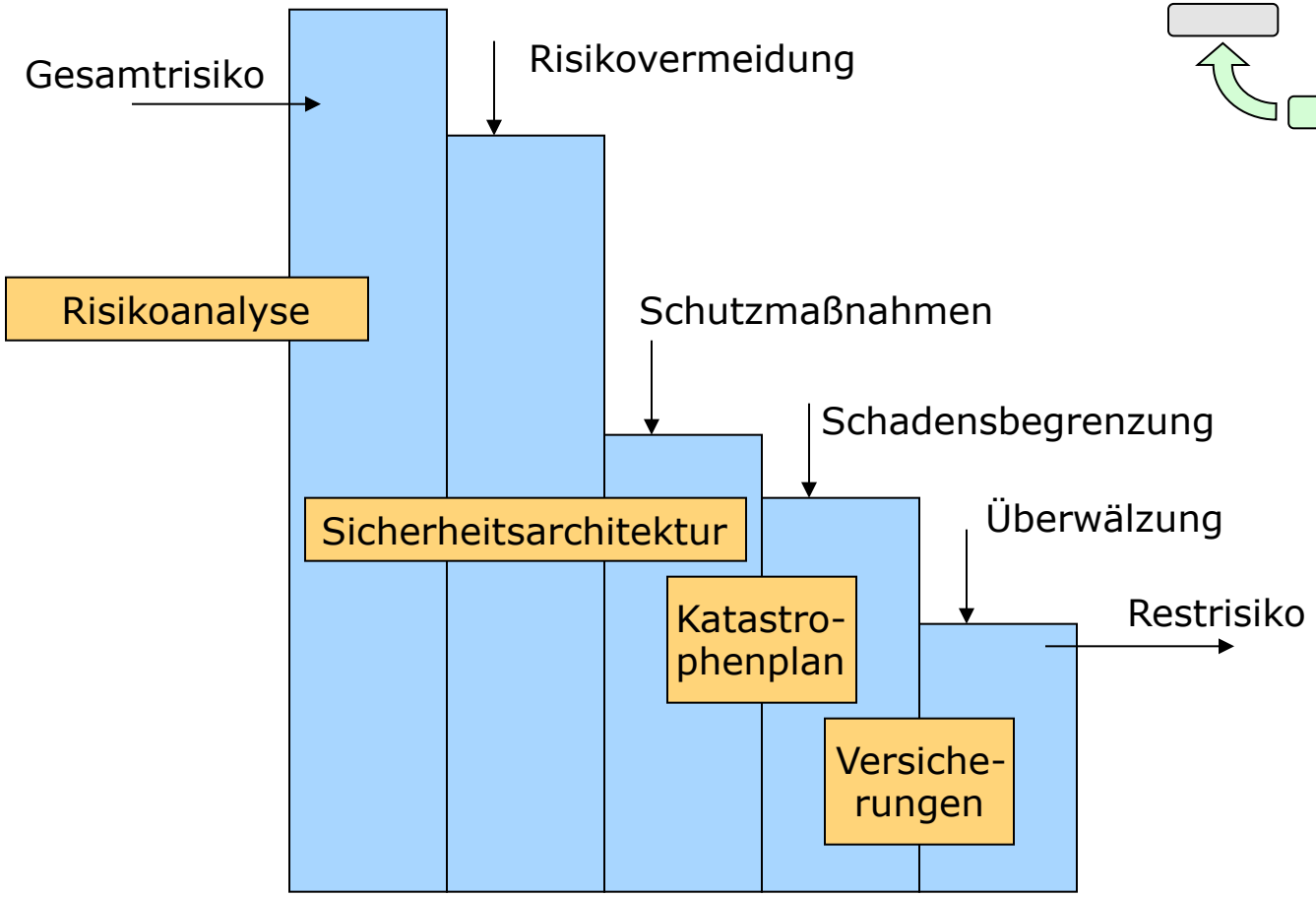


- Methoden
  - Risikovermeidung
  - Risikobehandlung (z.B. nach IT-Grundschutz und ISO 27002)
  - Risikoüberwälzung
  - Risikoakzeptanz

- Herausforderungen
  - Komplexität der Problemstellung
  - Finden von geeigneten Musterlösungen
  - Komposition eines sicheren Gesamtsystems aus sicheren Teillösungen

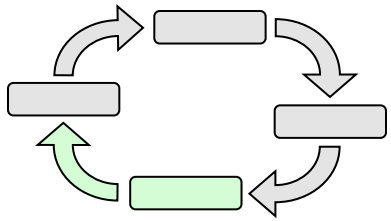
Risiko-Management für IT-Systeme

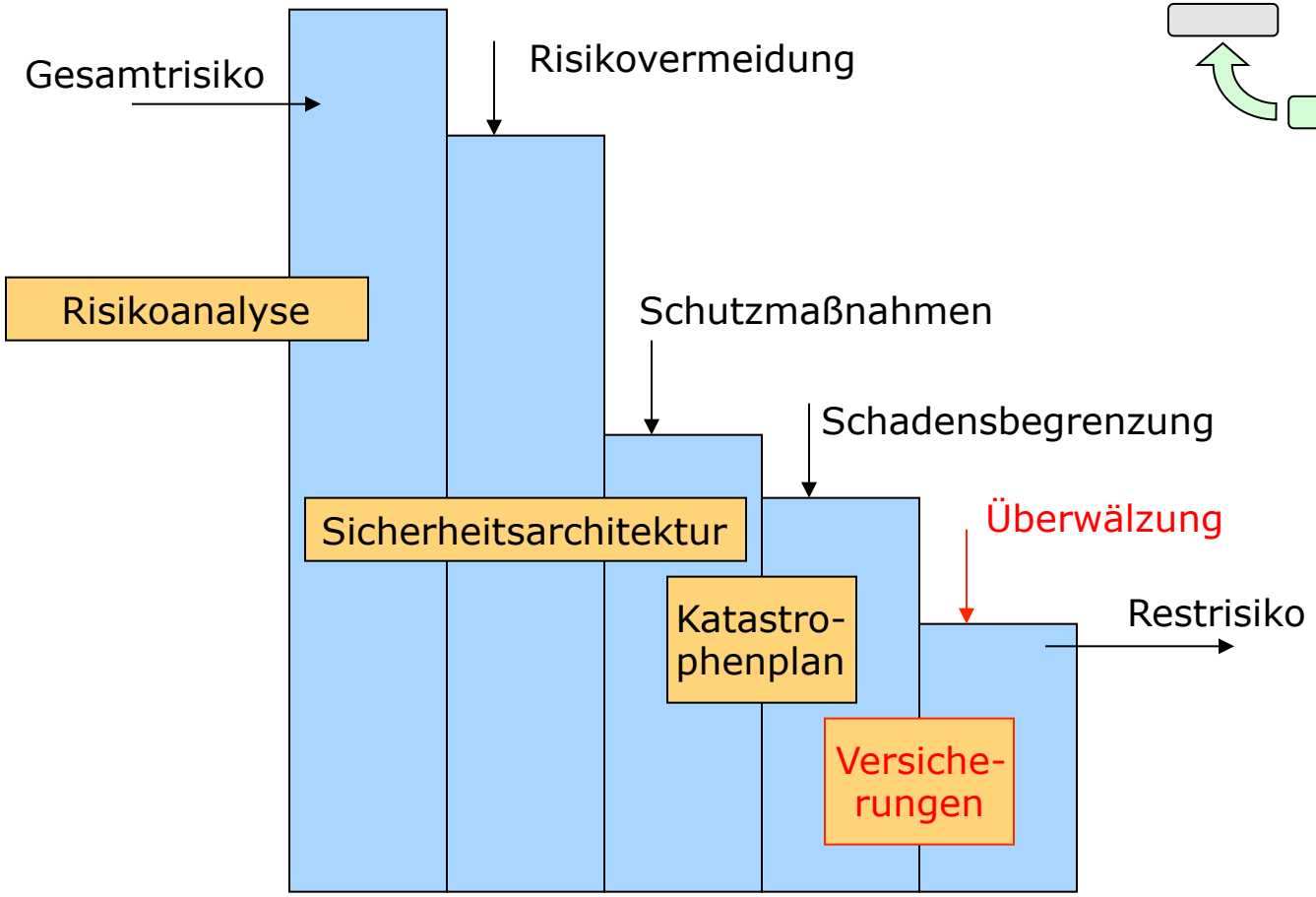




nach: Schaumüller-Bichl

Risiko-Management für IT-Systeme

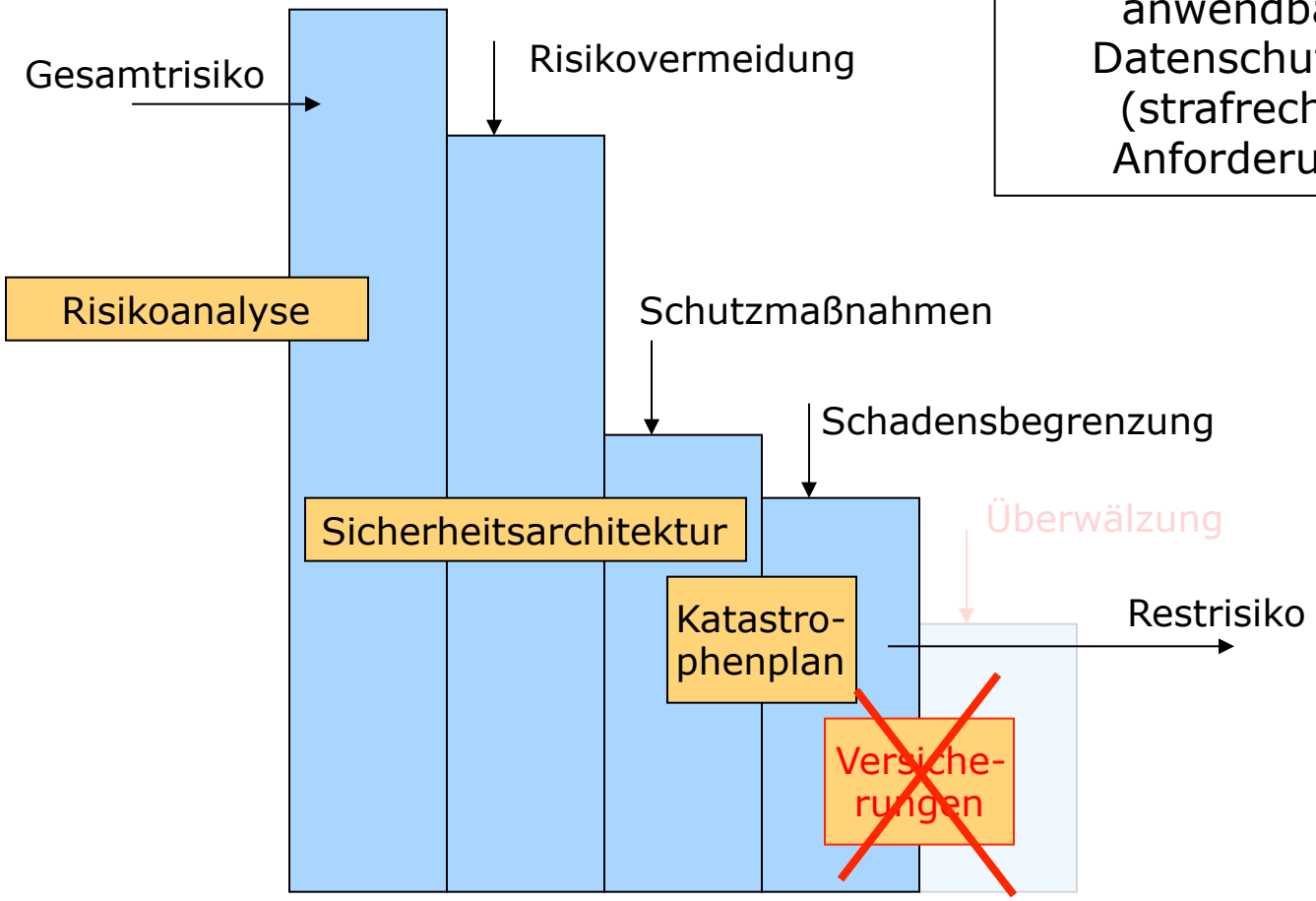




nach: Schaumüller-Bichl

Risiko-Management im Datenschutz

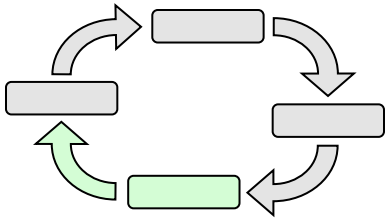
Überwälzung nicht anwendbar auf Datenschutz (und (strafrechtliche Anforderungen)



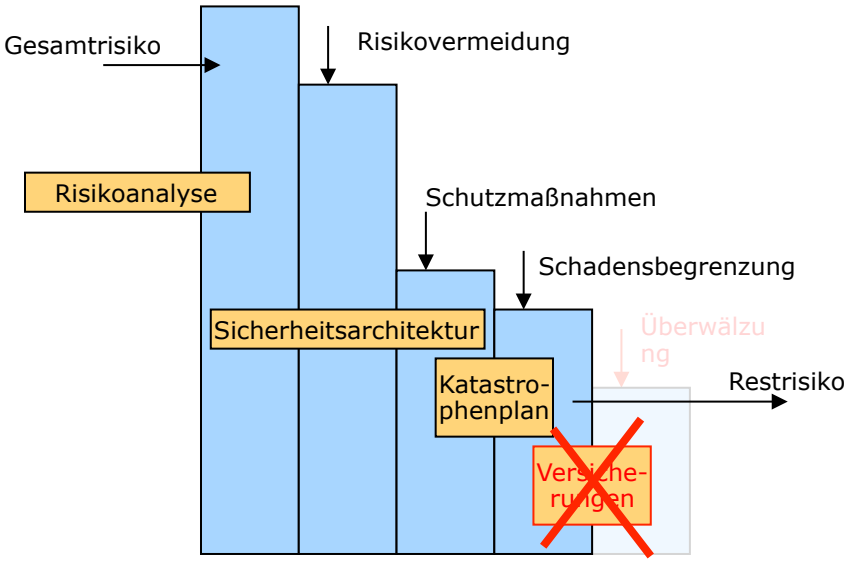
nach: Schaumüller-Bichl

Risiko-Management im Datenschutz

- IT-Sicherheit:
  - Risiko = Wahrscheinlichkeit · Schadenshöhe
  - Schäden sind systematisch tolerierbar

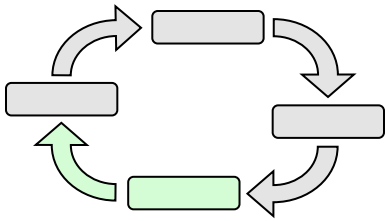


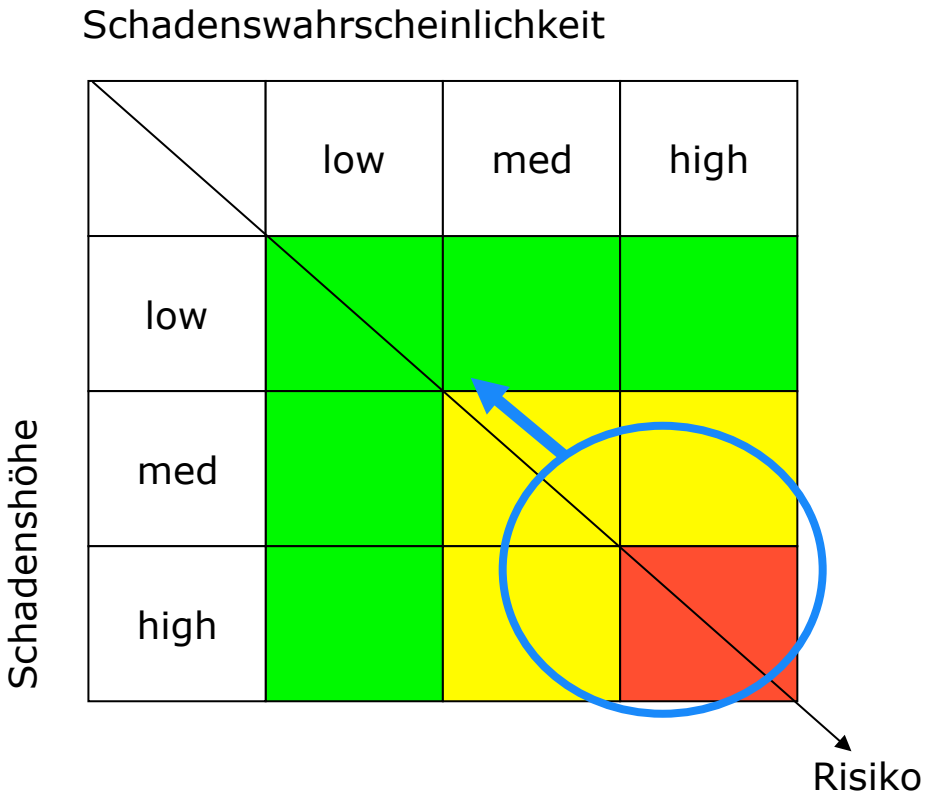
- Datenschutz:
  - Alles-Oder-Nichts-Ansatz
  - Rechtliche Vorgaben müssen umgesetzt werden



nach: Schaumüller-Bichl

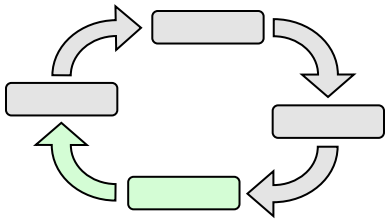
Risiko-Management für IT-Systeme





Risiko-Management für IT-Systeme

Typische Positionen für Vermeidung, Akzeptanz und Überwälzung:

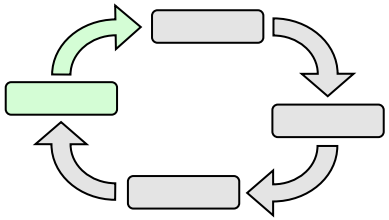


Schadenswahrscheinlichkeit

Schadenshöhe	low	med	high
low	Akzep-tanz	Vermeidung	Vermeidung
med		Schutzmaß-nahmen	Schutzmaß-nahmen
high	Über-wälzung	Schutzmaß-nahmen	Schutzmaß-nahmen

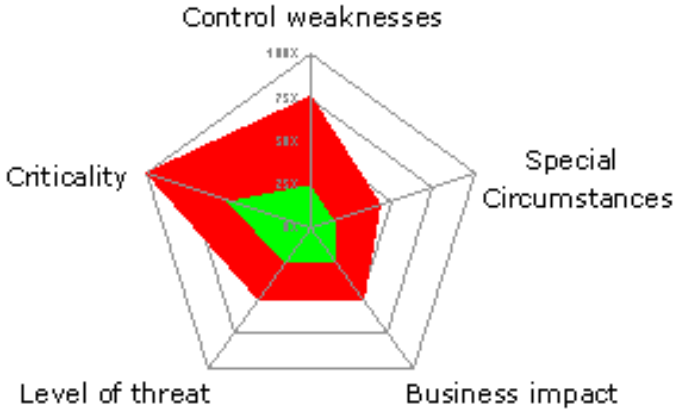
Überwachung der Risiken und Maßnahmen

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



- Methoden
  - Kennzahlen- und Scorecard-Systeme
  - Return on Security Investment (ROSI)

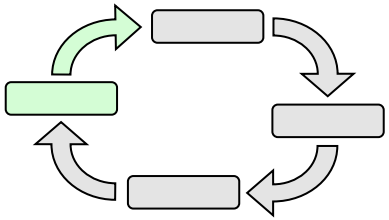
- Herausforderungen
  - Die »richtigen« Kennzahlen verwenden
  - Kennzahlen »richtig« ermitteln/messen
  - Kennzahlen aktuell halten



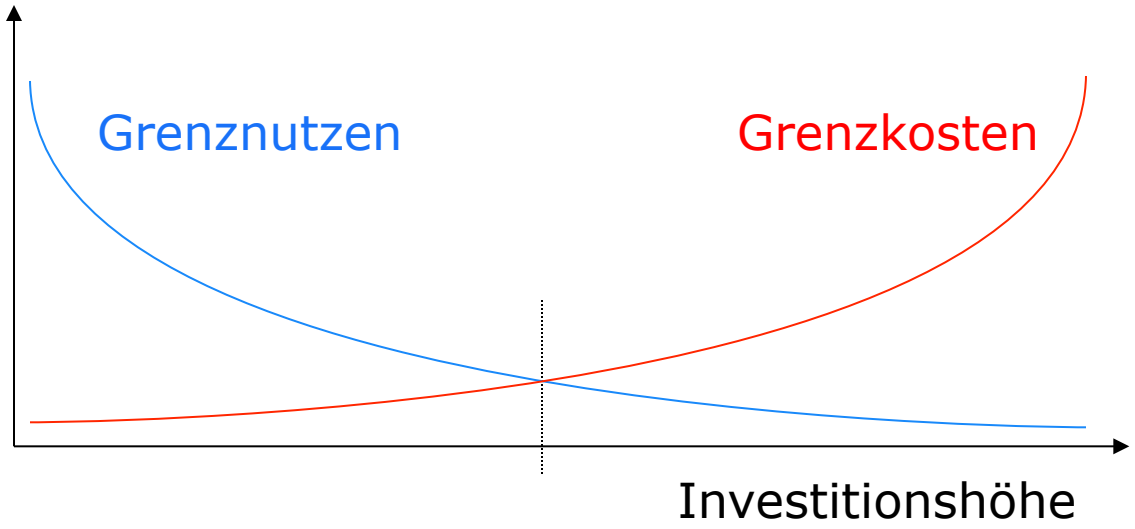
nach: Loomans, 2002

Überwachung der Risiken und Maßnahmen

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



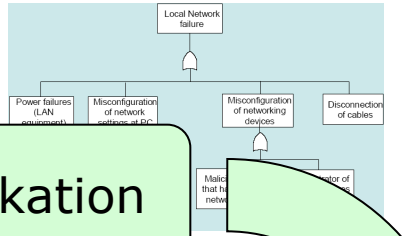
Viel hilft nicht unbedingt viel, es kommt auch darauf an, wie das Geld ausgegeben wird



Risikomanagement Kreislauf

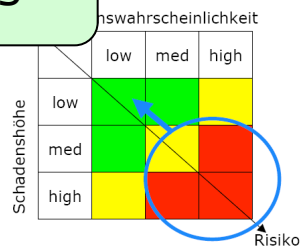
Checklisten
Workshops
Experten
Histor. Daten

Identifikation



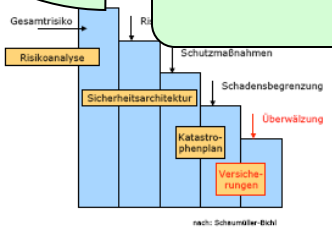
Basisansatz
Kategorien
Quantitative
Verfahren

Bewertung



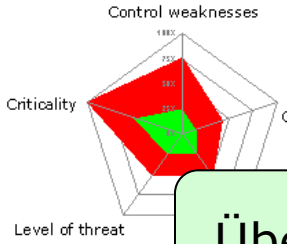
Risiko =
Eintrittswahrschein-
lichkeit · Schadenshöhe

Steuerung



Best Practice
Scoring
Quant.
Verfahren

Überwachung



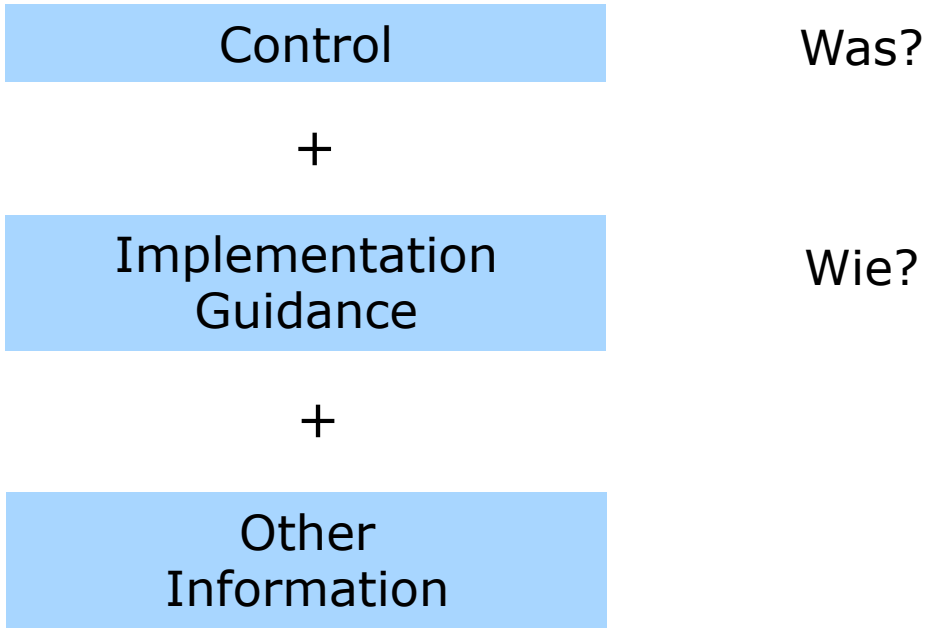
Checklisten
Scorecards
Kennzahlen

Internationaler Standard ISO 27002

- Control Areas
  1. Security Policy
  2. Organization of Information Security
  3. Human Resources Security
  4. Asset Management
  5. Access Control
  6. Cryptography
  7. Physical and Environmental Security
  8. Operations security
  9. Communications Security
  10. Information Systems Acquisition, Development, Maintenance
  11. Supplier Relationships
  12. Information Security Incident management
  13. Information Security Aspects of Business Continuity
  14. Compliance

Grundsätzlicher Aufbau der Controls

- Controls=Maßnahmen



Beispiel für ein Control

Bewusstsein, Ausbildung und Schulung für Informationssicherheit

8.2.2 nach ISO27002:2005
7.2.2 nach ISO27002:2013

Maßnahme

Alle Angestellten der Organisation, und, falls relevant, Auftragnehmer und Drittbenutzer, sollten geeignete Schulungen zur Bewusstseinsbildung erhalten, und regelmäßige Aktualisierungen bei organisationseigenen Politiken und Verfahren, die für ihre Arbeit von Bedeutung sind.

Anleitung zur Umsetzung

Die Schulung zur Bewusstseinsbildung sollte mit einem formalen Einführungsprozess beginnen, um die Sicherheitspolitiken und Erwartungen der Organisation vorzustellen, bevor Zugang zu Informationen oder Services gestattet wird.

Fortlaufende Schulungen sollten Sicherheitsanforderungen, gesetzliche Verantwortung und Geschäftsmaßnahmen beinhalten, genauso wie Schulungen in der ordnungsgemäßen Anwendung von informationsverarbeitenden Einrichtungen, z.B. Verfahren zum Einloggen, Benutzung von Programmpaketen und Informationen über Disziplinarverfahren (siehe 8.2.3);

Weitere Informationen

Die Aktivitäten für Sicherheitsbewusstsein, Ausbildung und Schulung sollten passend und von Bedeutung für die Aufgaben, Verantwortung und Fähigkeiten der Person sein, und sollten Informationen über bekannte Bedrohungen, wer für weiteren Rat in Sicherheitsfragen zu kontaktieren ist, und die geeigneten Kanäle für das Berichten von Informationssicherheitsvorfällen (siehe auch 13.1) enthalten.

Schulungen zur Verbesserung des Bewusstseins sollten es ermöglichen, dass Personen Informationssicherheitsprobleme und –Vorfälle erkennen, und dass sie im Einklang mit den Erfordernissen ihrer Arbeitsaufgabe reagieren.

IT-Grundschutz

Online erhältlich unter
http://www.bsi.de/gshb/

BSI-Standards
grundsätzliche Empfehlungen

- 100-1: ISMS
- 100-2: IT-Grundschutz-Vorgehensweise
- 100-3: Risikoanalyse
- 100-4: Notfallmanagement

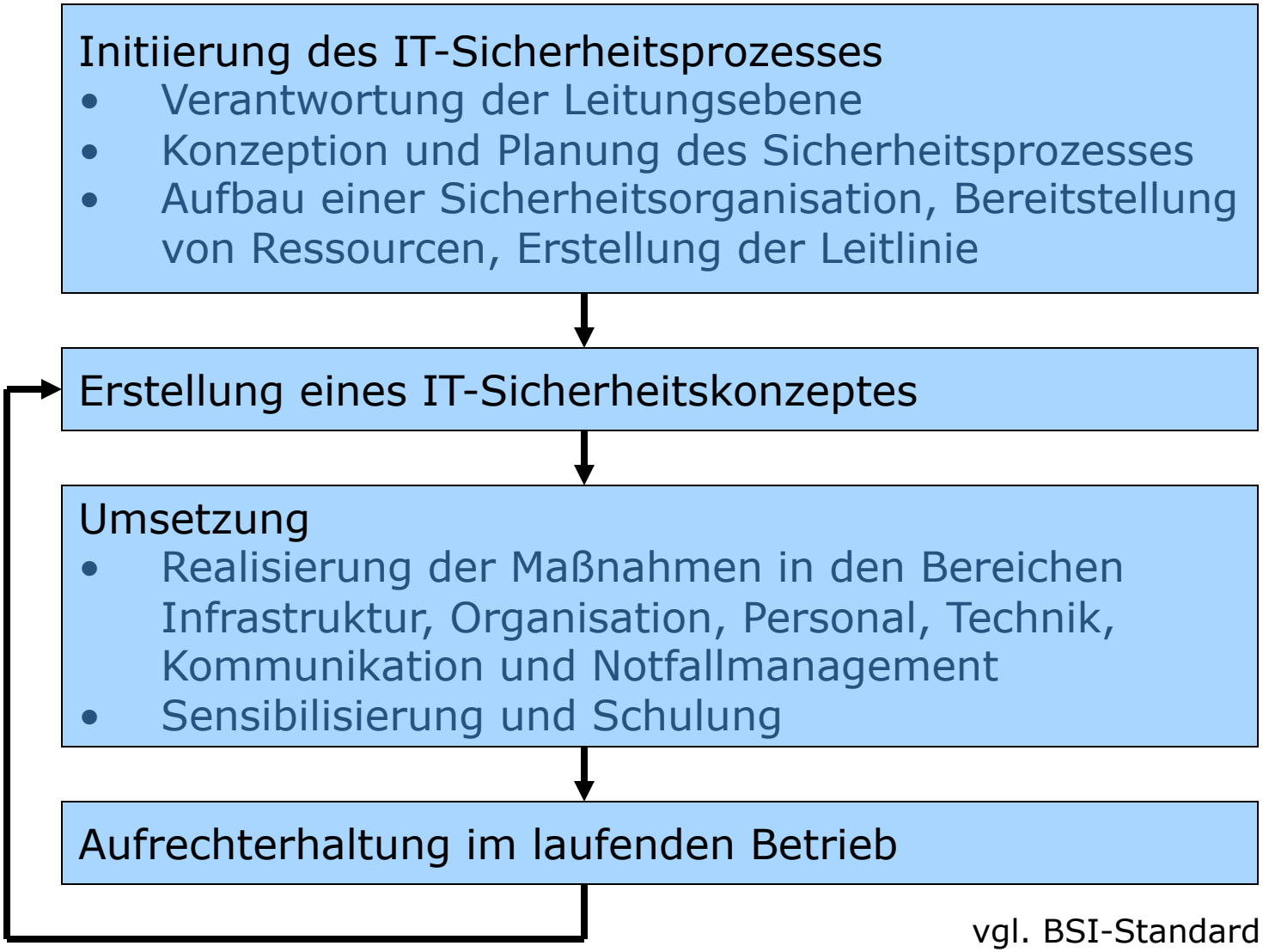
Grundschutz-Kataloge
Handlungsempfehlungen

ca. 4000 Seiten

- Bausteine
- Gefährdungskataloge
- Maßnahmenkataloge

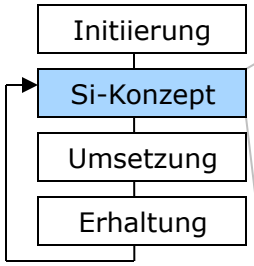
Grundschutz-Zertifikat
Bestätigung der Umsetzung

Der IT-Sicherheitsprozess nach BSI-Standard 100-2



vgl. BSI-Standard 100-2

Erstellung eines IT-Sicherheitskonzepts



IT-Strukturanalyse
- Erfassung der IT und der IT-Anwendungen
- Gruppenbildung

Schutzbedarfsfeststellung

IT-Grundschutzanalyse
- Modellierung nach IT-Grundschutz
- Basis-Sicherheitscheck mit Soll-Ist-Vergleich

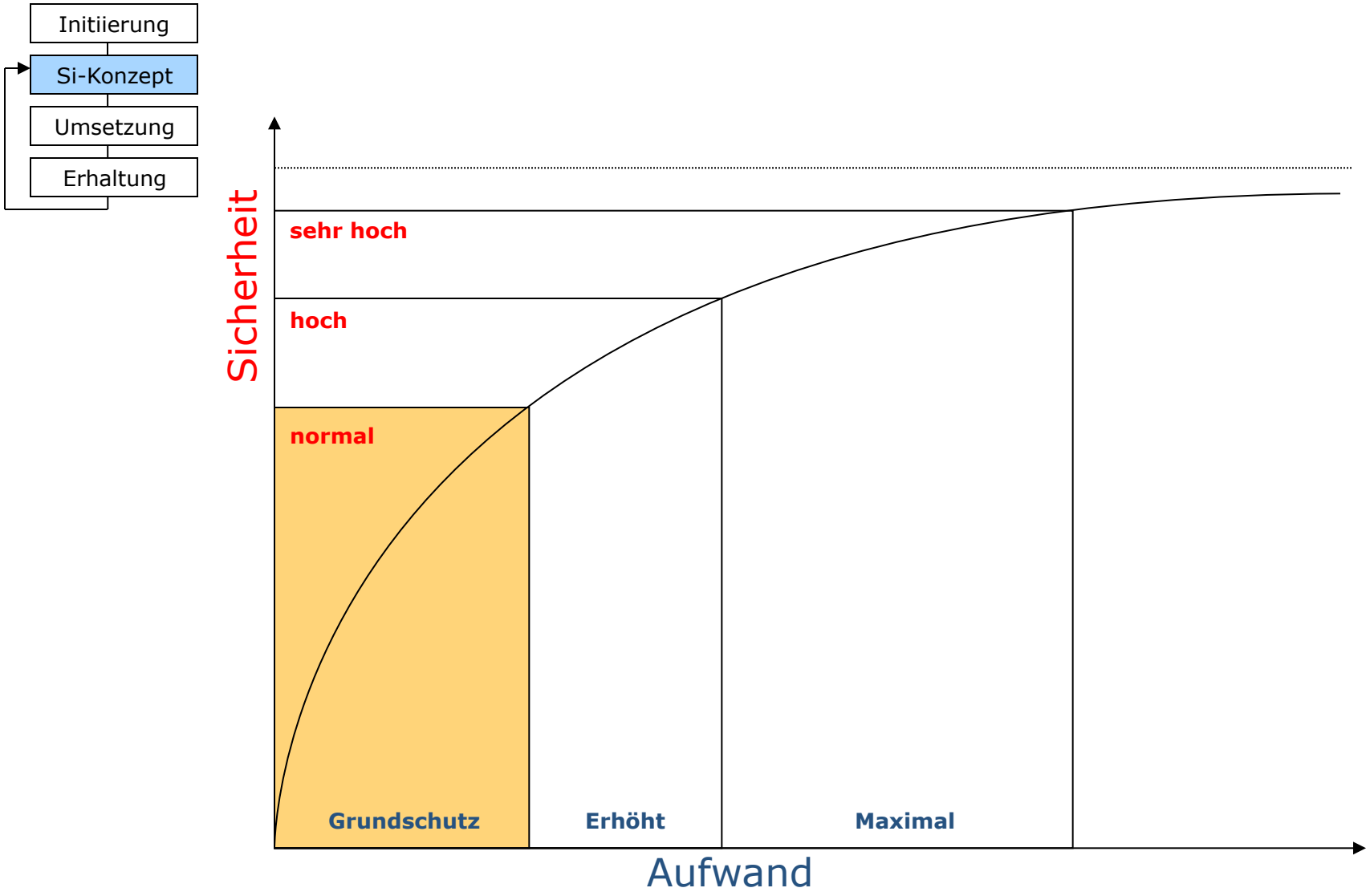
Ergänzende Sicherheitsanalyse
- bei hohem Schutzbedarf
- bei zusätzlichem Analysebedarf

Konsolidierung der Maßnahmen

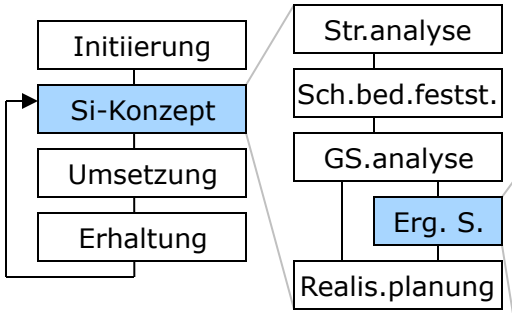
Realisierung der Maßnahmen („Planung der …")

vgl. BSI-Standard 100-2

Aufwand-Nutzen-Relation nach BSI-Standard 100-2



Risikoanalyse auf der Basis von IT-Grundschutz (BSI 100-3)



Gefährdungsübersicht
- Tabelle, die jedem Zielobjekt eine Liste mit relevanten Gefährdungen zuordnet

Zusätzliche Gefährdungen
- Gefährdungen die nicht im Grundschutz-Katalog enthalten sind

Gefährdungsbewertung
- Ausreichender Schutz durch Mechanismen des Maßnahmen-Katalogs?

Behandlung von Risiken
- Risiko-Reduktion durch zusätzliche Maßnahmen oder Umstrukturierung, Risiko-Transfer, Risiko-Akzeptanz

Konsolidierung der Maßnahmen

vgl. BSI-Standard 100-3

IT-Grundschutz-Zertifikat

- Seit 2002 erhältlich
- Seit 2006 Anpassung an internationale Zertifizierung

- 2 Vorstufen, werden von BSI-lizenzierten Auditoren vergeben
  - IT-Grundschutz Einstiegsstufe
  - IT-Grundschutz Aufbaustufe

- ISO 27001-Zertifikate auf Basis von IT-Grundschutz
  - Überprüfung durch einen BSI-lizenzierten ISO 27001-Grundschutz-Auditor: Sichtung der Referenzdokumente, Vor-Ort-Prüfung, Report
  - BSI entscheidet auf Basis des Audit-Reports und des ISO 27001-Grundschutz-Zertifizierungsschemas (http://www.bsi.de/gshb/zert/ISO27001/schema.htm)

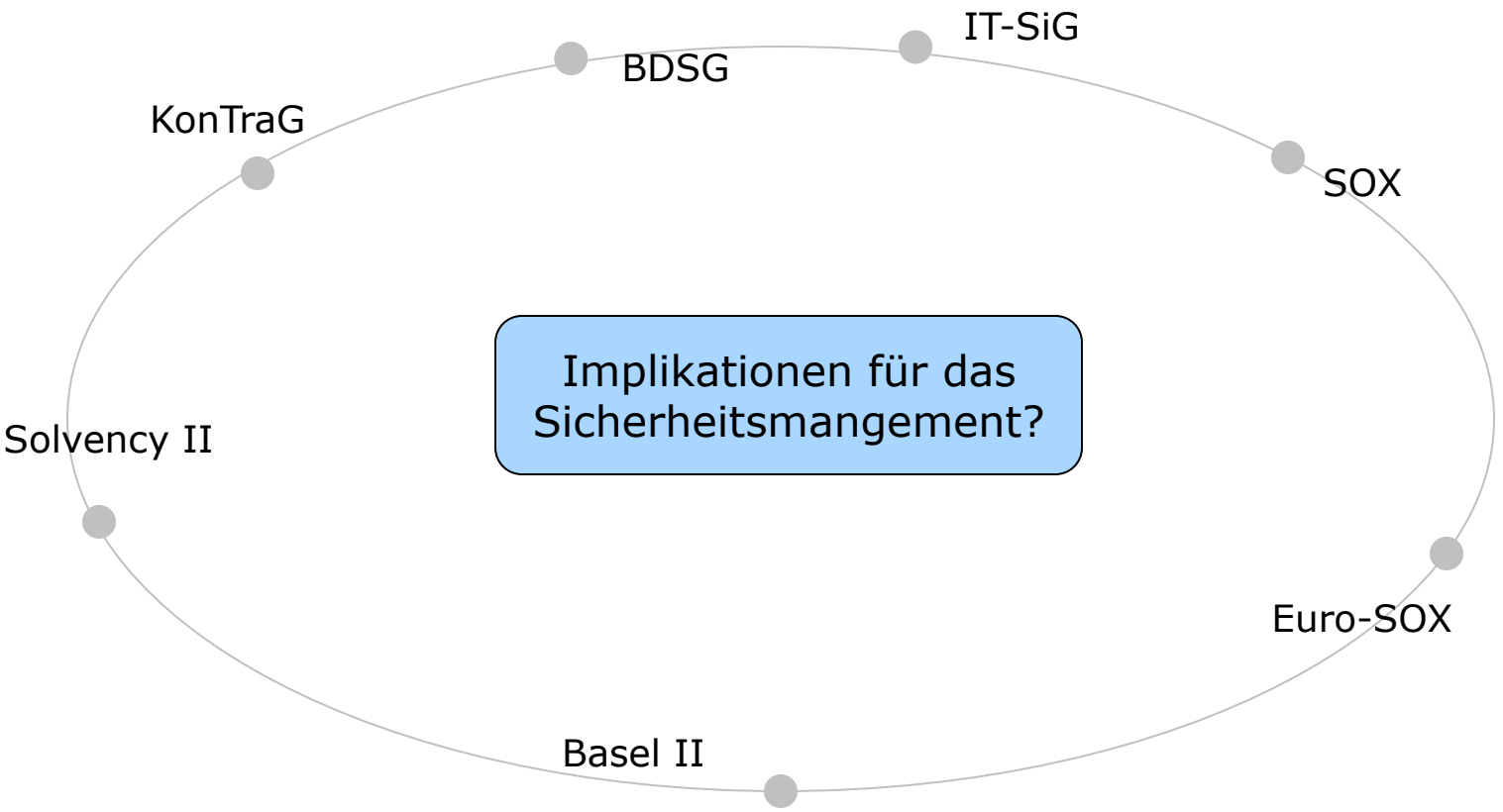
- Für Auditoren existiert ein Lizenzierungsschema (basierend auf ISO 27006)

Internationaler Standard ISO 27002

- Control Areas
  1. Security Policy
  2. Organization of Information Security
  3. Human Resources Security
  4. Asset Management
  5. Access Control
  6. Cryptography
  7. Physical and Environmental Security
  8. Operations security
  9. Communications Security
  10. Information Systems Acquisition, Development, Maintenance
  11. Supplier Relationships
  12. Information Security Incident management
  13. Information Security Aspects of Business Continuity
  14. Compliance

IT-Compliance

- Die Übereinstimmung mit gesetzlichen Vorgaben und externen Richtlinien ist ein zentraler Grundsatz der IT-Governance und wird als IT-Compliance bezeichnet.



Überblick über wichtige Vorgaben

	Für wen verbindlich?	Auswirkungen auf Sicherheitsmanagement
KonTraG	viele Deutsche Kapitalgesellschaften	indirekt; Risikomanagement- und -steuerungssysteme müssen installiert werden; IT-(Sicherheits)-Risiken sind mögliche bestandsgefährdende Risiken
BDSG	alle Organisationen in Deutschland	direkt; beschreibt, wie mit bestimmten Daten umgegangen werden soll; fordert konkrete Mechanismen wie z.B. Zugriffskontrolle (siehe Anlage zu § 9 Satz 1)
IT-SiG	alle Organisationen in Deutschland	direkt; Betreiber Kritischer Infrastrukturen, TK-Dienstleister und Telemedienanbieter haben Mindestniveau an IT-Sicherheit einzuhalten, Melde- und Nachweispflicht
SOX	an US-Börsen notierte Unternehmen	indirekt; internes Kontrollsystem gefordert; korrekte Finanzberichterstattung erfordert korrekte Funktion der IT und damit auch IT-Sicherheit
Euro-SOX	größere und börsennotierte Kapitalgesellschaften	indirekt; fordert internes Risikomanagement- und Kontrollsystem
Basel II	Kreditinstitute in Europa	relativ direkt; internes Kontrollsystem muss etabliert werden; Risiken müssen bewertet werden; MaRisk: Einsatz gängiger ISMS-Standards gefordert
Solvency II	Versicherungs-gesellschaften in Europa	analog Basel II, aber genaue Umsetzung noch unklar; internes Kontrollsystem gefordert; Risiken müssen bewertet werden

Folgerungen

- BDSG und IT-Sicherheitsgesetz: konkrete Anforderungen an Informationssicherheit
- Sonst: indirekte Auswirkungen
  - funktionierende interne Kontrollsysteme (IT-Risiken erfassen)
  - korrekte Finanzberichterstattung (wenn IT-basiert erstellt)
  - Erkennung und Behandlung bestandsgefährdender Risiken (auch IT-Sicherheitsrisiken)

- Die Gesetze nennen meist nicht explizit, wie die Erfüllung dieser Anforderungen umgesetzt und nachgewiesen werden soll.

- Management haftet nach SOX, KonTraG bei grober Fahrlässigkeit persönlich, deshalb:
  - Einsatz etablierter IT-Sicherheitsstandards
  - Auditierung als Nachweis

IT-Sicherheitsgesetz

- Artikelgesetz
  - am Juli 2015 in Kraft getreten
  - ändert und ergänzt u.a. BSI-, BKA-, Telemedien-, TK-, Atom- und Energiewirtschaftsgesetz
- Adressaten – ca. 2000 Unternehmen lt. Gesetzesbegründung
  - Betreiber Kritischer Infrastrukturen
    - hohe Bedeutung für das Funktionieren des Gemeinwesens
  - TK-Dienstleister, Telemedienanbieter, …
    - Social Media, Online Shopping, Online Banking, …
- Bußgeld bei Verstößen (§ 14 Abs. 2 BSI-Gesetz)
  - bis zu 100.000 EUR, wenn Betreiber Kritischer Infrastrukturen die Erfüllung der Anforderungen nicht nachweisen können (alle 2 Jahre)
  - bis zu 50.000 EUR in allen anderen Fällen
- Konkretisierung durch Rechtsverordnung (§ 10 Abs. 1 BSI-Gesetz)

IT-Sicherheitsgesetz – Typische Forderungen

- Mindestniveau an IT-Sicherheit (§ 8a Abs. 1 BSI-Gesetz) erreichen und aufrecht erhalten
  - Einführung eines Information Security Management System (ISMS) – etwa nach ISO 27001 oder BSI 100-1
  - Durchführung von Risikoanalysen – etwa nach BSI 100-3

- Nachweispflicht (§ 8a Abs. 3 BSI-Gesetz)
  - vermutlich durch Grundschutz- oder ISO27001-Zertifikat
  - Benennung einer Kontaktstelle für IT-Sicherheit – etwa eines IT-Sicherheitsbeauftragten

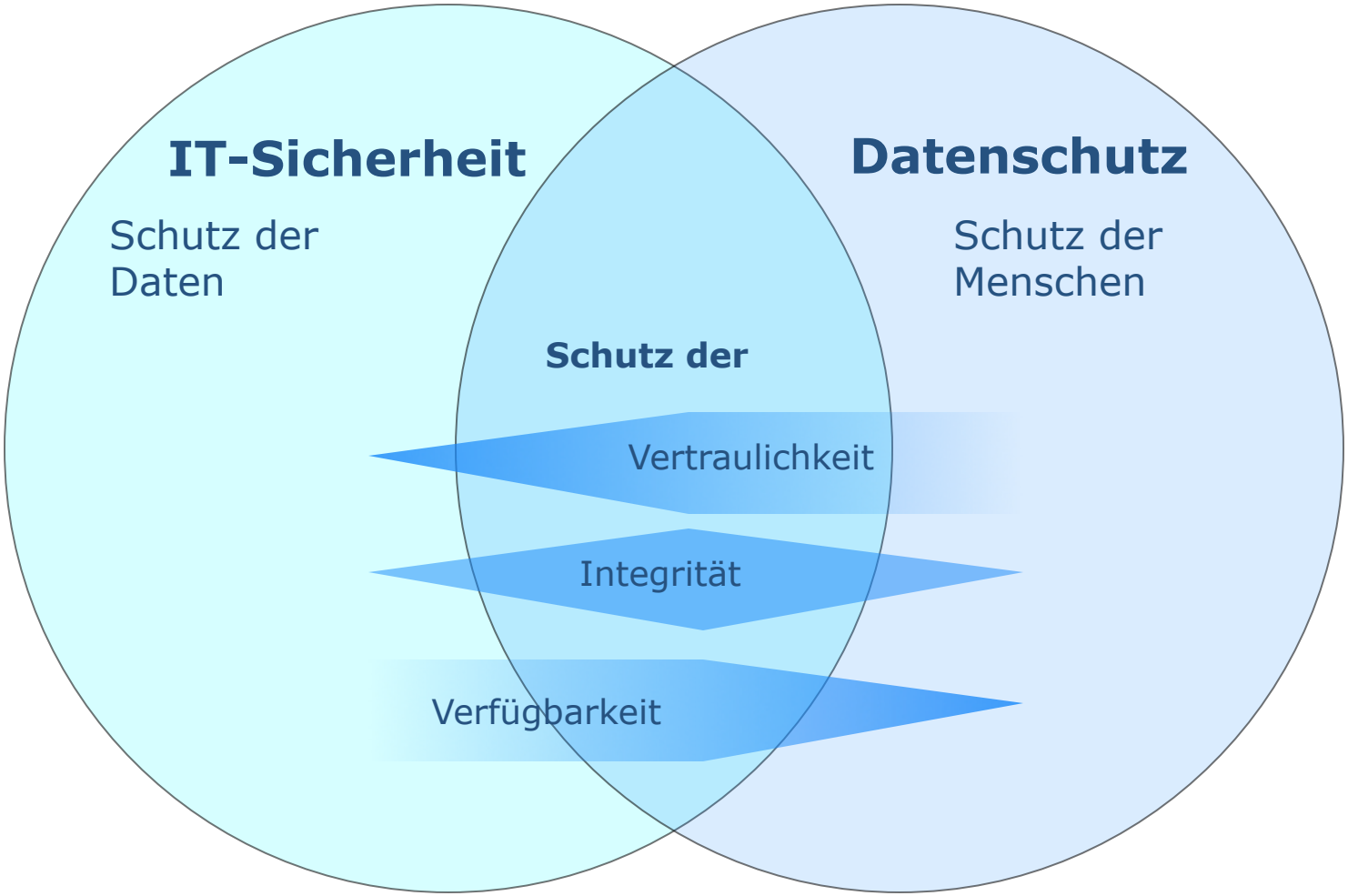
- Meldepflicht der Betreiber Kritischer Infrastrukturen an das BSI bei »erheblichen Störungen« der IT-Sicherheit (§ 8b Abs. 4 BSI-Gesetz)
  - Nennung des Betreibers: erforderlich, wenn Störung tatsächlich zum Ausfall oder zu einer Beeinträchtigung geführt hat
  - sonst: Meldepflicht ohne Angabe des Betreibers ist ausreichend

Abgrenzung von IT-Sicherheit und Datenschutz

- IT-Sicherheitsmanagement
  - IT-Sicherheitsmanagement versucht, die mit Hilfe von Informationstechnik (IT) realisierten Produktions- und Geschäftsprozesse in Unternehmen und Organisationen systematisch gegen beabsichtigte Angriffe (Security) und unbeabsichtigte Ereignisse (Safety) zu schützen.

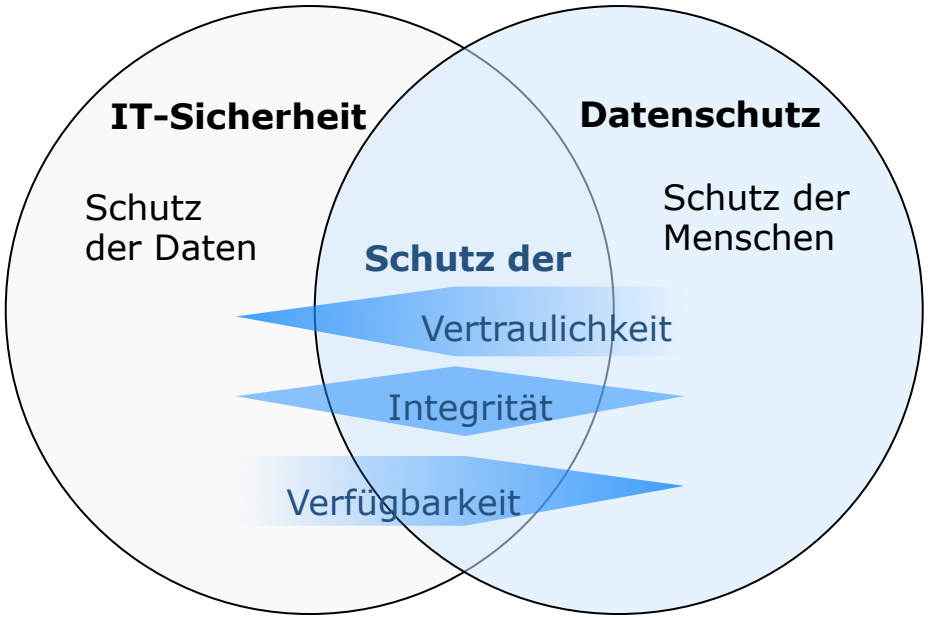
- Datenschutz
  - Mit dem Begriff Datenschutz wird das Recht des Einzelnen auf informationelle Selbstbestimmung umschrieben. «Das Grundrecht gewährleistet [...] die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.» (BVerfG) Eine Organisation hat technisch-organisatorische Maßnahmen zu treffen, um dieses Recht zu gewährleisten.

Verknüpfung von Sicherheit und Datenschutz



BDSG § 9 Technische und organisatorische Maßnahmen

- Öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.



Anlage zu § 9 Abs. 1 BDSG

1. Zutrittskontrolle (räumlicher Zutritt, Gebäude)
2. Zugangskontrolle (Benutzung, Passwort)
3. Zugriffkontrolle (Berechtigung, Administratoren)
4. Weitergabekontrolle (Transport, Netze)
5. Eingabekontrolle (Nutzer-Protokoll)
6. Auftragskontrolle (Outsourcing, Wartung)
7. Verfügbarkeitskontrolle (Zerstörung)
8. Trennungsgebot (Zwecktrennung)

Sicherheit: Abgrenzung von Security & Safety

Security
Schutz gegen beabsichtigte Angriffe

Vertraulichkeit
- Abhörsicherheit
- Sicherheit gegen unbefugten Gerätezugriff
- Anonymität
- Unbeobachtbarkeit

Integrität
- Übertragungsintegrität
- Zurechenbarkeit
- Abrechnungsintegrität

Verfügbarkeit
- Ermöglichen von Kommunikation

Safety
Schutz vor unbeabsichtigten Ereignissen

Fehlertoleranz

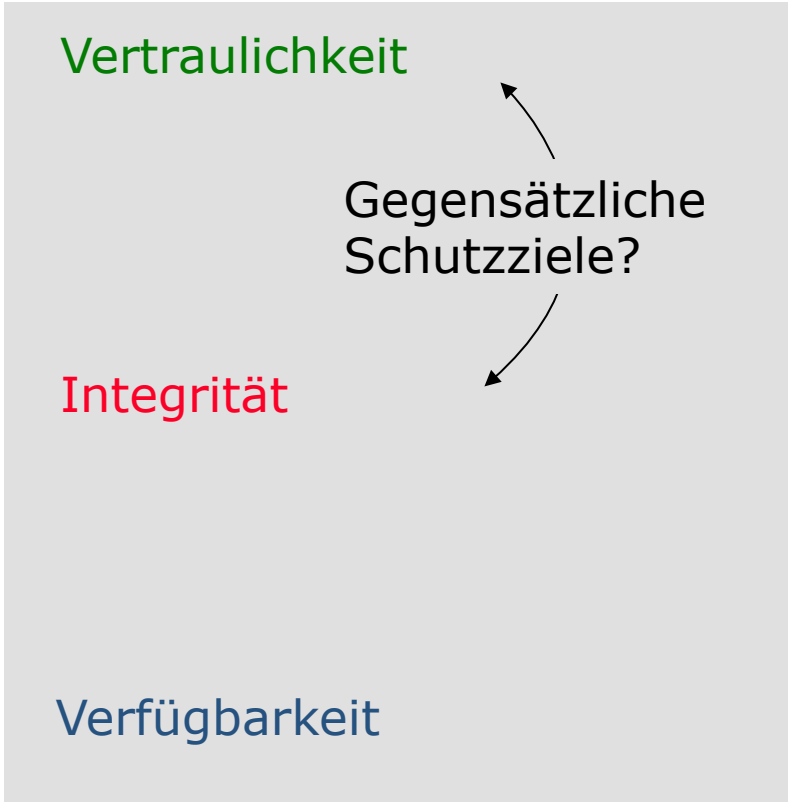
Verfügbarkeit
- Funktionssicherheit
- Technische Sicherheit
- Schutz vor Überspannung, Überschwemmung, Temperaturschwankungen
- Schutz vor Spannungsausfall

Sonstige Schutzziele
- Maßnahmen gegen hohe Gesundheitsbelastung
- …

Schutzziele

Voydock, Kent 1983

- Klassische IT-Sicherheit berücksichtigt im Wesentlichen Risiken, die durch *regelwidriges Verhalten* in IT-Systemen entstehen.



unbefugter Informationsgewinn

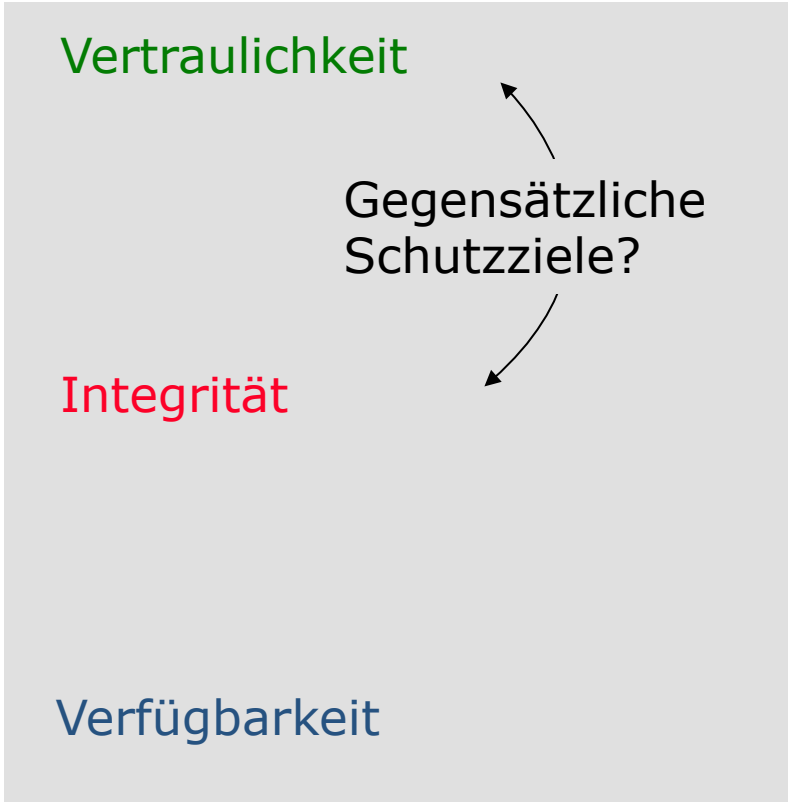
unbefugte Modifikation

unbefugte Beeinträchtigung der Funktionalität

Mehrseitige Sicherheit

Müller et. al. 1997

- Mehrseitige Sicherheit bedeutet die Einbeziehung der Schutzinteressen aller Beteiligten sowie das Austragen daraus resultierender Schutzkonflikte.



- Voraussetzung
  - regelwidriges Verhalten hält Systeme und Nutzer schadlos
- Ziel
  - gegensätzliche Sicherheitsinteressen werden erkannt, Lösungen ausgehandelt und durchgesetzt

Schutzziele der mehrseitigen Sicherheit

Kommunikationsgegenstand Was?, Worüber?	Kommunikationsumstände Wann?, Wo?, Wer?
Inhaltsdaten	Verkehrsdaten
Vertraulichkeit **Verdecktheit**	**Anonymität** **Unbeobachtbarkeit**
Inhalte	Sender, Ort, Empfänger
Integrität	**Zurechenbarkeit** **Rechtsverbindlichkeit**
Inhalte	Absender, Bezahlung, Empfänger
Verfügbarkeit	**Erreichbarkeit**
Inhalte	Nutzer, Rechner

Vertraulichkeit: Verfahren und Algorithmen

Was wird geschützt?

Beispiele für Verfahren

Beispiele für Algorithmen

Verfahren des technischen Datenschutzes

Inhaltsdaten

Vertraulichkeit

Verschlüsselung

Inhalte

DES, 3-DES, OTP, IDEA, AES, RSA, ElGamal, …

Verdecktheit

Steganographie

Inhalte + Existenz

F5, …

Verkehrsdaten

Anonymität Unbeobachtbarkeit

Sender

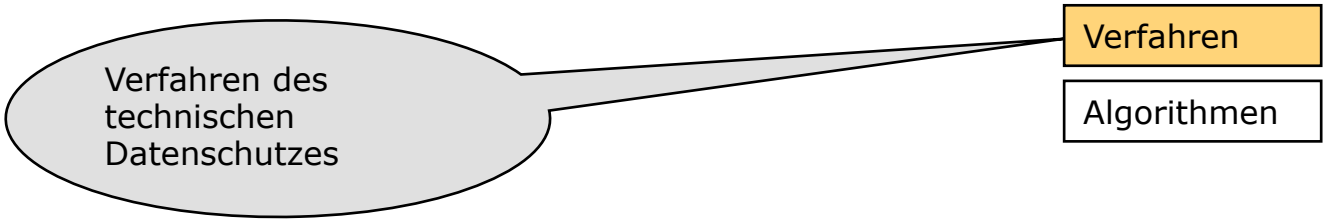
Ort

Empfänger

Web-Anonymisierer, Remailer, anonyme Zahlungssysteme

Pseudonyme, Proxies, umkodierende Mixe, DC Netz, Private Information Retrieval, …

Integrität und Zurechenbarkeit, Rechtsverbindlichkeit



Inhaltsdaten

Kommunikationsumstände
Wann?, Wo?, Wer?

Integrität

Zurechenbarkeit
Rechtsverbindlichkeit

auch:
Authentizität
Unabstreitbarkeit

Inhalte

Message Authentication Codes

Challenge-Response-Authentikation

Absender

Bezahlung

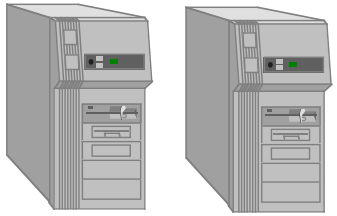
Empfänger

Digitale Signaturen

RSA, ElGamal, …

Verfügbarkeit: Redundanz und Diversität

- Redundanz
  - Mehrfache Auslegung von Systemkomponenten
  - Bei Ausfall übernimmt Ersatzkomponente



Beispiel: Doppelung

- Diversität
  - Verschiedenartigkeit der Herkünfte
  - Tolerieren von systematischen Fehlern und verdeckten trojanischen Pferden
  - Unabhängige Entwicklung von redundanten (Software)-Komponenten

Verfügbarkeit

Inhalte

Erreichbarkeit

Nutzer | Rechner

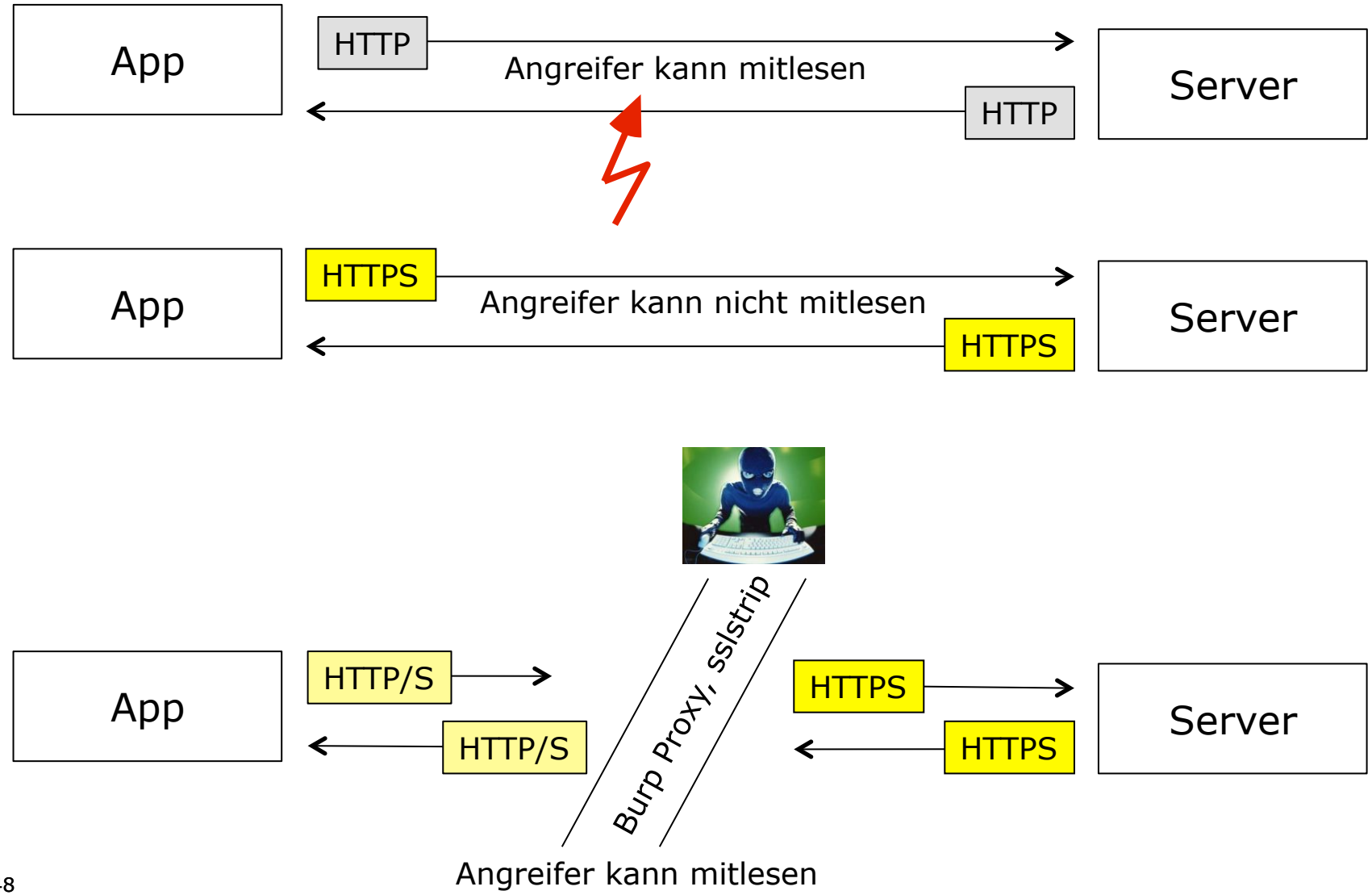
Vollständiges Durchsuchen (brute-force, exaustive search)

- Angriff über Supercomputer und künftig Quantencomputer
  - betrifft nur komplexitätstheoretisch sichere Systeme
- Schutz gegen Supercomputer
  - Schlüssel ausreichend lang wählen
- Schutz gegen Quantencomputer
  - symmetrisch: Schlüssellänge verdoppeln auf mind. 256 Bit
  - asymmetrisch: [post-quantum cryptography]

	Key lengths	Complexity		nach: Bernstein, Buchmann, Dahmen: Post Quantum Cryptography. Springer, 2009
		Super Computer	Quantum Computer	
Symm.	128 Bit	2^{127}	2^{64}	Grover, 1996
	256 Bit	2^{255}	2^{128}	
Asymm.	1024 Bit	$\approx 2^{90}$	$\approx 2^{25}$	Shor, 1994
	2048 Bit	$\approx 2^{117}$	$\approx 2^{28}$	

Fehlende oder fehlerhafte Zertifikatsvalidierung in Clients

Fehlende oder fehlerhafte Zertifikatsvalidierung in Clients



www.informationisbeautiful.net/visualizations/worlds-biggest-data-

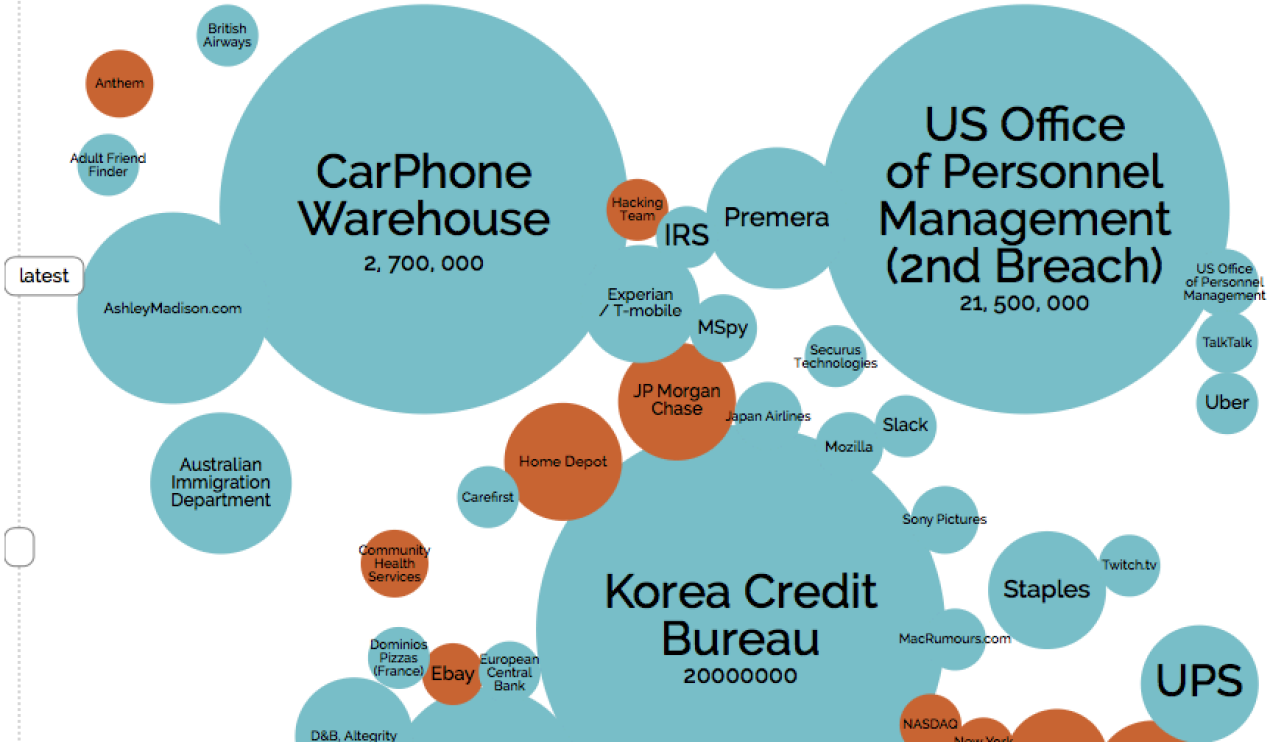
Information is Beautiful
the best-selling infographic classic
Now in Second Edition
revised, recalculated and reimagined

World's Biggest Data Breaches

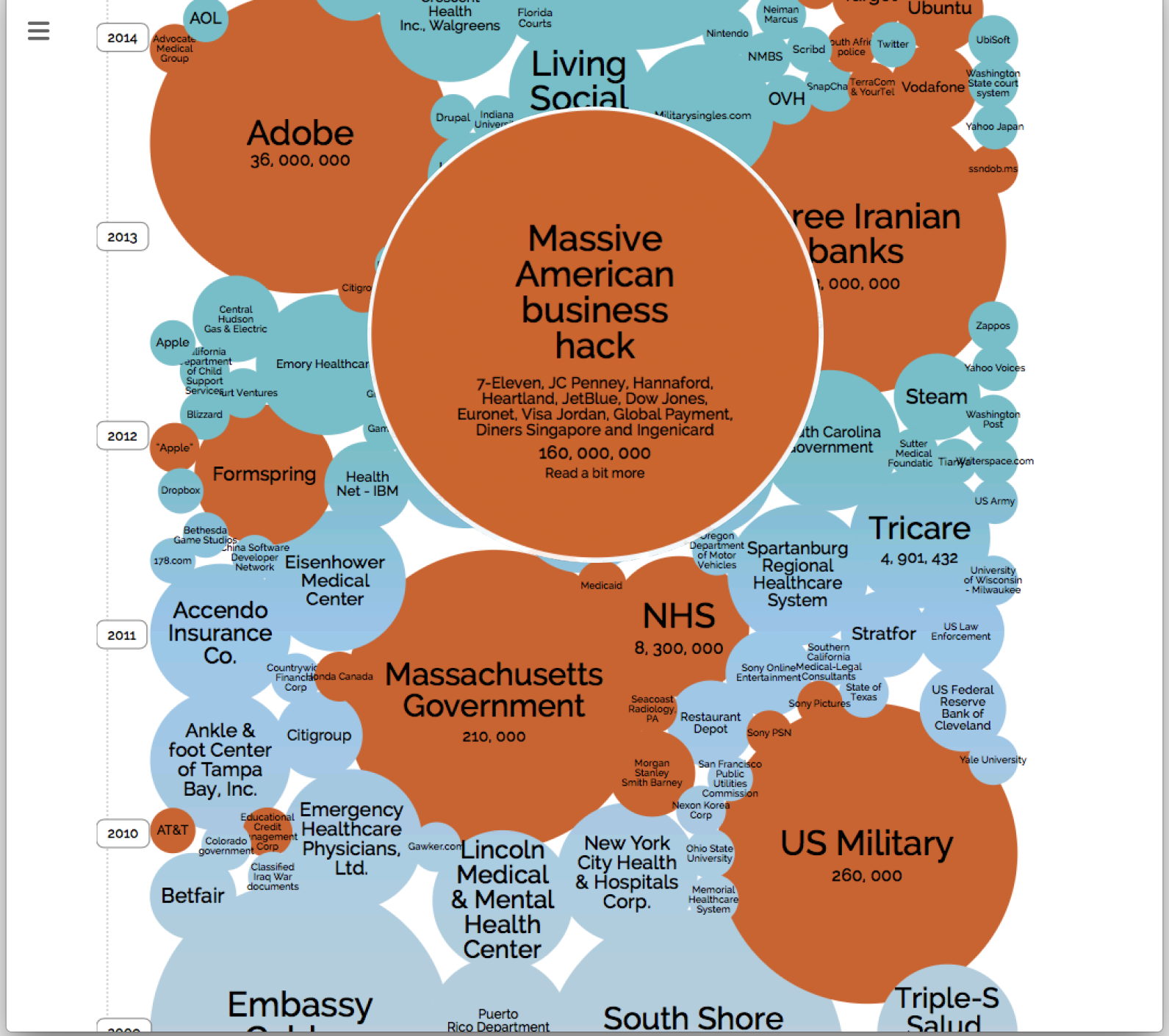
Selected losses greater than 30,000 records
(updated 2nd October 2015)

interesting story

YEAR | BUBBLE COLOUR | YEAR | METHOD OF LEAK | BUBBLE SIZE | NO OF RECORDS STOLEN | DATA SENSITIVITY | SHOW FILTER



http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/



http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

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

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

Universität Hamburg
DER FORSCHUNG | DER LEHRE | DER BILDUNG