Masterseminar WS 2016/17
IT-Sicherheitsmanagement

Prof. Dr. Kai Rannenberg
Christopher Schmitz, M.Sc.
Deutsche Telekom Chair of Mobile Business & Multilateral Security
Goethe University Frankfurt
www.m-chair.de

Agenda

I. Organisatorisches

II. Anforderungen und Bewertung

III. Literaturrecherche

IV. Einführung: IT-Sicherheitsmanagement

V. Themenvorstellung

VI. Themenverteilung

I. Organisatorisches

Allgemeines

Seminaranmeldung

- Seminaranmeldung und -rücktritt sind vom 13. bis 26. Oktober möglich und werden in erster Linie in der Vorbesprechung am 24.10.2016 ausgeübt.
- Nach erfolgter Anmeldung und Ablauf der Rücktrittsfrist führt die Nichtteilnahme am Seminar zum Nichtbestehen.

Allgemeines

Kontakt

- Alle organisatorischen und inhaltlichen Fragen bitte ausschließlich an folgende E-Mail-Adresse senden: secmgt@m-chair.de
- Individuelle Sprechstunden werden nach vorheriger Vereinbarung per E-Mail angeboten.

Informationen

- Sämtliche Materialien, Informationen und Neuigkeiten werden auf der Lehrstuhl-Website veröffentlicht: www.m-chair.de
- Zur ersten Orientierung erhält jede Gruppe in den nächsten Tagen einführende Literatur in ihr Thema.

Wichtige Termine

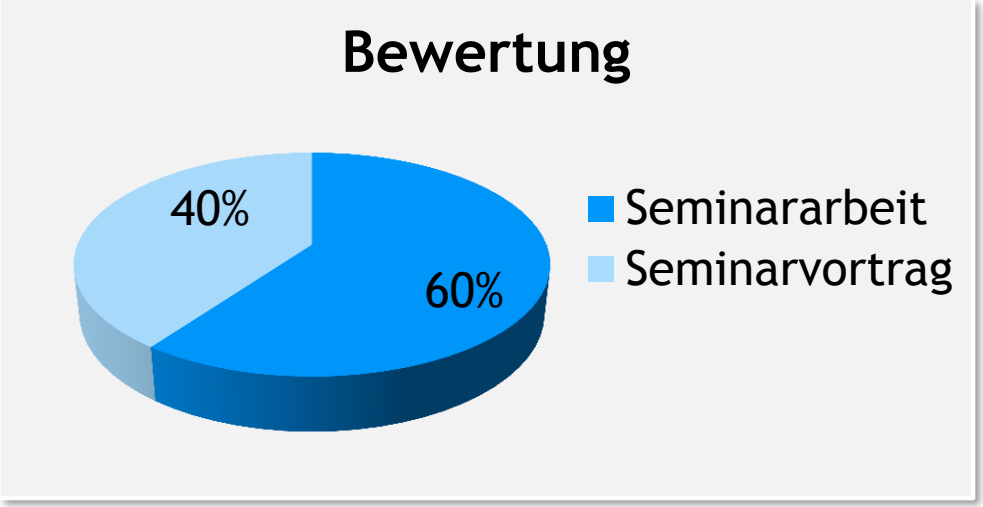
Zeiten	Wo/Wie	Was
24.10.16, 10 - 14 Uhr	RuW 2.202	Einführung und Themenvergabe
15.12.16, 11:30 Uhr	Im Sekretariat und E-Mail an: secmgt@m-chair.de	Abgabe der Arbeit
09.01.17, 17:00 Uhr	E-Mail an: secmgt@m-chair.de	Abgabe der Präsentation
12.01.17, 10 - 18 Uhr	RuW 2.202	Präsentationen (Tag 1)*
13.01.17, 10 - 18 Uhr	RuW 2.202 RuW 2.102 (ab 12 Uhr)	Präsentationen (Tag 2)*

* Die Agenda wird im Vorhinein an alle Teilnehmer geschickt

II. Anforderungen und Bewertung

Bewertung

- Der Leistungsnachweis setzt sich aus zwei Bestandteilen zusammen:



- Für das erfolgreiche Bestehen des Seminars müssen beide Teilleistungen bestanden werden.
- Bearbeitung erfolgt in Zweiergruppen. Benotung erfolgt aber auf individueller Basis. Daher Verantwortlichkeiten in separatem Dokument kenntlich machen!

Seminararbeit

- Umfang: Insgesamt 30-40 Seiten
- Einhaltung der Bearbeitungsrichtlinie und Verwendung der Formatvorlage des Lehrstuhls:
  - https://m-chair.de/index.php/teaching/theses

Abgabe zweier Fassungen bis zum 15.12.16, 11:30 Uhr:

- Eine digitale Version per E-Mail an: secmgt@m-chair.de
- Eine gedruckte Version an Elvira Koch, RuW 2.257 (Sprechzeiten beachten!)

Seminarvortrag

- Vortragsdauer: 30 Minuten
- Anschließende Diskussion: 10 Minuten

Abgabe vorab per E-Mail bis zum 09.01.17, 17:00 Uhr

- Format: PowerPoint
- E-Mail an: secmgt@m-chair.de

III. Literaturrecherche

Literaturrecherche

- EBSCOhost http://www.ebscohost.com
- Web of Knowledge http://apps.webofknowledge.com
- ScienceDirect http://www.sciencedirect.com
- SpringerLink http://link.springer.com
- IEEE_Xplore http://ieeexplore.ieee.org/Xplore
- ACM http://dl.acm.org
- Google Scholar https://scholar.google.de
- RUW-Bibliothek https://www.ub.uni-frankfurt.de/bruw/
- …

- Ausgewählte Workshops/Konferenzen/Journals:
  - Z.B. WEIS (Workshop on the Economics of Information Security) http://econinfosec.org/

III. Einführung: IT-Sicherheitsmanagement

mobile business

IT-Sicherheit

www.spiegel.de/netzwelt/netzpolitik/angriff-auf-irans-atomprogramm-stuxnet-virus-koennte-tausend-uran-zentrifugen-zerstoert-haben-

SPIEGEL ONLINE DER SPIEGEL SPIEGEL TV

NETZWELT

Schlagzeilen | Wetter | DAX 10.520,97 | TV-Programm

Nachrichten > Netzwelt > Netzpolitik > Computerviren > Angriff auf Irans Atomprogramm: Stuxnet-Virus könnte tausend Uran-Zentrifugen

Angriff auf Irans Atomprogramm

Stuxnet-Virus könnte tausend Uran-Zentrifugen zerstört haben

Neue Erkenntnisse über d
iranischen Anreicherungs
eingestehen will. Bis zu t

Von Christian Stöcker

Mahmud Ahmadinedschad beim E

Teilen

Sonntag, 26.12

Hamburg - D
renommiert

estag-gesamtes-it-netz-des-bundestages-muss-ausgetauscht-werden-1.2519934

München 12°

Süddeutsche Zeitung

SZ.de Zeitung Magazin

Shop Jobs Immobilien Anzeigen

Login Abo

Politik Wirtschaft Panorama Sport München Bayern Kultur Wissen Digital Chancen Reise Auto Stil mehr...

Home > Politik > Hackerangriff auf den Bundestag - Gesamtes IT-Netz des Bundestages muss ausgetauscht werden

14. Juni 2015, 11:25 Uhr Hackerangriff auf den Bundestag

Gesamtes IT-Netz des Bundestages muss ausgetauscht werden

r Schaden nach dem Hackerangriff auf den Bundestag ist
her als bislang angenommen. Experten zufolge könnte die
stallierung eines neuen IT-Systems mehr als ein Jahr
nern.

nem Medienbericht zufolge ist auch auf einem Computer
s dem Bundestagsbüro von Angela Merkel Schadsoftware

ANZEIGE

riminelle-verkaufen-millionen-gehackte-linkedin-passwoerter-1.2998039

München 12°

Süddeutsche Zeitung

SZ.de Zeitung Magazin

Shop Jobs Immobilien Anzeigen

Login Abo

Politik Wirtschaft Panorama Sport München Bayern Kultur Wissen Digital Chancen Reise Auto Stil

Home > Digital > Linkedin-Hack: 117 Millionen Passwörter zum Verkauf

18. Mai 2016, 15:04 Uhr Gehacktes Karrierenetzwerk

Kriminelle verkaufen 117 Millionen gehackte Linkedin-Passwörter

Linkedin-Ch
Weiner bei e
Veranstaltu
Mountain V
Kalifornien.

117 Millionen E-Mail-Adressen und Passwörter von Nutzern des Karrierenetzwerks Linkedin stehen im Internet zum Verkauf.

ANZEIGE

in den U

www.spiegel.de/netzwelt/web/hacker-attacke-in-den-usa-stoert-twitter-spotify-und-andere-dienste-a-1117820.html

SPIEGEL ONLINE DER SPIEGEL SPIEGEL TV

Anmelden

NETZWELT

Schlagzeilen | Wetter | DAX 10.710,73 | TV-Programm | Abo

Nachrichten > Netzwelt > Web > Hacker > Hacker-Attacke in den USA stört Twitter, Spotify und andere Dienste

Attacke auf Internetdienstleister

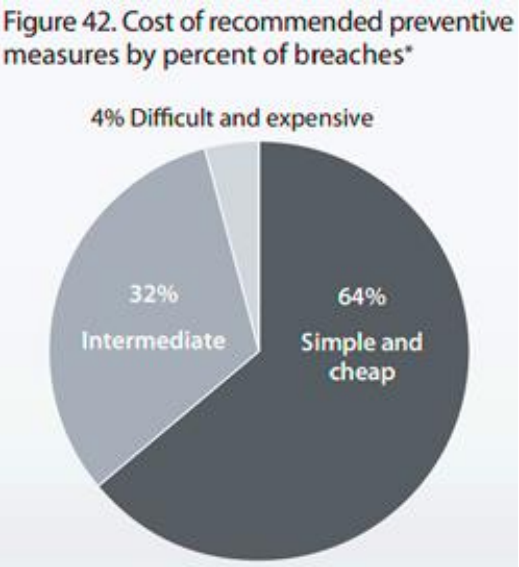
Hackerangriff - Störung bei Twitter und Co.

Mit massenhaften Anfragen an den Webdienstleister Dyn haben Unbekannte Portale wie Twitter, Spotify und Amazon zeitweise gestört. Betroffen waren vor allem Nutzer in den USA, aber auch in Europa und Japan.

IT-Sicherheitsmanagement

- Gemäß einer Studie des US Secret Service und Verizon könnten 64% der Sicherheitsvorfälle durch **einfache und günstige** Sicherheitsmaßnahmen verhindert werden
- Nur 4% der Vorfälle erfordern **aufwendige und teure** Maßnahmen

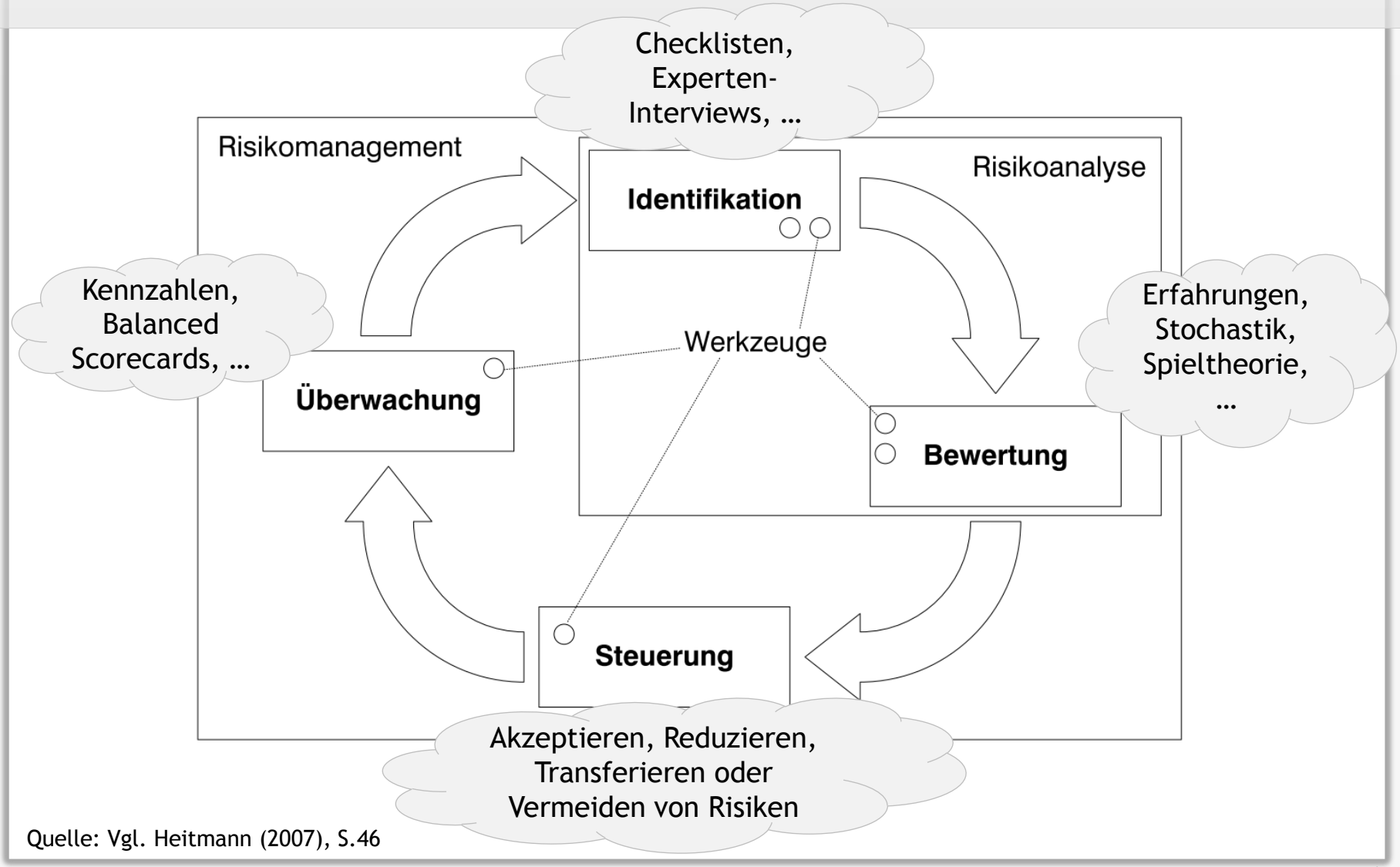
(vgl. US Secret Service/Verizon (2010))



→ Die Ursachen für Sicherheitsprobleme sind häufig nicht durch Technikversagen bedingt, sondern durch **Fehlentscheidungen beim Einsatz von Sicherheitsmaßnahmen**

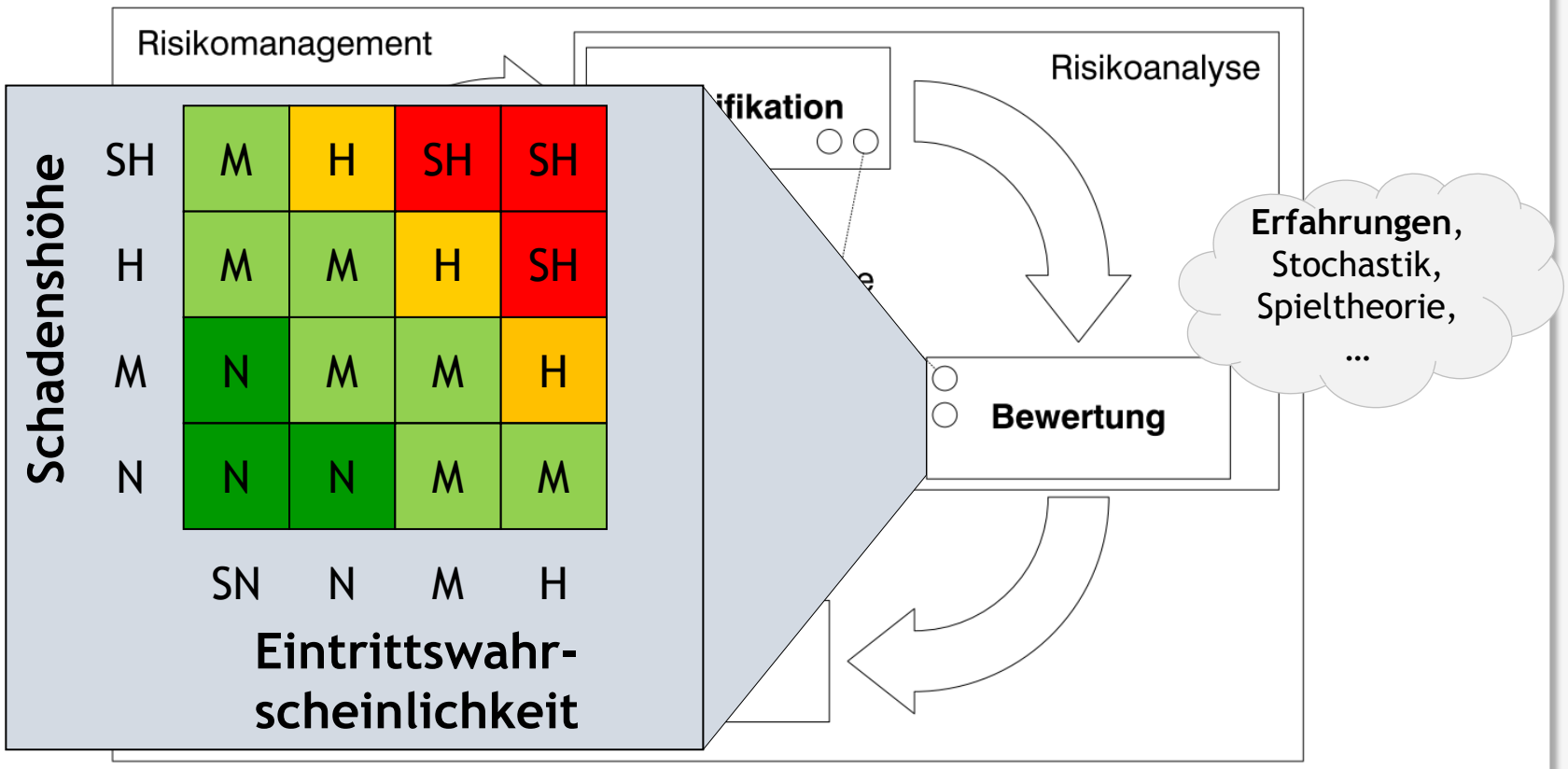
Quelle: Vgl. US Secret Service/Verizon (2010), S.56

Risikomanagement-Kreislauf



Quelle: Vgl. Heitmann (2007), S.46

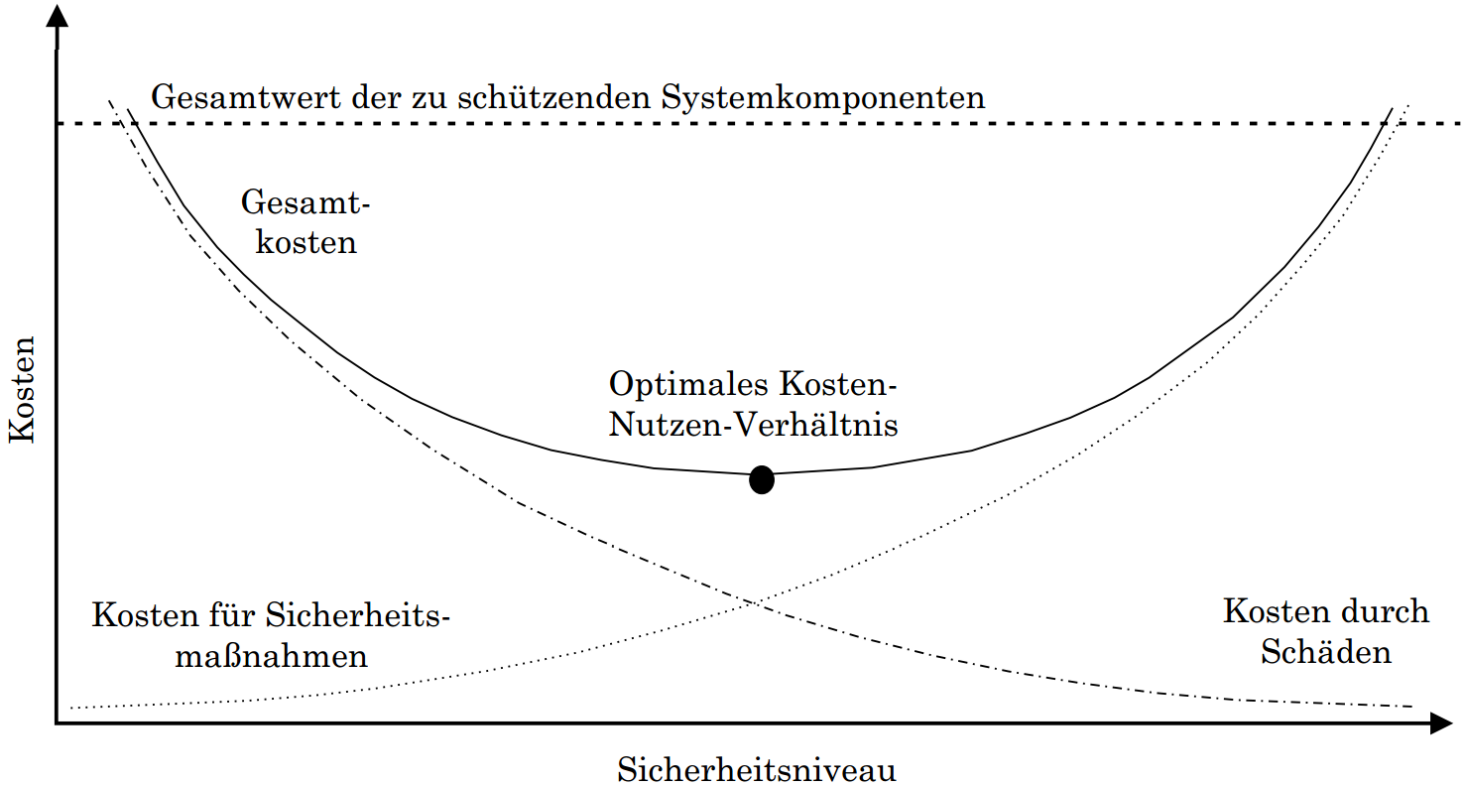
Risikomanagement-Kreislauf



Quelle: Vgl. Heitmann (2007), S.46

Zentrale Fragestellungen (1/2)

- Wie viel Ressourcen sollten Unternehmen im Sinne einer ökonomischen Kosten/Nutzen-Abwägung in IT-Sicherheit investieren?



Quelle: Heitmann (2007), S.30

Zentrale Fragestellungen (2/2)

Risikoidentifikation

- Welche Bedrohungen und Schwachstellen existieren und welche Sicherheitsvorfälle bzw. Risiken können daraus resultieren?

Risikobewertung

- Wie sind die identifizierten Risiken aus technisch-ökonomischer Perspektive zu bewerten und zu priorisieren?
- Wie lassen sich z.B. Eintrittswahrscheinlichkeit und Schadenshöhe für Risikoszenarien bestimmen?

Risikosteuerung

- Welche Maßnahmen zur Risikobehandlung gibt es und welche sollten konkret umgesetzt werden?

  (Allgemeine Maßnahmen: Akzeptieren, Reduzieren, Transferieren oder Vermeiden von Risiken)

Risikoüberwachung

- Wie kann man den Erfolg umgesetzter Maßnahmen (z. B. erzielte Schadensreduktion) messen?

III. Themenvorstellung

Themenüberblick

Risikoanalyse (Risikoidentifikation und -bewertung)

(1) Ansätze zur Sicherheitsbewertung von IT-Infrastrukturen

(2) Vergleichende Analyse von Frameworks zur Bewertung von IT-Sicherheitsrisiken

(3) Einfluss von Sicherheitsvorfällen auf den Geschäftserfolg von Unternehmen

(4) Bewertungsansätze der IT Security Compliance

Risikosteuerung

(5) Investitionsentscheidungen anhand Return on Security Investment-basierter Ansätze

(6) Spieltheoretische Ansätze zur Bewertung von IT-Sicherheitsmaßnahmen

(7) Graphen-basierte Ansätze zur Bewertung von IT-Sicherheitsmaßnahmen

(8) Versicherungsmöglichkeiten gegen IT-Risiken

Risikoüberwachung

(9) Balanced Scorecards als Steuerungs- und Kontrollinstrument im IT-Sicherheitsmanagement

Ansätze zur Sicherheitsbewertung von IT-Infrastrukturen

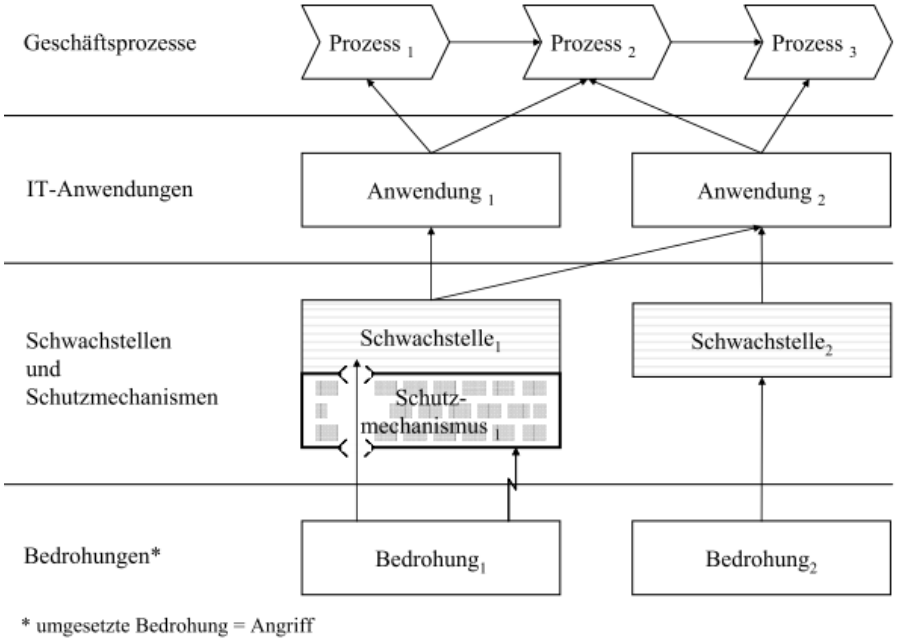
- Welche etablierten Ansätze zur Bewertung des Sicherheitsniveaus (technische und nicht-technische Aspekte) von IT-Infrastrukturen existieren und wie sind diese zu bewerten?
- Inwieweit ist mit diesen Ansätzen eine schnelle und einfache Selbst-einschätzung (Self-Assessment) bzgl. des Sicherheitsniveaus möglich?

Vergleichende Analyse von Frameworks zur Bewertung von IT-Sicherheitsrisiken

- Welche etablierten Frameworks zur IT-Risikobewertung gibt es?
- Vergleichende Gegenüberstellung der identifizierten Methoden anhand **fachlich-inhaltlicher Kriterien** (z.B. erforderliche Aktivitäten, Arbeitsergebnisse der Prozessschritte) sowie **organisatorischer Kriterien** (z.B. Aufwand, benötigtes Know-how).

Einfluss von Sicherheitsvorfällen auf den Geschäftserfolg von Unternehmen

- Welche Schadensklassen gibt es und welche Ansätze zur Ermittlung der Schadenshöhe werden jeweils in der Literatur genannt?
- Inwieweit lässt sich die Schadenshöhe der einzelnen Kategorien mit den identifizierten Ansätzen abschätzen?



Quelle: Prokein (2008), S.2

Bewertungsansätze der IT Security Compliance

- Welche gesetzlichen Anforderungen müssen Unternehmen bzgl. ihrer IT-Sicherheit berücksichtigen? Welche besonderen Anforderungen gelten für kritische Infrastrukturen in der Energiebranche?
- Welche Ansätze zur Bewertung der IT-Compliance gibt es?

Investitionsentscheidungen anhand Return on Security Investment-basierter Ansätze

$$ROSI = \frac{ALE_0 - ALE_1 - Costs}{Costs}$$

mit

ALE_0, ALE_1 = Jährliche Verlusterwartung (Annual Loss Expectancy) ohne/mit Maßnahme

$Costs$ = Kosten für Sicherheitsmaßnahme

- Was sind die Vor- und Nachteile des Return on Security Investment (ROSI)?
- Welche Ansätze zur Verbesserung des klassischen ROSI gibt es (z.B. aus der Spieltheorie oder der Stochastik) und wie sind diese zu bewerten?

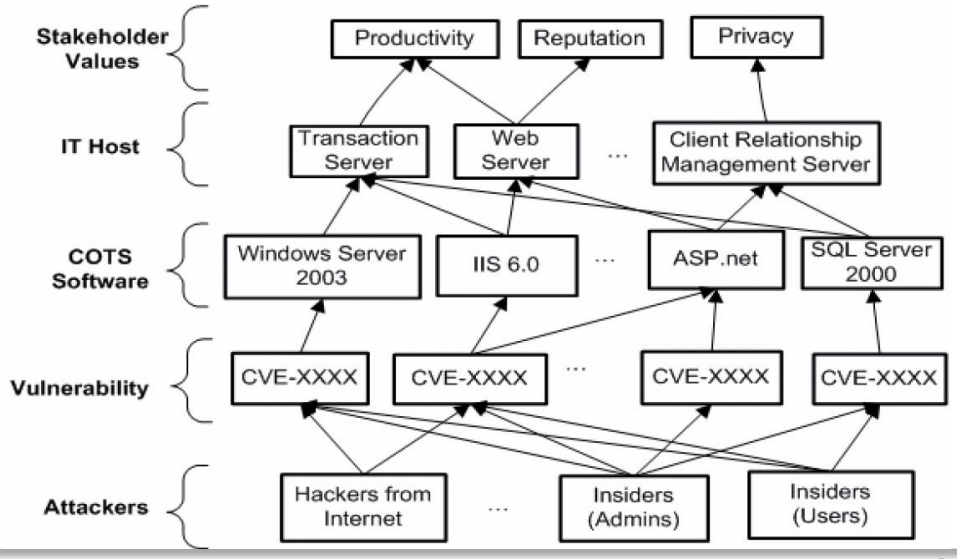
Spieltheoretische Ansätze zur Bewertung von IT-Sicherheits-maßnahmen

- Zielsetzung spieltheoretischer Konzepte in der IT-Sicherheit ist, strategisches Angreiferverhalten präziser modellieren zu können als z.B. mit stochastischer Risikotheorie.

- Welche Ansätze finden sich hierfür in der Literatur?
- Inwieweit lassen IT-Sicherheitsentscheidungen dadurch verbessern und wie sind diese hinsichtlich ihres praktischen Nutzens zu bewerten?

Graphen-basierte Ansätze zur Bewertung von IT-Sicherheits-maßnahmen

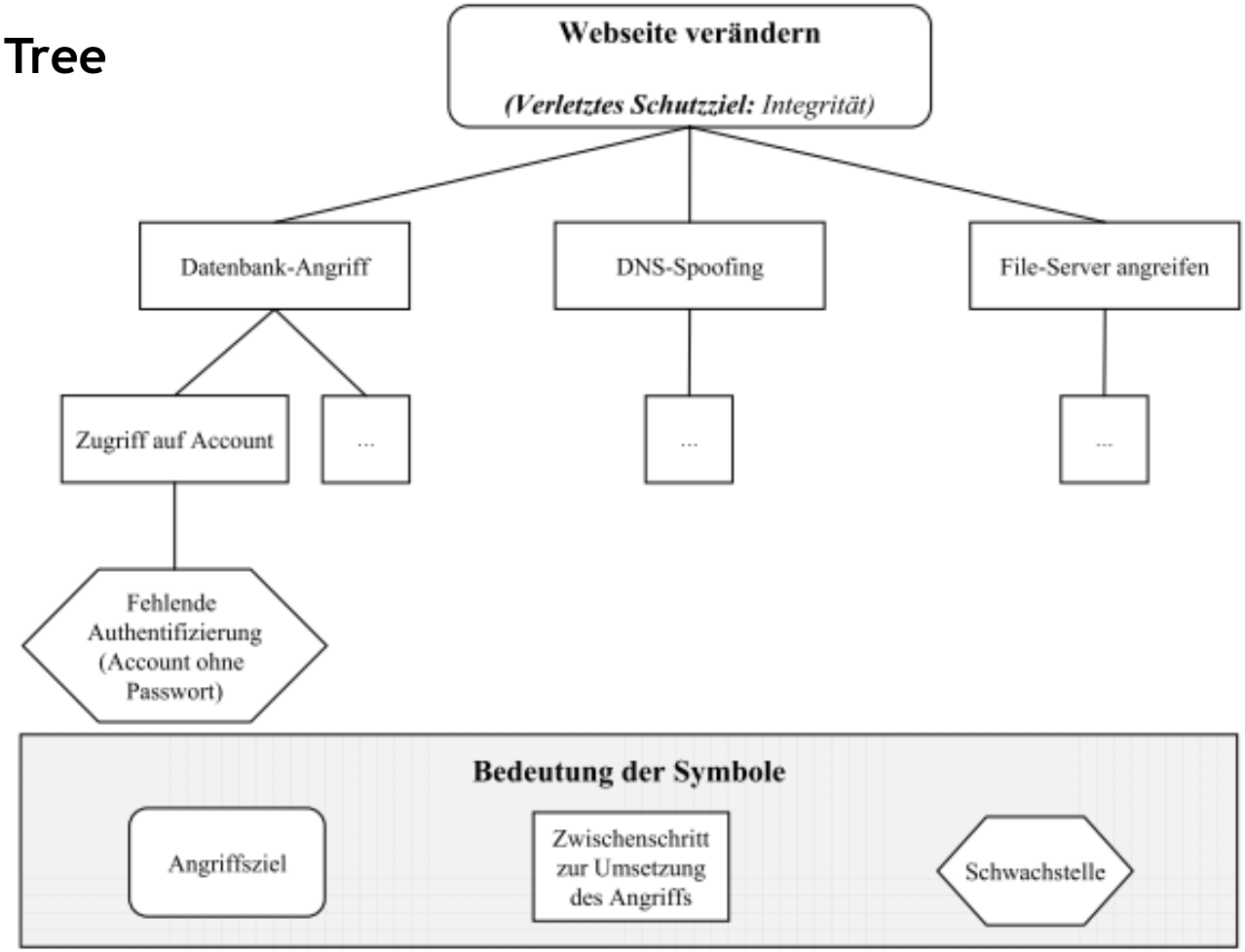
- Welche graphentheoretischen Konzepte zur Modellierung von Angriffen gibt es?
- Welche Graphen-basierten Ansätze zur Bewertung von IT-Infrastrukturen und IT-Sicherheitsmaßnahmen werden in der Literatur diskutiert?
- Wie sind diese hinsichtlich ihres praktischen Nutzens zu bewerten?



Quelle: Chen (2007), S.5

Thema 7 (2/2)

Attack Tree



Quelle: Prokein (2008), S.27

Versicherungsmöglichkeiten gegen IT-Risiken

- Welche Versicherungsmöglichkeiten gegen IT-Risiken existieren in der Praxis?
- Welche Konzepte und Bewertungsmodelle werden in der Theorie diskutiert?
- Inwiefern lassen sich die theoretischen Modelle aus der Literatur in die Praxis überführen?

Balanced Scorecards als Steuerungs- und Kontrollinstrument im IT-Sicherheitsmanagement

- Inwiefern/wie lässt sich das Konzept der Balanced Scorecard (BSC) für das IT-Sicherheitsmanagement adaptieren?
- Welche Ansätze solcher Security Scorecards werden in der Literatur genannt?
- Was sind die Vor- und Nachteile der Verwendung von BSC im IT-Sicherheitsmanagement?

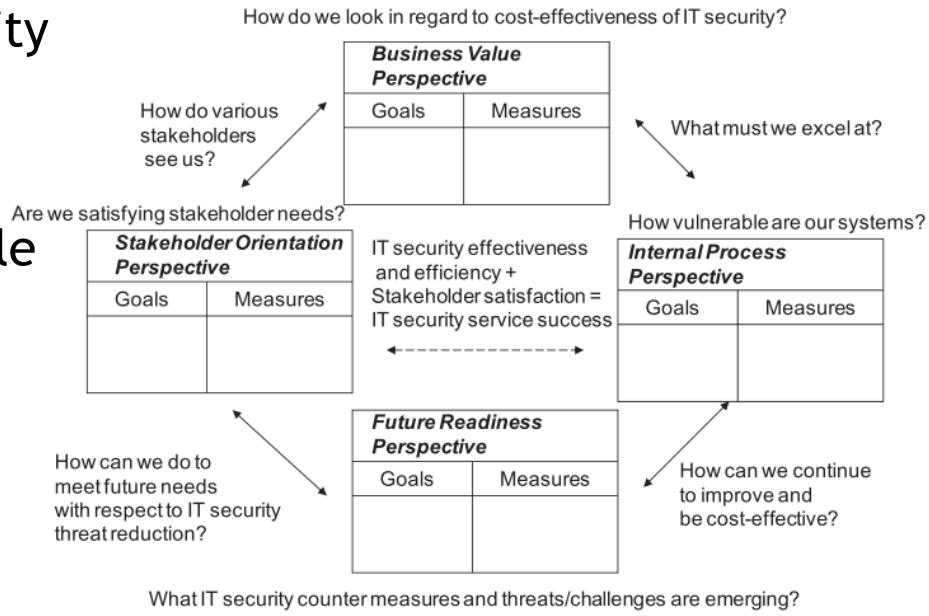


FIG. 3. Proposed BSC model for Information Security.

Quelle: Herath (2010), S.6

IV. Themenverteilung

Themenverteilung

Risikoanalyse (Risikoidentifikation und -bewertung)

(1) Ansätze zur Sicherheitsbewertung von IT-Infrastrukturen

(2) Vergleichende Analyse von Frameworks zur Bewertung von IT-Sicherheitsrisiken

(3) Einfluss von Sicherheitsvorfällen auf den Geschäftserfolg von Unternehmen

(4) Bewertungsansätze der IT Security Compliance

Risikosteuerung

(5) Investitionsentscheidungen anhand Return on Security Investment-basierter Ansätze

(6) Spieltheoretische Ansätze zur Bewertung von IT-Sicherheitsmaßnahmen

(7) Graphen-basierte Ansätze zur Bewertung von IT-Sicherheitsmaßnahmen

(8) Versicherungsmöglichkeiten gegen IT-Risiken

Risikoüberwachung

(9) Balanced Scorecards als Steuerungs- und Kontrollinstrument im IT-Sicherheitsmanagement

Quellen

(1) Chen, Y., Boehm, B., & Sheppard, L.: Measuring security investment benefit for off the shelf software systems-a stakeholder value driven approach. The sixth workshop on the economics of information security, Carnegie Mellon University, USA, 2007.

(2) Heitmann, M.: IT-Sicherheit in vertikalen F&E-Kooperationen der Automobilindustrie, Deutscher Universität Verlag, Wiesbaden, 2007.

(3) Herath, T., Herath, H., and Bremser, W. G.: Balanced Scorecard Implementation of Security Strategies: A Framework for It Security Performance Management, Information Systems Management, 2010.

(4) Prokein, O., IT-Risikomanagement: Identifikation, Quantifizierung und wirtschaftliche Steuerung, Springer Verlag, Wiesbaden, 2008.

(5) Verizon, US Secret Service: 2010 Data Breach Investigations Report (DBIR) (Verfügbar unter: http://www.verizonenterprise.com/resources/reports/rp_2010-data-breach-report_en_xg.pdf), 2010.

mobile business

Deutsche Telekom Chair of Mobile Business & Multilateral Security

Prof. Dr. Kai Rannenberg
Christopher Schmitz, M.Sc.
Goethe University Frankfurt
WWW: www.m-chair.de

GOETHE UNIVERSITÄT FRANKFURT AM MAIN