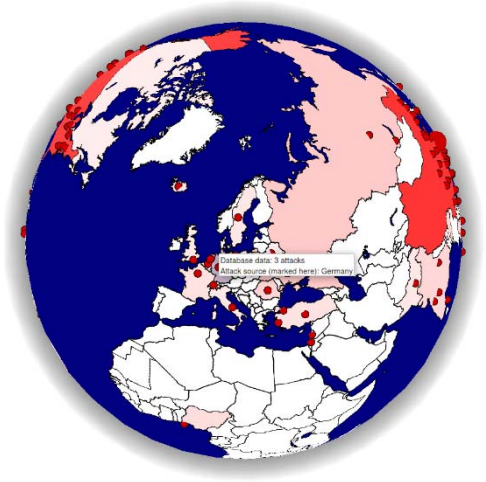
Universität Hamburg
DER FORSCHUNG | DER LEHRE | DER BILDUNG



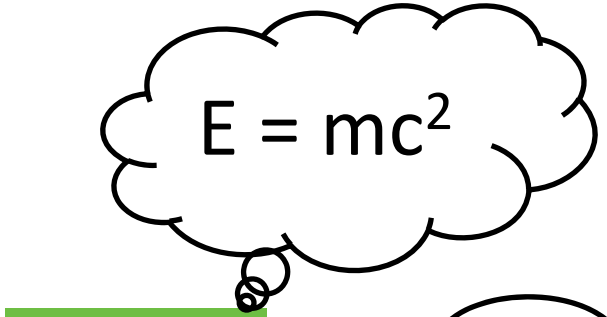
IT-Sicherheit in einer vernetzten Welt

Prof. Dr. Mathias Fischer

Wer bin ich?

Mein Auto

- Wie ich aussehe
- Was ich habe
- Was ich weiß
- Was ich kann
- Was ich mag
- Mein soziales Netz
- Was über mich gesagt wird

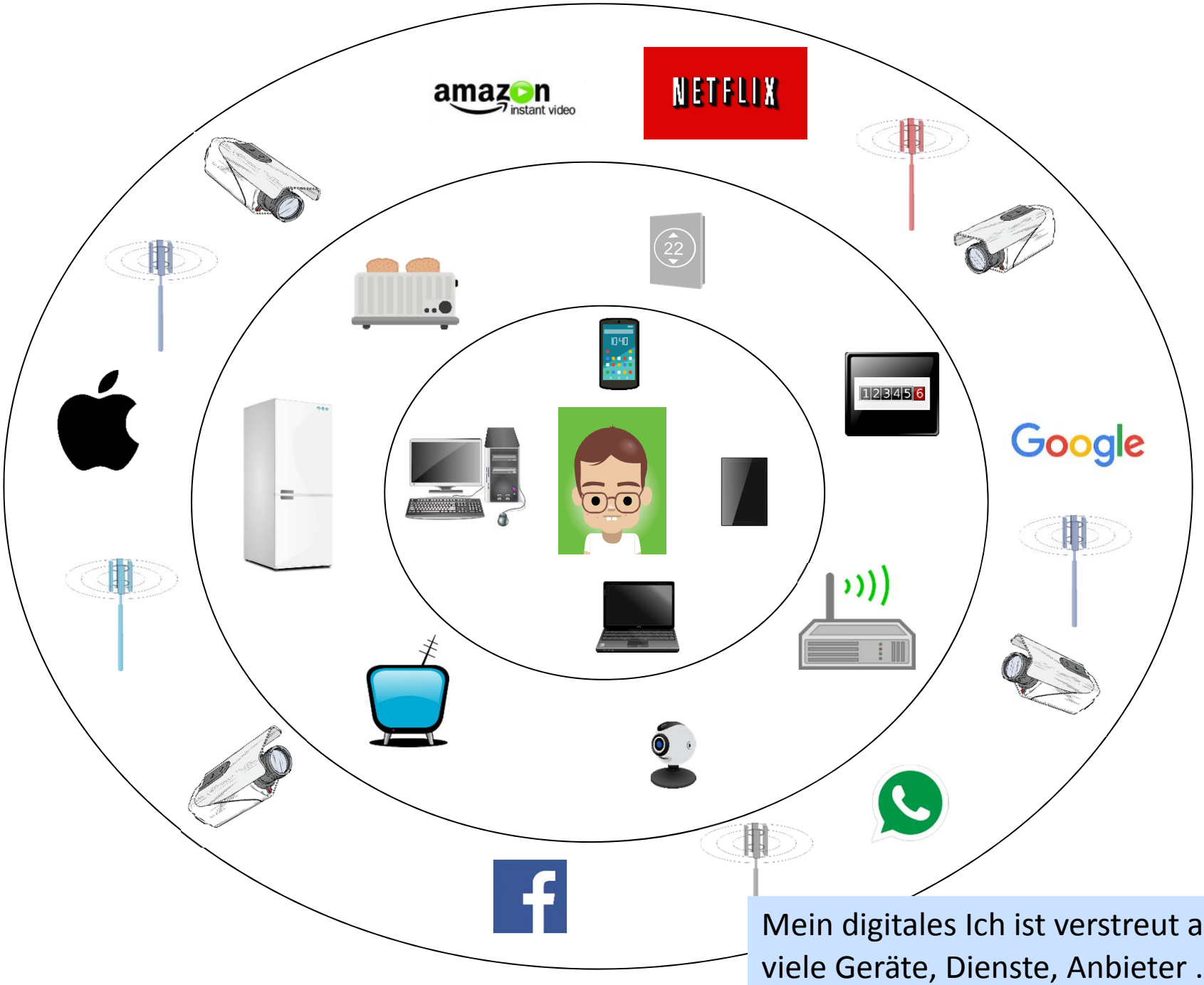


Ich

Meine Freunde

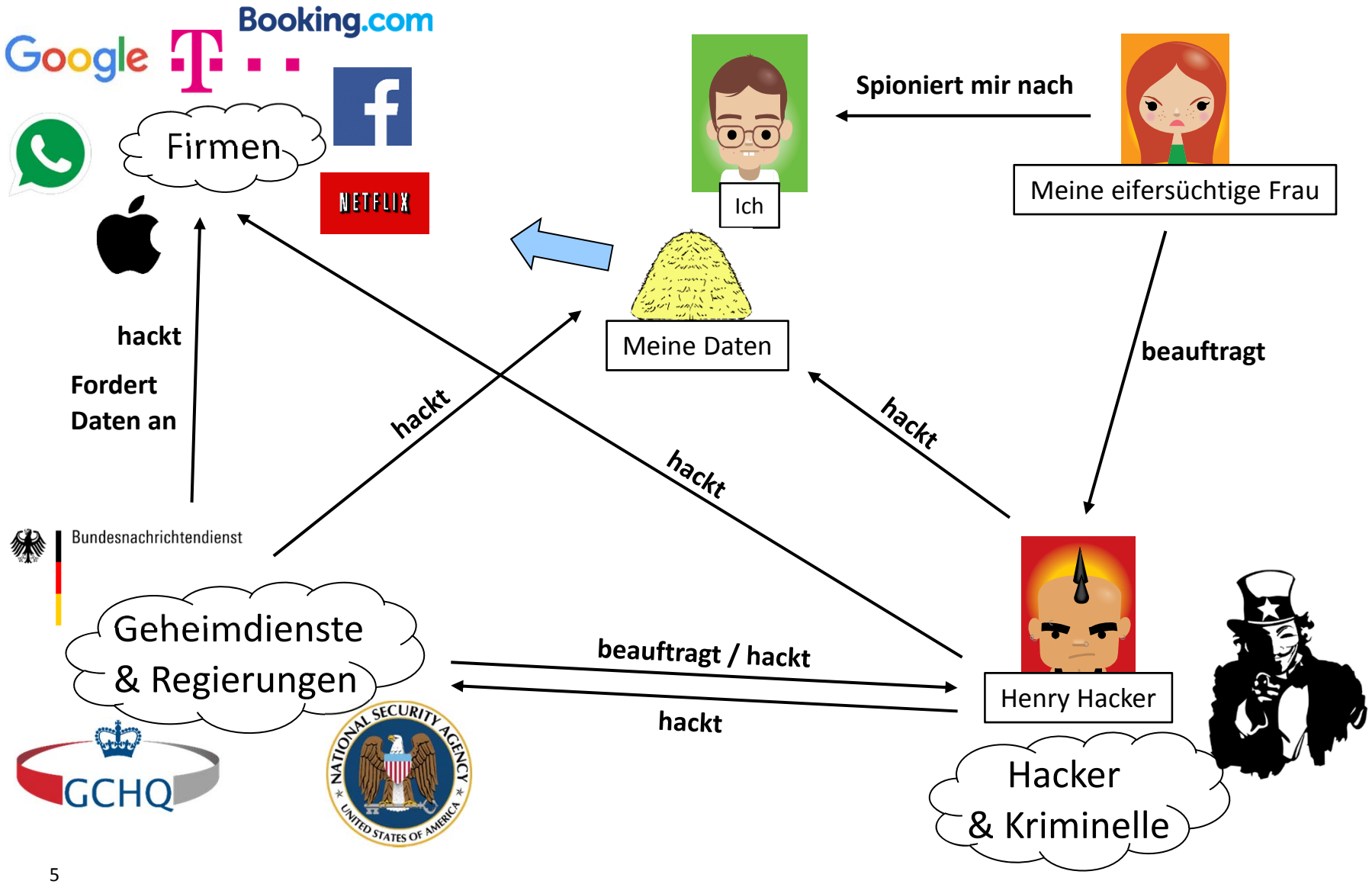
Ich liebe Kaffee

Mein Diplom

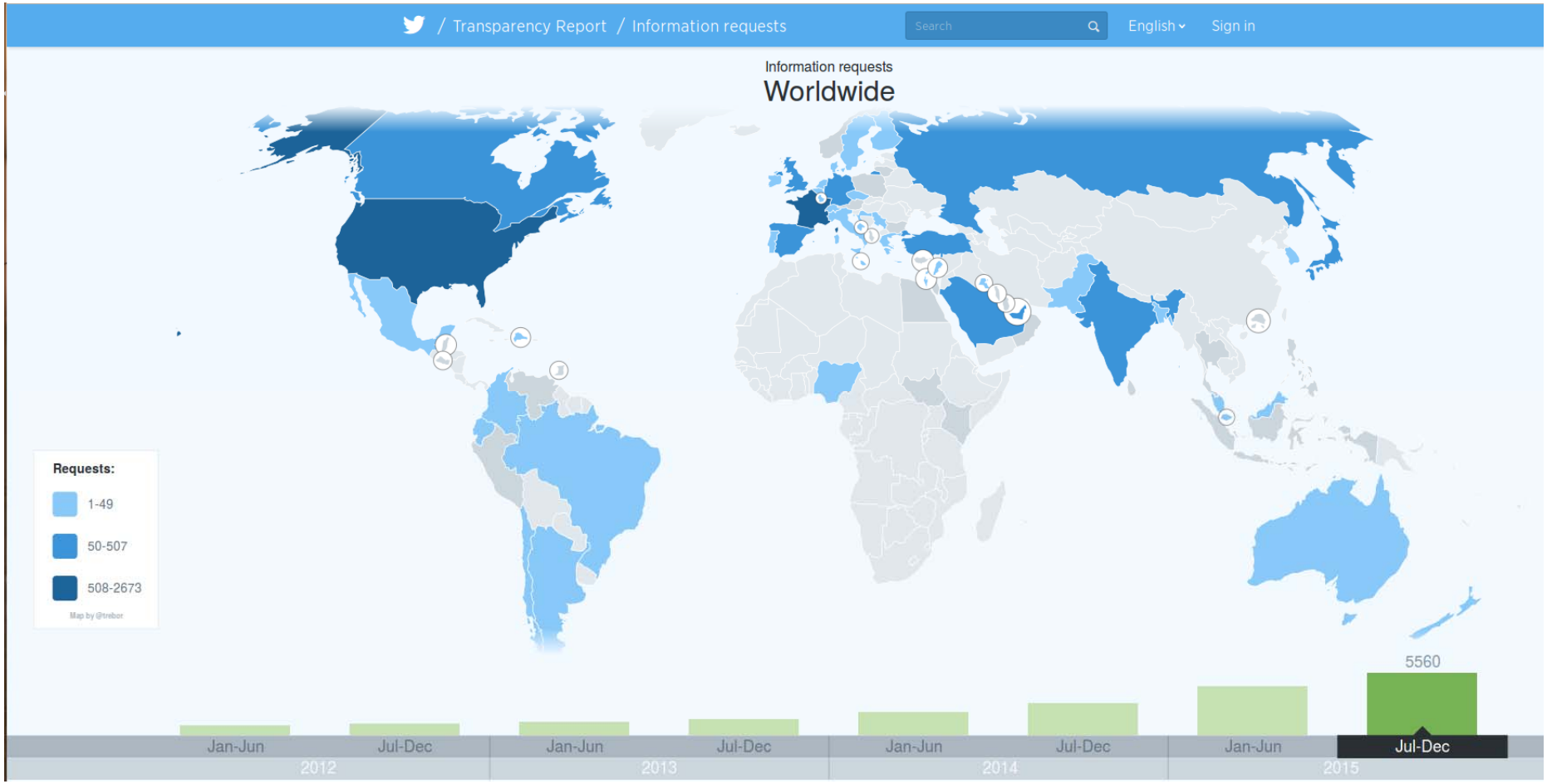

amazon instant video
NETFLIX
Google
Mein digitales Ich ist verstreut auf viele Geräte, Dienste, Anbieter …

Aber, ich habe doch nichts zu verbergen!

Wer interessiert sich überhaupt für meine Daten?



Aber gerade Firmen haben doch kein Interesse daran meine Daten an den Staat weiterzugeben!?



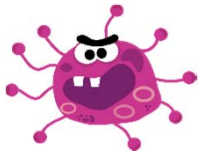
Interesse daran haben sie nicht, machen müssen sie es trotzdem…

"Wer behauptet, er interessiere sich nicht für Privatsphäre, weil er nichts zu verbergen habe, verhält sich genau wie jemand, der sagt, Meinungsfreiheit sei ihm egal, weil er nichts zu sagen hat."

Edward Snowden

Bildquelle: www.wired.com

Datenschutz ist das eine, Datensicherheit das andere…
- Das Jahr 2015 aus Sicherheitsperspektive



430 Millionen Malware-Programme

Pro Woche eine Zero-Day Schwachstelle

Halbe Milliarde gestohlener Datensätze

Sicherheitslücken auf ¾ aller populären Webseiten

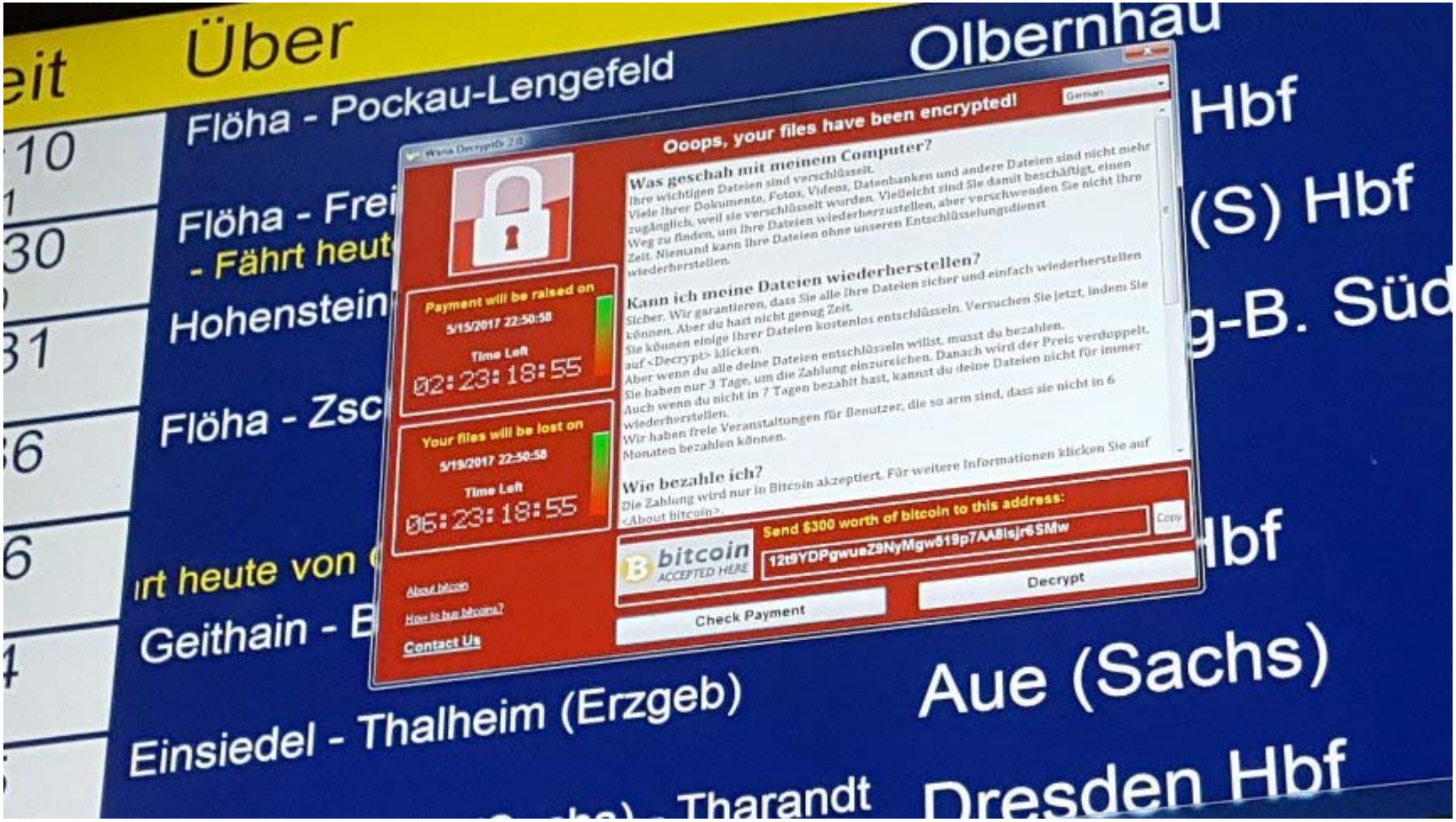
55% Anstieg von Spear-Phishing Kampagnen gegen Angestellte

35% Anstieg bei Ransomware (Verschlüsselungstrojaner)

[Sym2016]

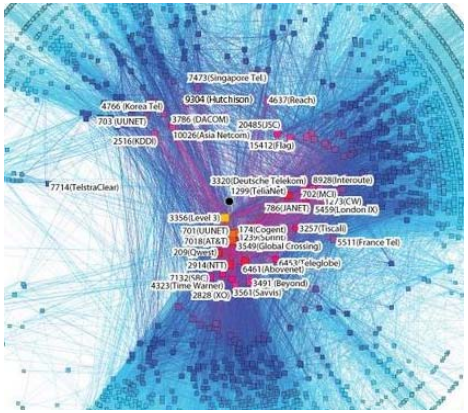
Ransomware: WannaCry

Ransomware: WannaCry



Quelle: spiegel.de

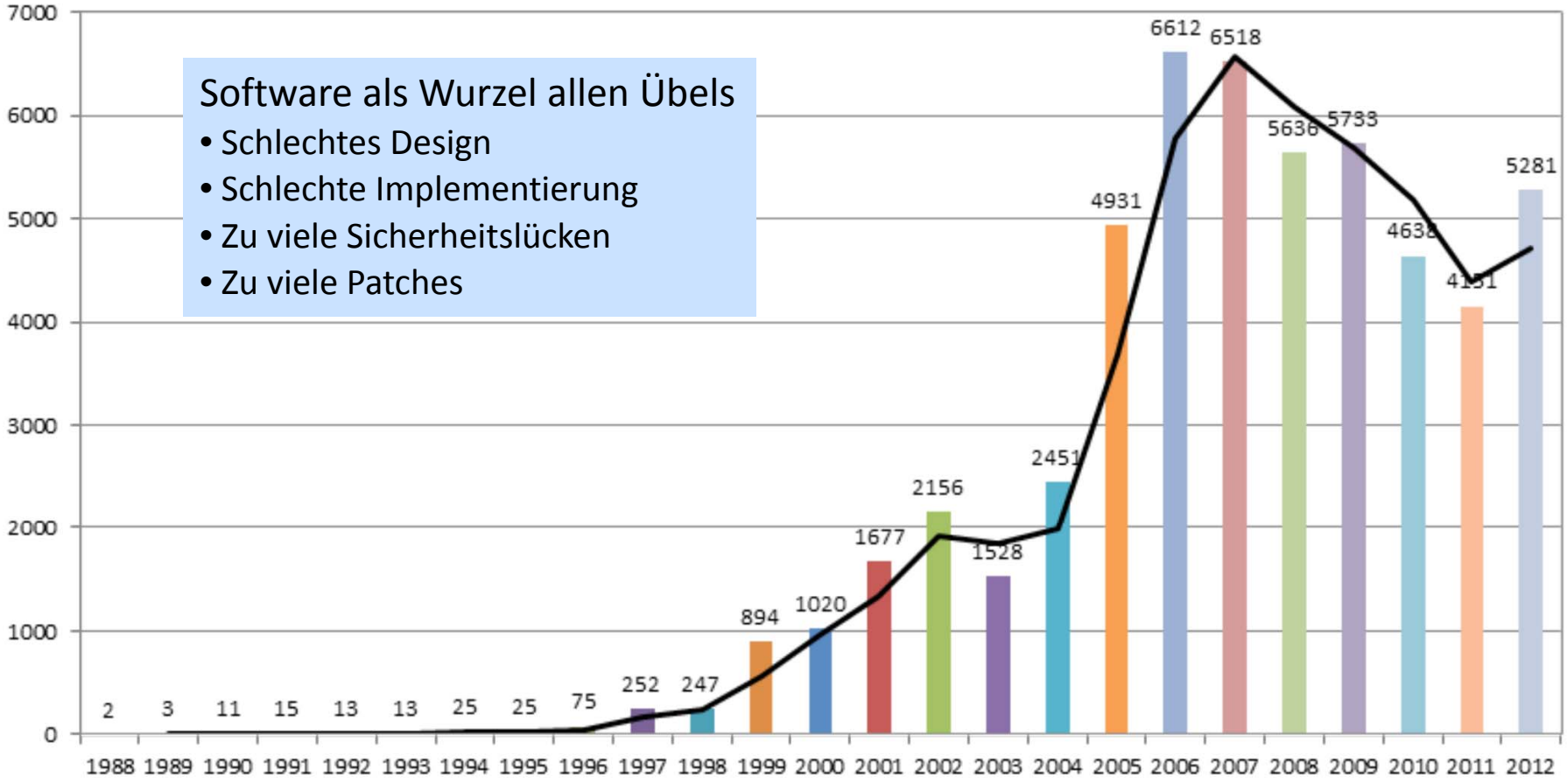
Internet als kritische Infrastruktur



- Das Internet ist eine kritische Infrastruktur
  - Zielgerichtete Hacker-Angriffe
  - Kriegsschauplatz und Cyber-Waffen
- Neue Bedrohungen:
  - Cyber-physikalische Systeme
  - Internet of Things (IoT) und Industrie 4.0

Die Rolle von Software

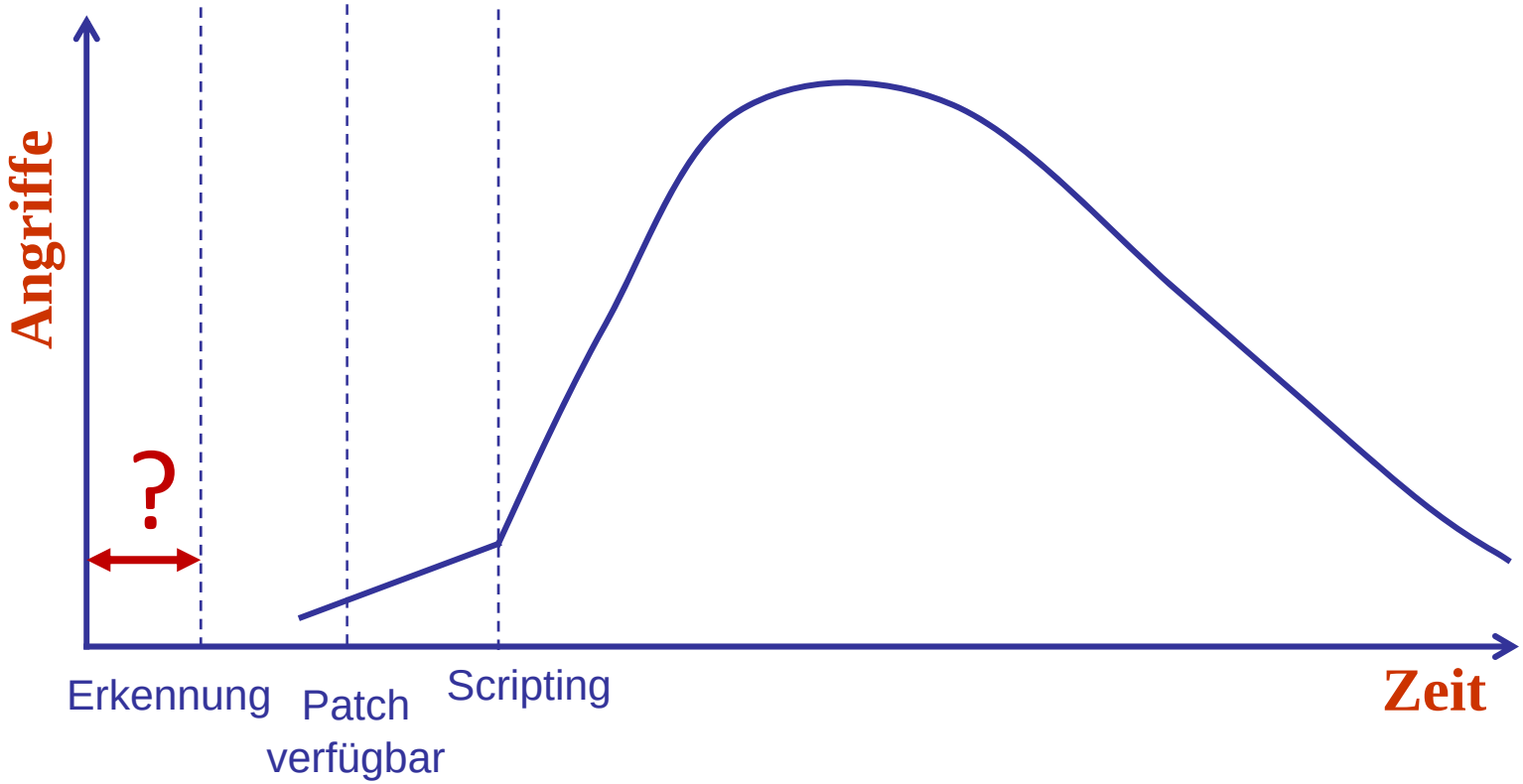
Unmöglich Sicherheit auch nur moderat komplexer Software zu beweisen



Software-Schwachstellen pro Jahr [Yo2012]

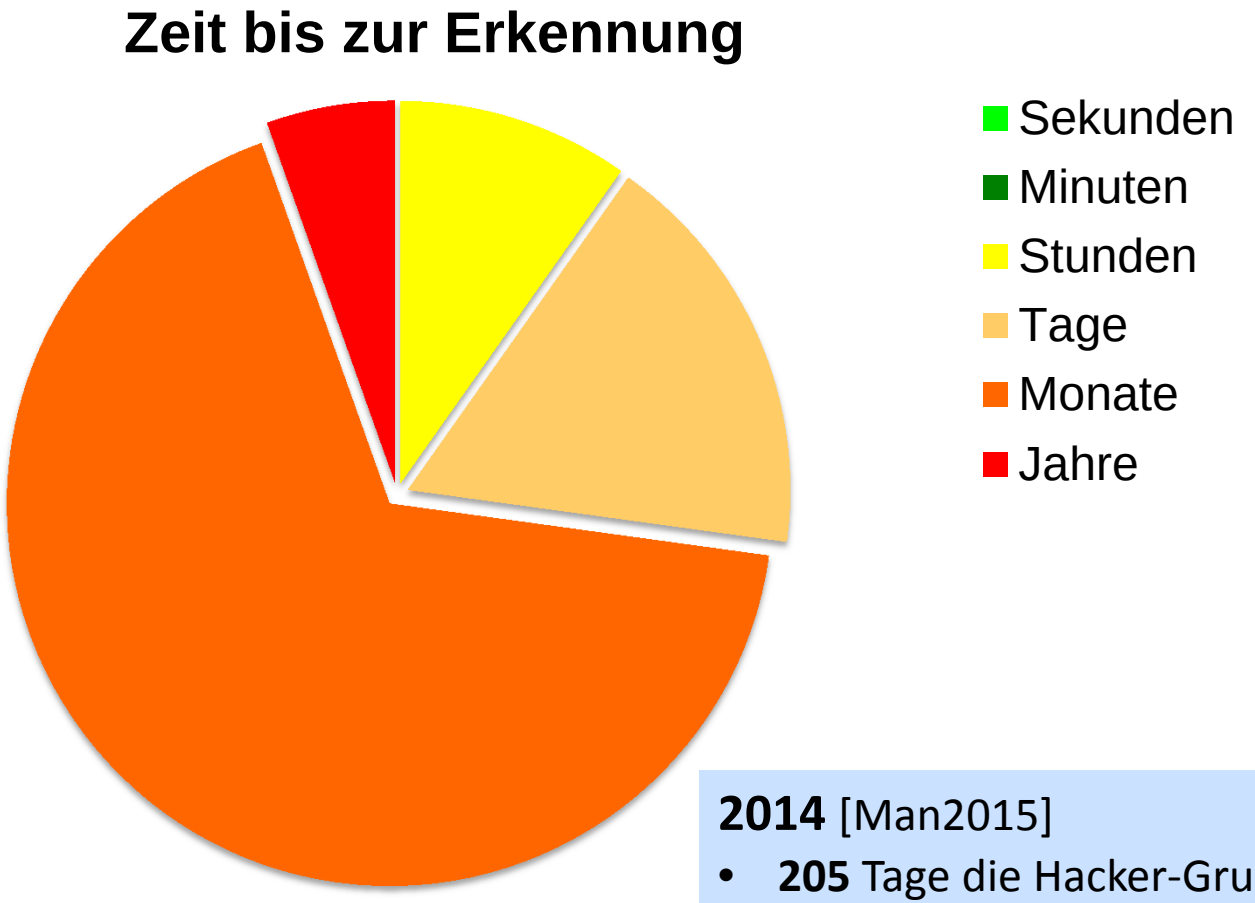
Der Lebenszyklus einer Software-Schwachstelle

[Arb2000]



- Schwachstellen werden öfters ausgenutzt, sobald ein Patch verfügbar ist
- Aber: Zero Day Exploits, Hersteller die Schwachstellen nicht beheben

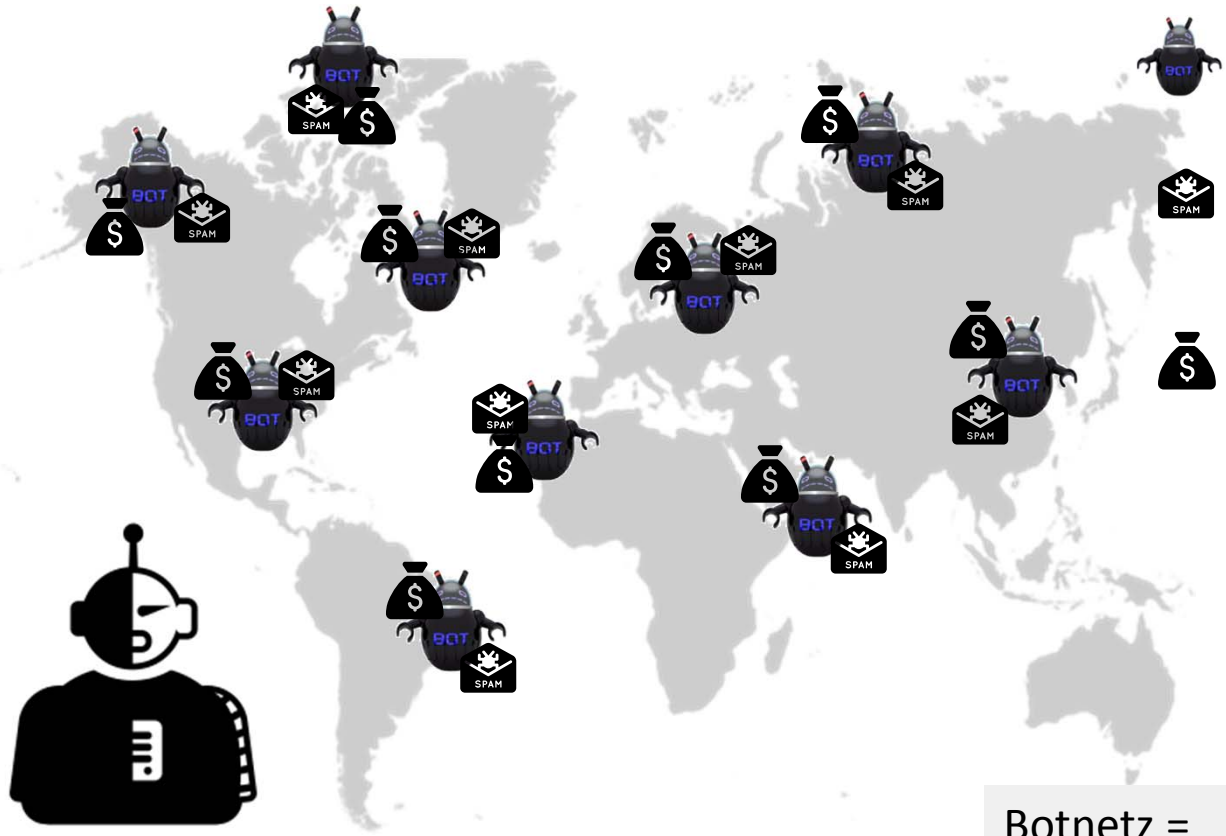
Zeit bis zur Erkennung von Cyber-Angriffen



2014 [Man2015]

- **205** Tage die Hacker-Gruppen in Netzwerken präsent waren bevor sie erkannt wurden
- Längste Präsenz: **2982 Tage**
- **31**% Opfer erkennen Angriff intern
- **69**% Opfer werden von externen Stellen informiert

Beispiel für fortschrittliche Malware: Botnetze



Botmaster

Conficker: 15 Millionen Bots (2009)

Grum: 39.9 Milliarden Spam-Emails pro Tag (2010)

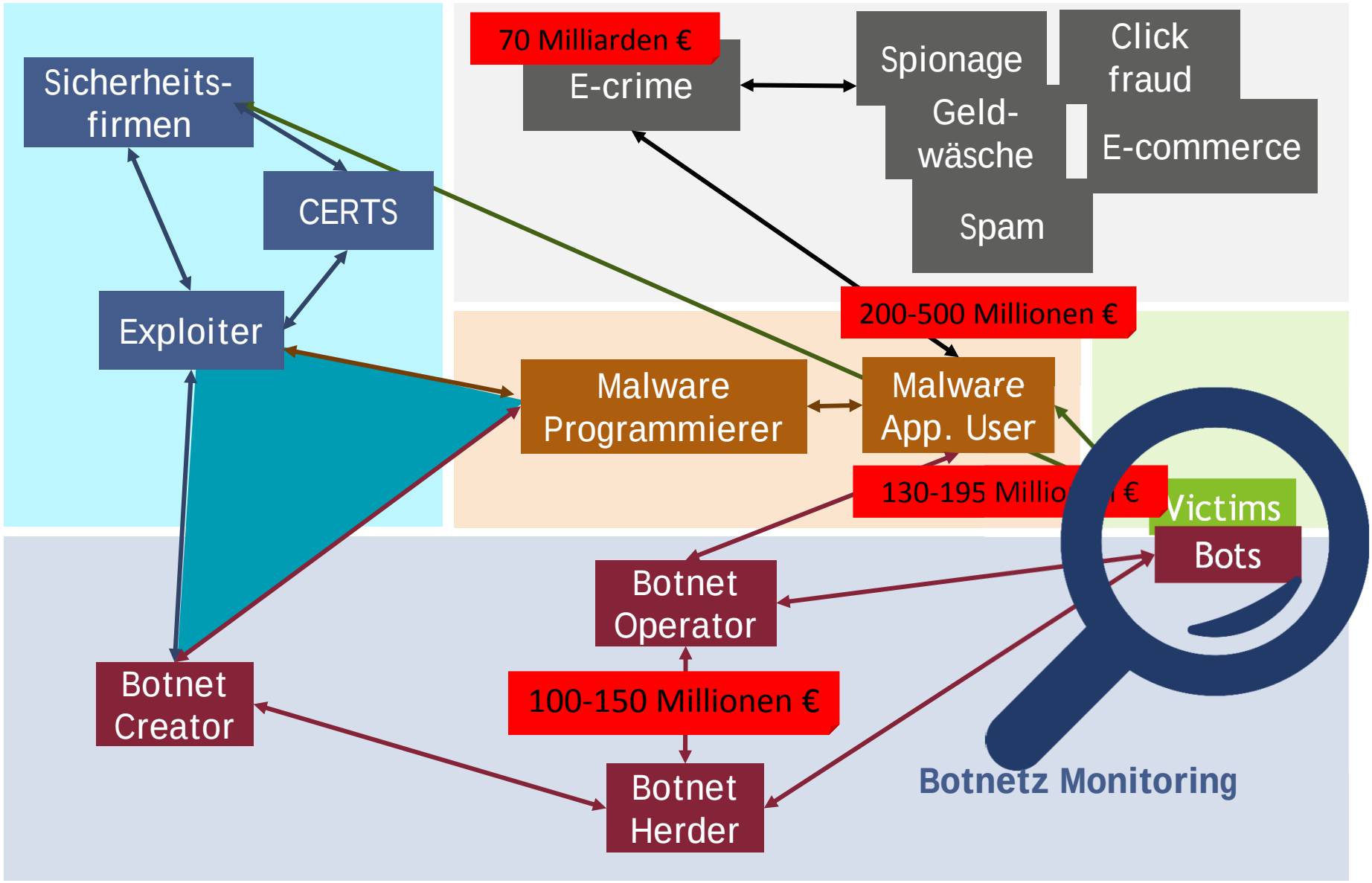
ZeroAccess: $100.000 pro Tag (2012)

Dridex (Bugat v5): Bank-Trojaner stielt $30.5 Millionen (October 2015)

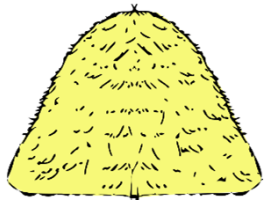
Botnetz =
Armee infizierter Computer (Bots)
Kontrolliert von einer Instanz
Automatischer Update Mechanismus

Das Botnetz Ökosystem

[KoKu2011]



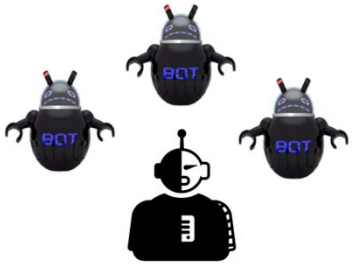
Zwischenstand



- Daten sind das neue Öl
- Firmen und Geheimdienste als größte Datensammler
- Wirtschaftsspionage und Erpressung

- Software ist zu komplex
- Zu viele Verwundbarkeiten in Software
- Zu viele Patches

- Erfolgreiche Angriffe sind die neue Normalität
- Wir brauchen viel zu lange um Angriffe überhaupt zu bemerken



- Angreifer sind höchst arbeitsteilig
- Eigene Schattenwirtschaft mit massiven Profiten

Und nun? Cyber-Depression?

FUD-Strategie — Fear, Uncertainty, Doubt

Wieviel muss wirklich in Sicherheit investiert werden?

vs.

Furcht, Ungewissheit, Zweifel

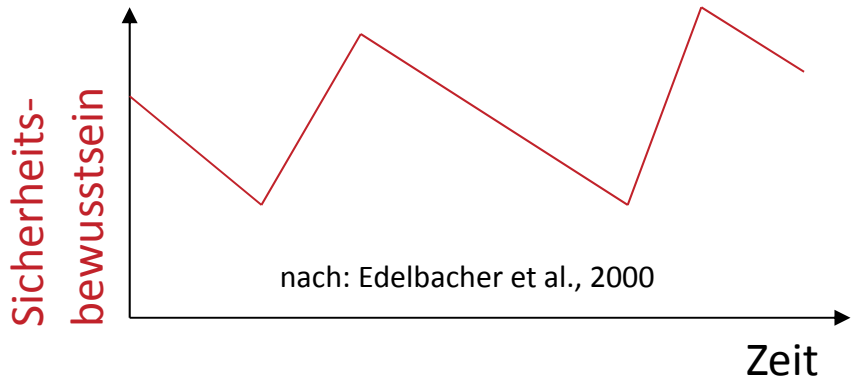


Bild: Bob Eggleton
Quelle: http://lair2000.net/Mermaids_Retreat/Research/Kraken.html

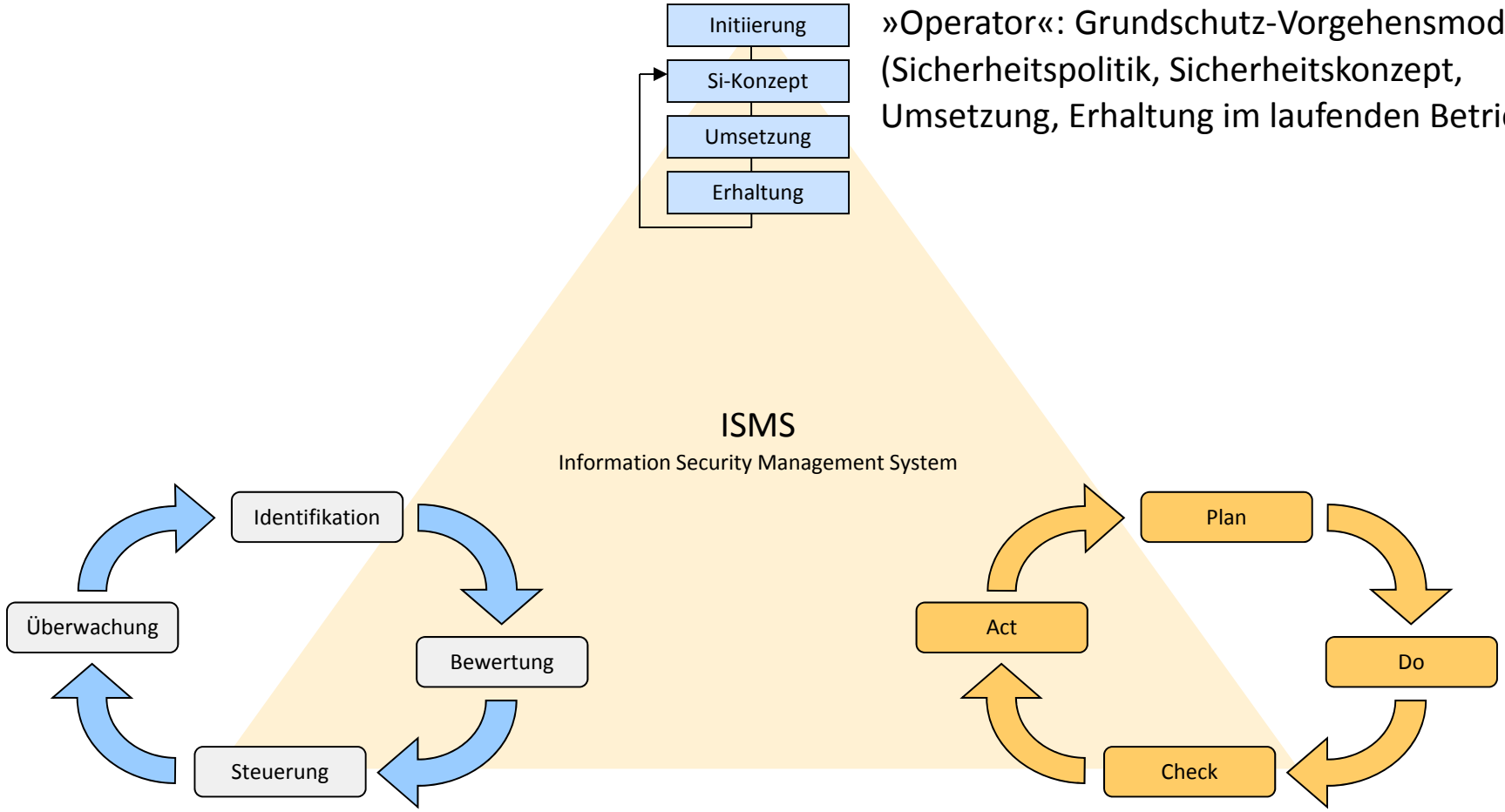
Also was tun?

- Aktives Sicherheitsmanagement in Unternehmen benötigt!
  - Tief verankert in Unternehmenskultur
  - Kontinuierlicher Prozess zur Etablierung und Wahrung von Informationssicherheit
- Best Practices – Lernen von anderen
- Informationsaustausch
  - Über Bedrohungen und Gegenmaßnahmen
  - Über erfolgreiche Angriffe
  - Die Angreifer arbeiten bereits zusammen!
- Beispiele
  - ISO 27000 Familie
  - BSI IT Grundschutz
    - Für kleine und mittlere Unternehmen: *Leitfaden zur Basisabsicherung nach IT-Grundschutz*

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 Sicherheitspolitik in Konkrete Maßnahmen; Risikoanalyse
Systemebene / Mechanismen	Unterstützung der Prozesse durch den Einsatz von Systemen; Analyse und Spezifikation der Anwendungssysteme	Detaillierung der Maßnahmen durch konkrete Mechanismen

Information Security Management System (ISMS)



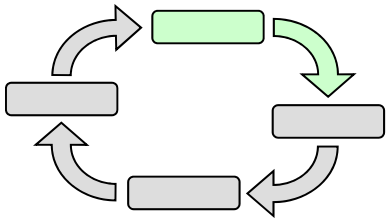
»Operator«: Grundschutz-Vorgehensmodell (Sicherheitspolitik, Sicherheitskonzept, Umsetzung, Erhaltung im laufenden Betrieb)

»Controller«: Risikomanagement (Identifikation, Bewertung, Steuerung, Überwachung)

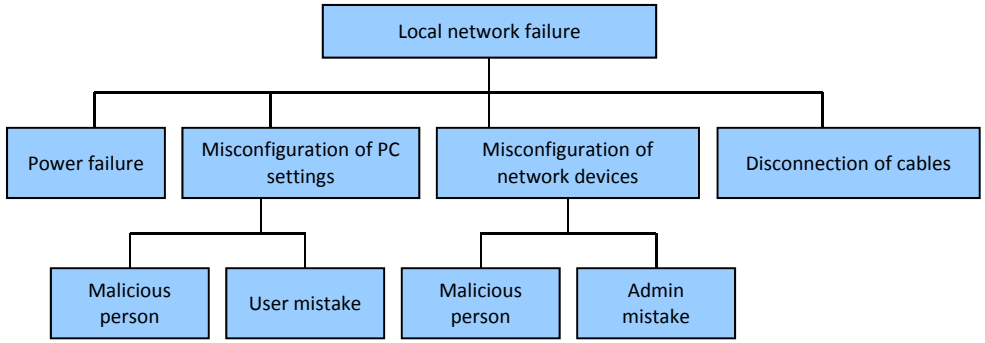
»Management«: Deming-Kreislauf (Plan, Do, Check, Act)

Identifikation von Bedrohungen

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



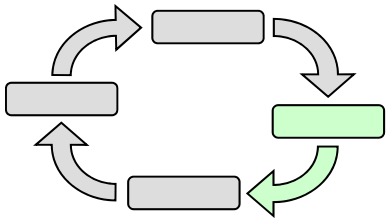
- Methoden & Werkzeuge
  - Checklisten und Workshops
  - Fehler- und Angriffsbäume
  - Szenarioanalysen
  - Historische Daten



- Herausforderungen
  - Vollständige Erfassung aller Bedrohungen

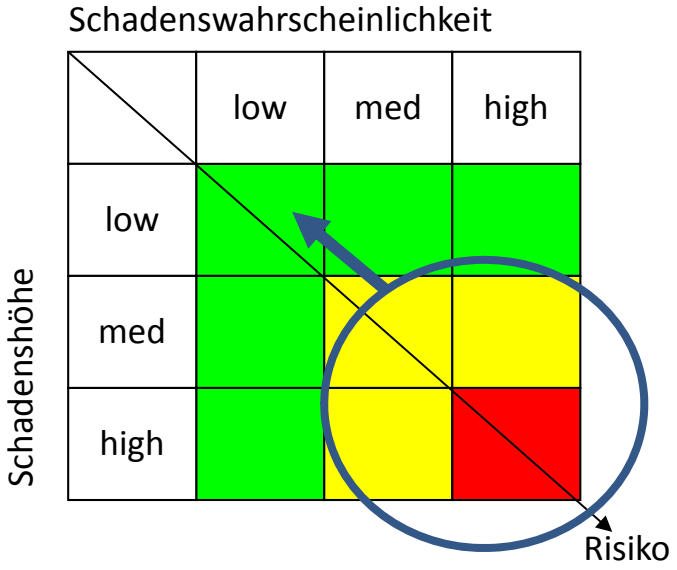
Bewertung von Risiken

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

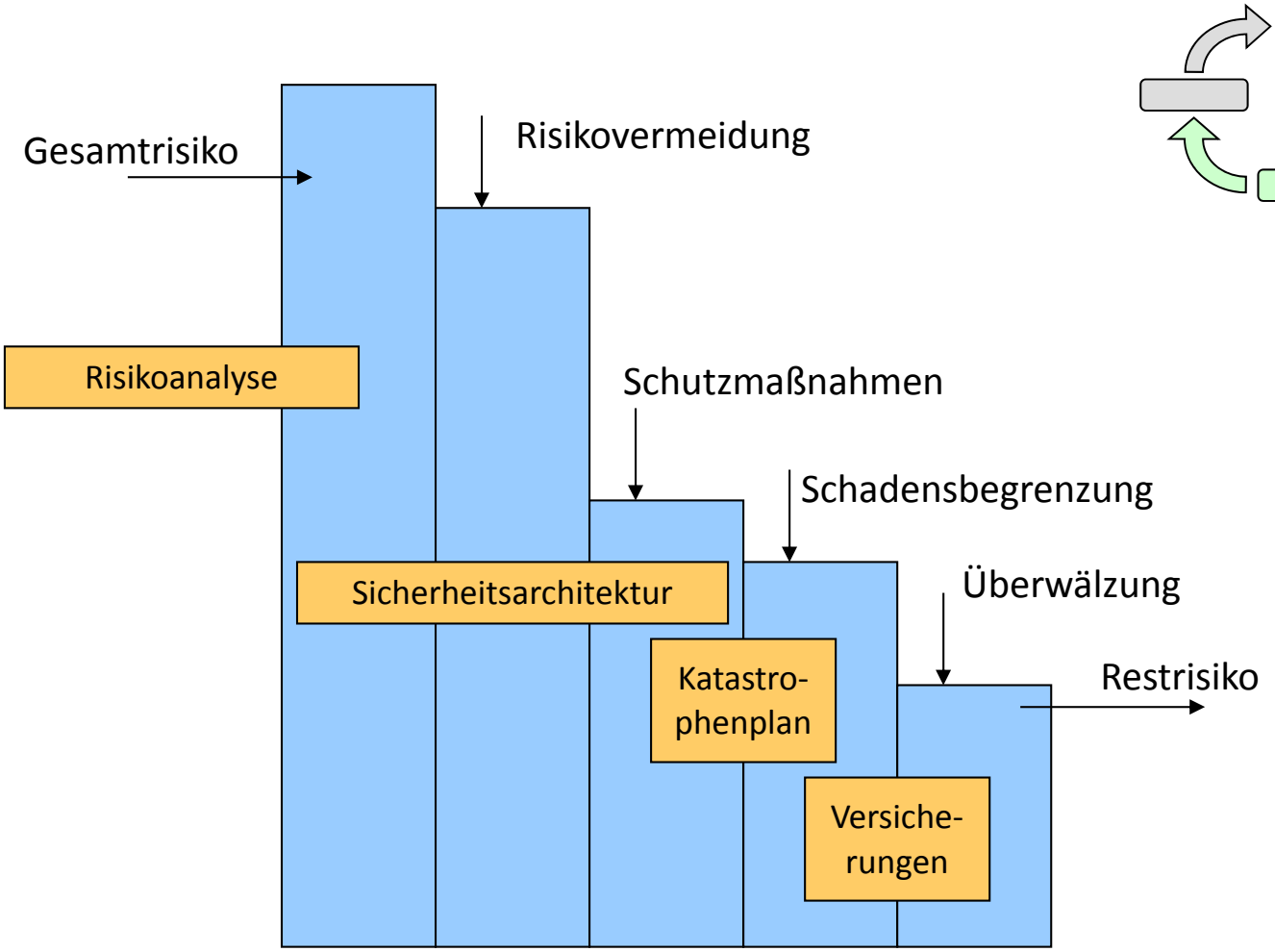


- Methoden & Werkzeuge
  - Qualitative Bewertung
  - Quantitative Bewertung
  - Maximalwirkungsanalyse

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

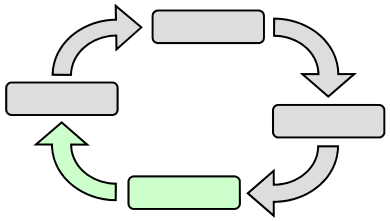


Risiko-Management für IT-Systeme



nach: Schaumüller-Bichl 1992

Typische Positionen für Vermeidung, Akzeptanz und Überwälzung:

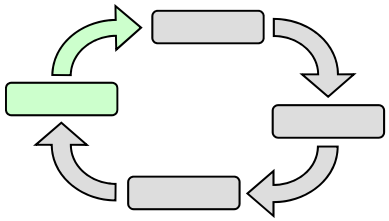


Schadenswahrscheinlichkeit

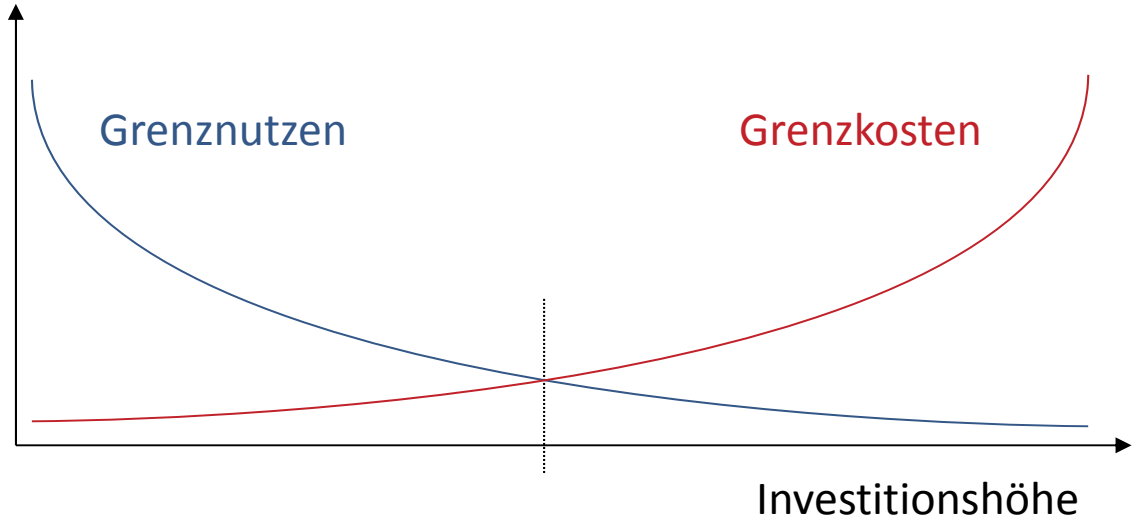
Schadenshöhe	low	med	high
low	Akzep-tanz	Vermeidung	
med		Schutzmaß-nahmen	
high	Über-wälzung		

Überwachung der Risiken und Maßnahmen

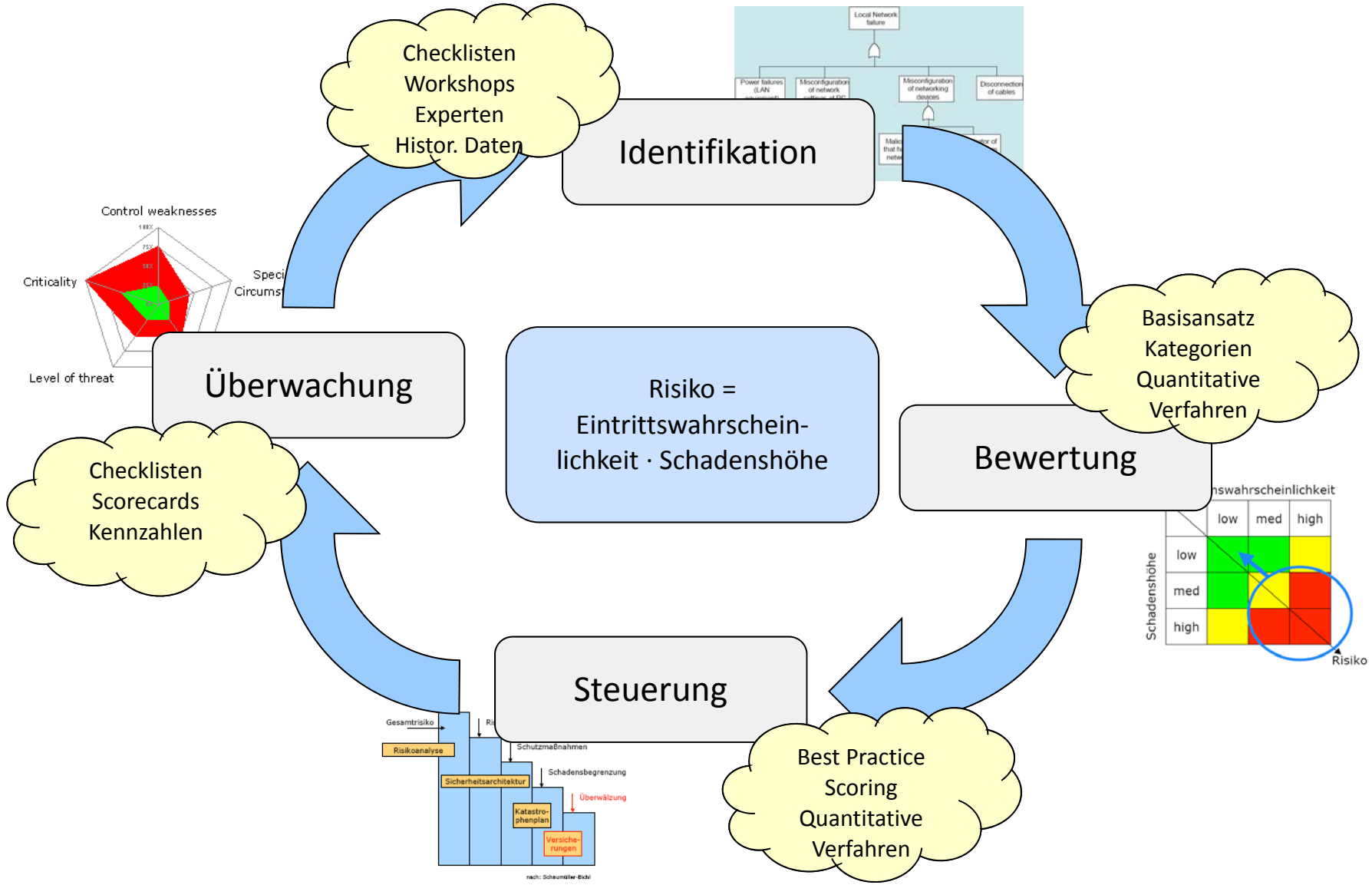
- Frage
  - »Waren die Maßnahmen effektiv und effizient? Wie sicher ist die Organisation?«



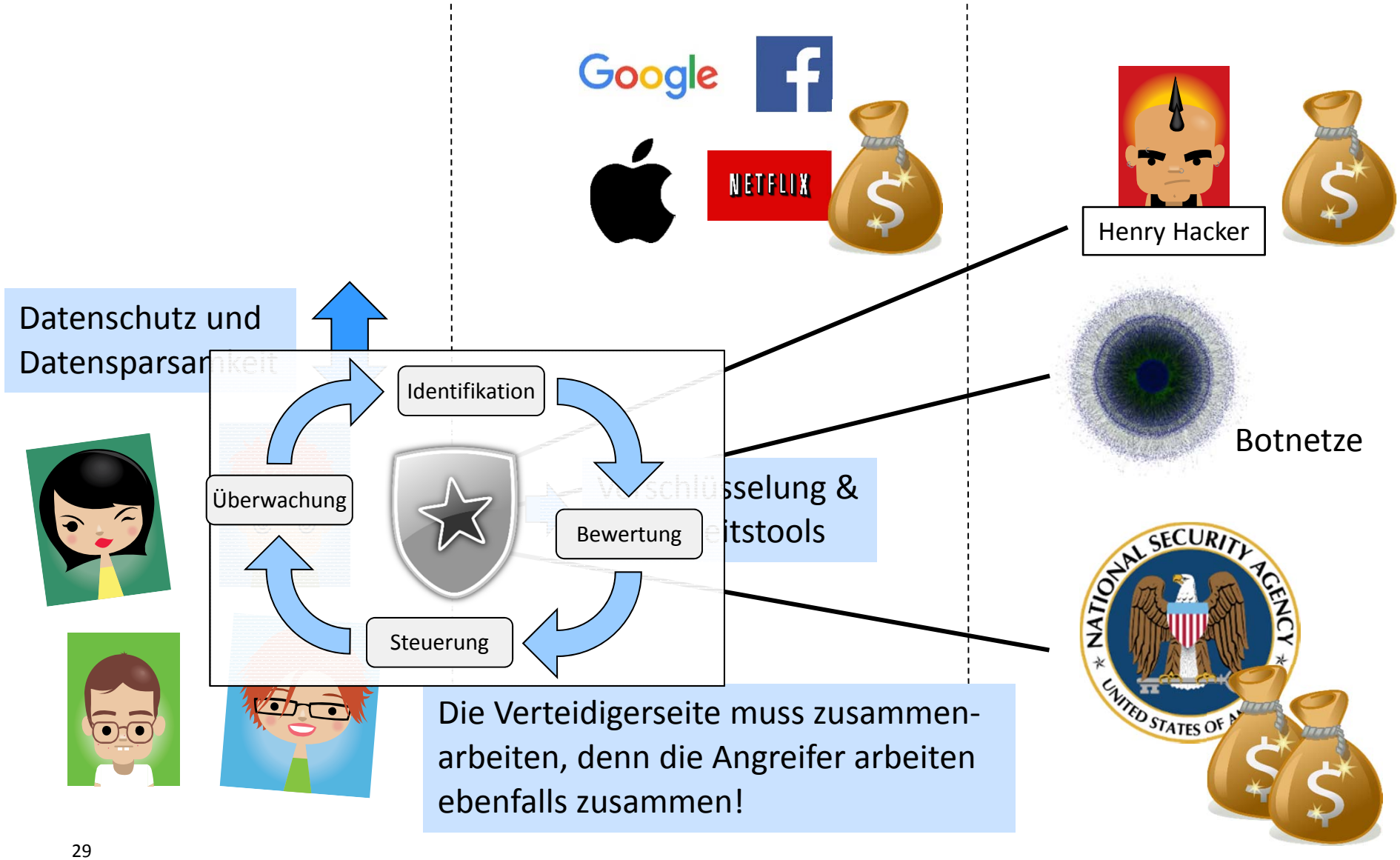
Viel hilft nicht unbedingt viel, es kommt auch darauf an, wie das Geld ausgegeben wird



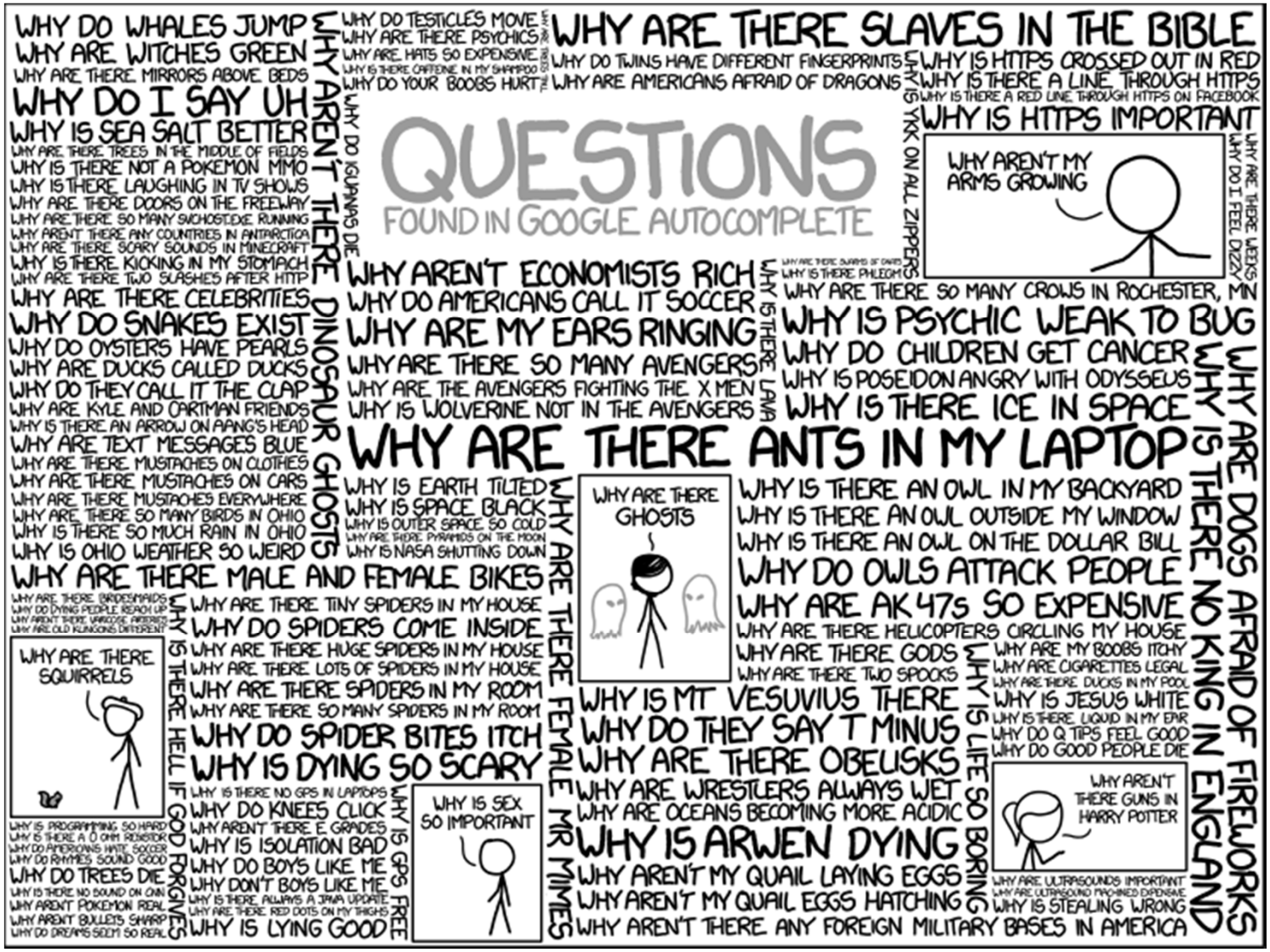
Sicherheits- / Risikomanagement Kreislauf



Zusammenfassung



Fragen?



Referenzen

[Man2015] Mandiant, M-Trends® 2015: A View from the Front Lines https://www2.fireeye.com/WEB-2015-MNDT-RPT-M-Trends-2015_LP.html

[Sym2016] Symantec, Internet Security Threat Report, 2016, https://www.symantec.com/security-center/threat-report

[Yo2012] Yves Younan, 25 Years of Vulnerabilities: 1988-2012, RESEARCH REPORT, Sourcefire Vulnerability Research Team (VRT)

[ICS2015] NCCIC/ICS-CERT Year in Review National Cybersecurity and Communications Integration Center/ Industrial Control Systems Cyber Emergency Response Team, 2015, https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/Year_in_Review_FY2015_Final_S508C.pdf

[Arb2000] “Windows of Vulnerability: A Case Study Analysis”, Arbaugh, et al IEEE Computer, Dec. 2000

[KoKu2011] “Analysis of the BotNet Ecosystem”, Conference on Telecommunication, Media and Internet Techno-Economics (CTTE), 2011

[ISO27001] ISO/IEC, “ISO/IEC 27001:2005—Information technology—Security techniques—Information security management systems—Requirements,” 2005.

[ISO27005] ISO/IEC, “ISO/IEC 27005:2008—Information technology—Security techniques—Information security risk management,” 2008.