Vortrag

Gefahrenabwehr in der Post-Snowden-Ära

Kiel, den 19. Mai 2014

erstellt für
DiWiSH-Veranstaltung

sure it .de
Stefan Rieber
consulting

Vorstellung

Stefan Rieber

- Diplom-Ingenieur (FH) Technische Informatik
- Berater für IT-/ Informationssicherheit
- > 20 Jahre IT-Erfahrung

Branchenkenntnisse

- Banken (IT-Sicherheit und operationelles Risikomanagement)
- Fertigungsindustrie (Software Entwicklung & Integration)
- Medien (Client Services)

Schwerpunkte

- IT-/ IT-Sicherheitsstrategie und IT Governance
- Management von IT-/ Informationssicherheit
- Systemanalyse und IT-Audit, Zertifizierung
- Management von operationellen Risiken
- Prozess- und Service-Management
- Projektportfolio- und Projektmanagement
- Software- und Systementwicklung
- Outsourcing und Steuerung externer Dienstleister

Kontakt

Telefon +49 151 17216257

eMail mail@sureit.de

Web www.sureit.de

Bedrohungen

Der NSA-Skandal

Quelle: Wikipedia

sure it .de
Stefan Rieber consulting

Bedrohungen

Industriespionage - Beispiel 1

Ziel des Angriffs

Mittelständisches Unternehmen im Energiesektor
mit eigener F&E-Abteilung

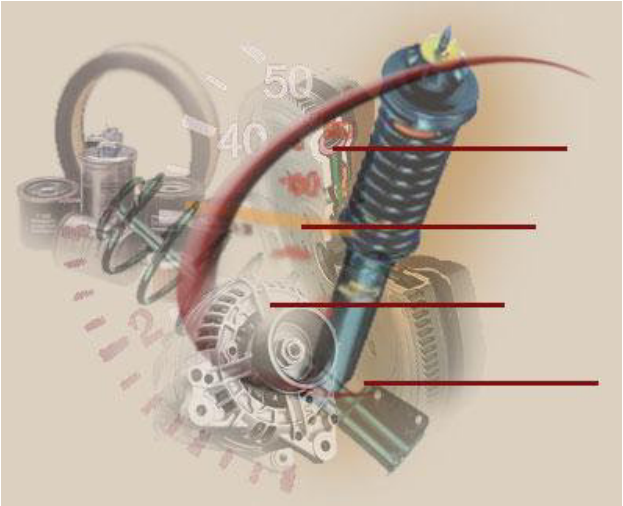
Analyse der Vorfalls

- Bei Bauarbeiten wird zufällig eine Manipulation des Firmennetzwerkes entdeckt
- Bei den verwendeten Komponenten handelt es sich um günstige Massenprodukte (keine Rückschlüsse aus Seriennummern, …)
- Keine relevanten (Zugriffs-)Spuren im Netzwerk
- Hinweise auf Insider
- Untersuchung der Zugangsdaten ergibt korrespondierendes Bewegungsmuster mit einer verlorenen Zugangskarte
- In der verdächtigen Zeitperiode kann ein IP-basierter Datentransfer nach China nachgewiesen werden …

Quelle: Verfassungsschutz

Bedrohungen

Industriespionage - Beispiel 2



Ziel des Angriffs

International agierender Automobil-Zulieferer
mit eigener F&E-Abteilung

Analyse des Vorfalls

- Software-Entwickler wird auffällig, als er versucht, die Telefonanlage zu manipulieren (freie Telefonate)
- Keine Anzeige - Behörden werden nicht aktiv
- Ungewöhnliche Arbeitszeiten, Löschung von Dateien, fragwürdige Kontakte, Spielschulden
- Mitarbeiter ist in westliches Land “geflohen”
- Einbruch in Unternehmensnetzwerk erfolgt aus der lokalen Niederlassung. Verwendet werden Zugangsdaten eines ehemaligen Mitarbeiters …

Quelle: Verfassungsschutz

Bedrohungen

Typische Quellen

Exploiting

Spam

Sniffer

APT

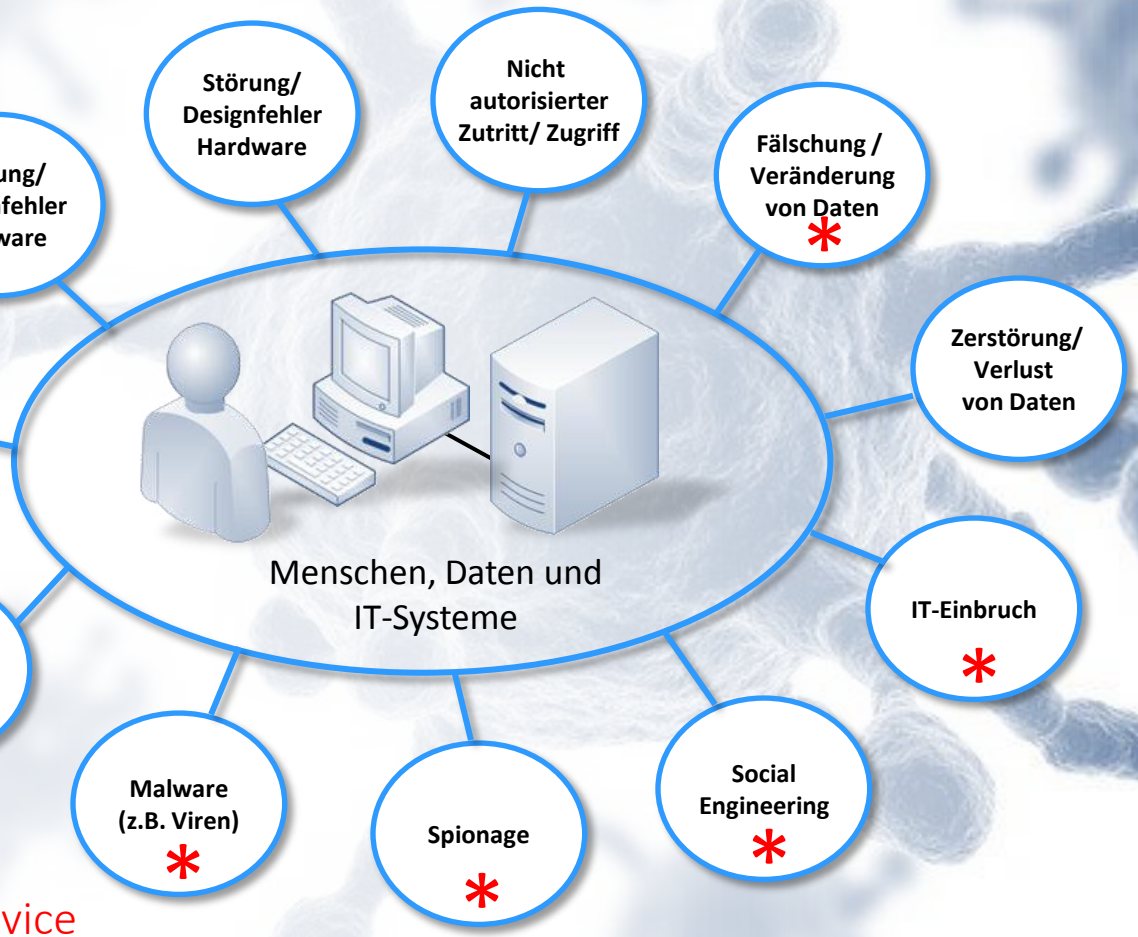
ID theft

Backdoor

Phishing

Root Kit

Denial of Service

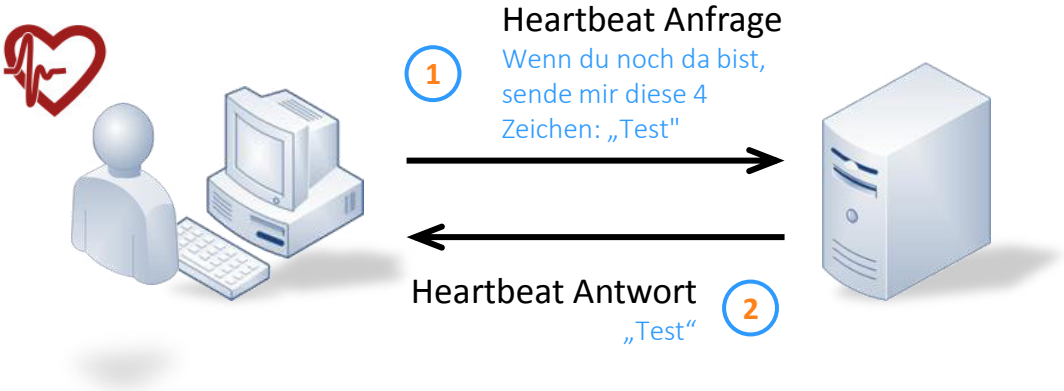


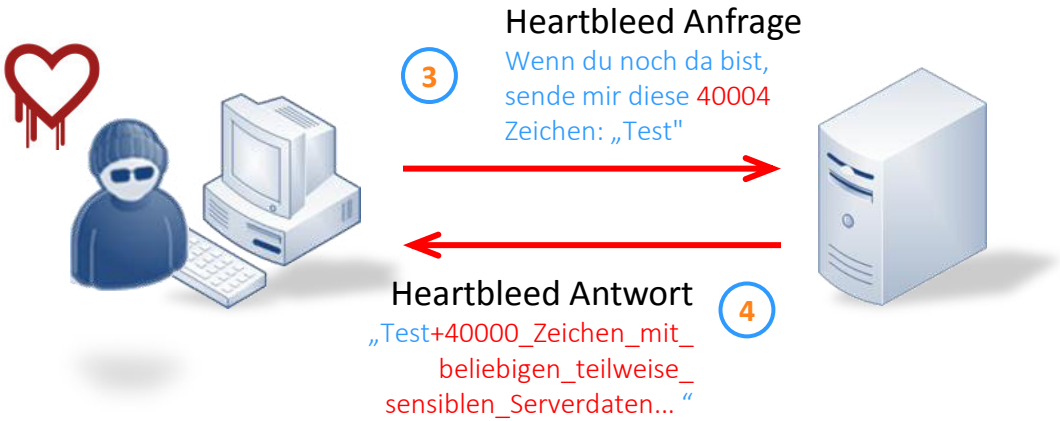
* : Vorsatz als Quelle der Bedrohung

sure it .de
Stefan Rieber consulting

Bedrohungen

Heartbleed (1/2)





Source: Wikipedia

Bedrohungen

Heartbleed (2/2)

Betroffen	**OpenSSL**
Seit	**14.03.2012**
Verwundbarkeit	Buffer-Overread Pro Anfrage können **64 kByte des Arbeitsspeichers** ausgelesen werden
Schaden	**Unklar**, da ein Angriff nur sehr wenig Spuren hinterlässt.

Empfehlung

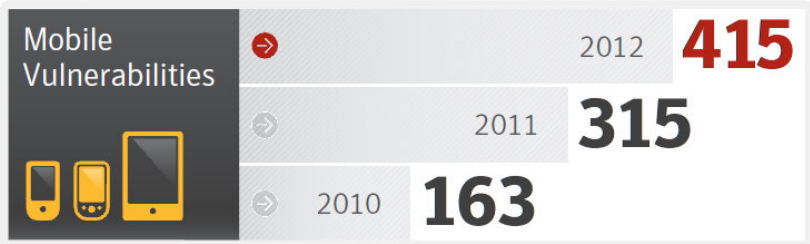
→ Austausch der Serverzertifikate.
→ Nutzern wird empfohlen, alle Passwörter zu ändern.

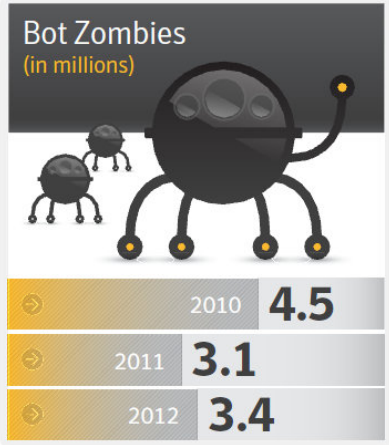
„Das OpenSSL-Team wies auf zu wenig Ressourcen als strukturelles Problem bei der Entwicklung der Software hin und bat um finanzielle Unterstützung.“

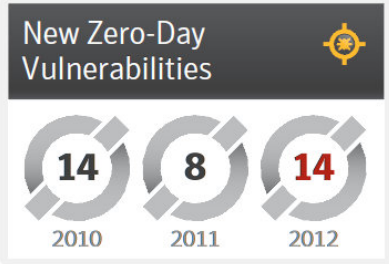
Quelle: Wikipedia

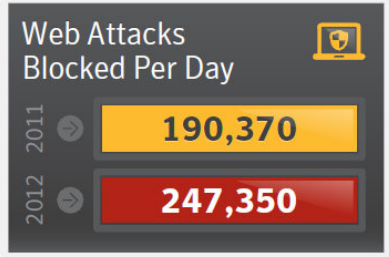
Bedrohungslage 2013

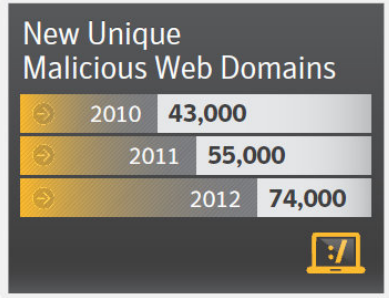
Auszug aus dem Symantec Internet Security Threat Report











Quelle: Symantec ISTR 2013

Bedrohungslage 2013

Targeted Attacks und Advanced Persistent Threats (APT)

Targeted Attacks

… werden für einzelne Unternehmen entwickelt.

Im Gegensatz zu weit verbreiteten Angriffen neigen gezielte Angriffe dazu, nicht gemeldet zu werden. Oft gibt es keine Werkzeuge für Erkennung und Gegenmaßnahmen (z. B. fehlende Muster für Malware-Scanner).

Advanced Persistent Threats

… hochentwickelte, getarnte, i.d.R. langandauernde, kontinuierliche Angriffe auf ein bestimmtes Unternehmen. Oft durch menschliche Interaktionen orchestriert.

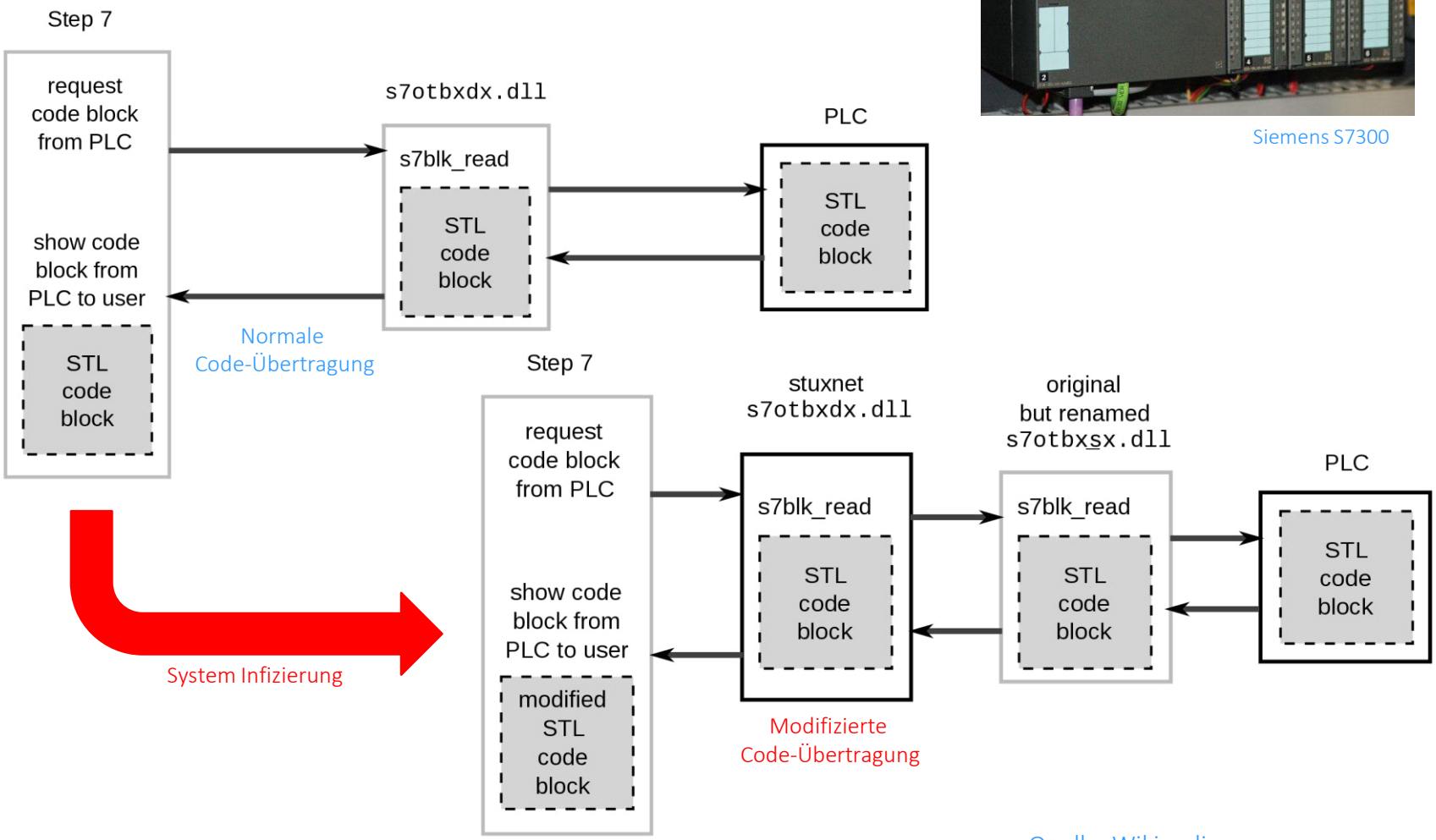
Advanced: Nutzung von anspruchsvollen Techniken, um sich zu tarnen und Sicherheitslücken auszunutzen.

Persistent: kontinuierliche Angriffe/ Überwachung und Extraktion von Daten von einem bestimmten Ziel.

Bedrohungen

Targeted Attack - Stuxnet

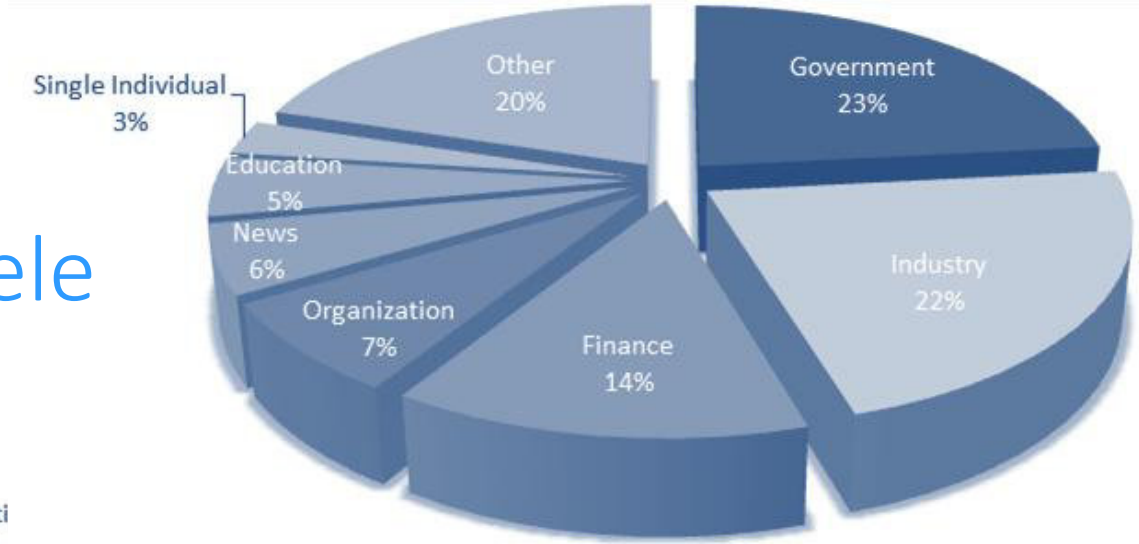
Siemens S7300



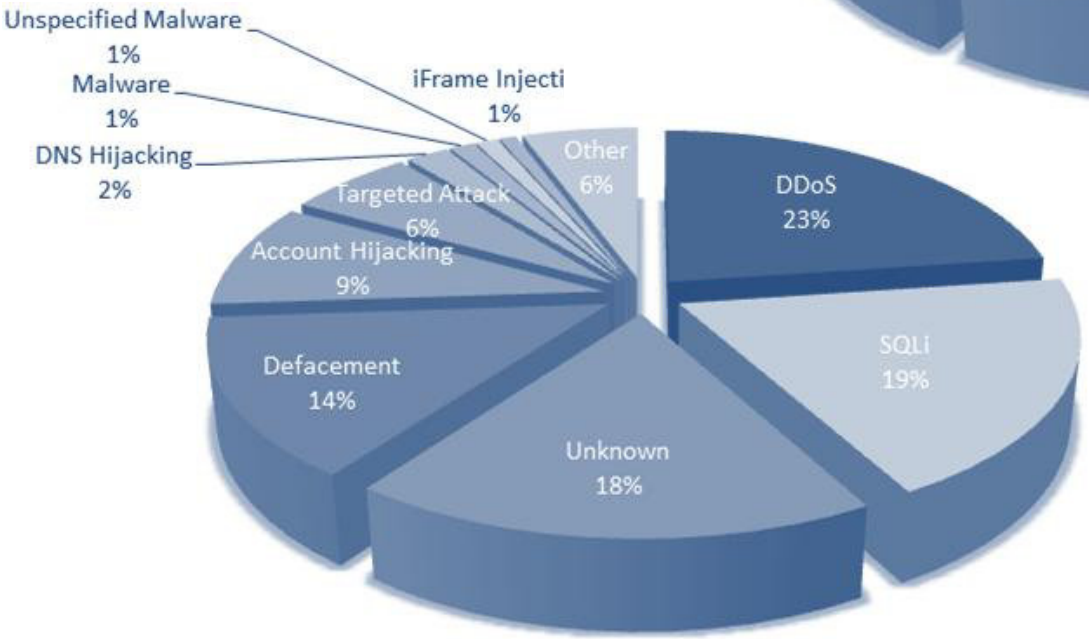
Quelle: Wikipedia

Bedrohungslage 2013

Ziele



Techniken



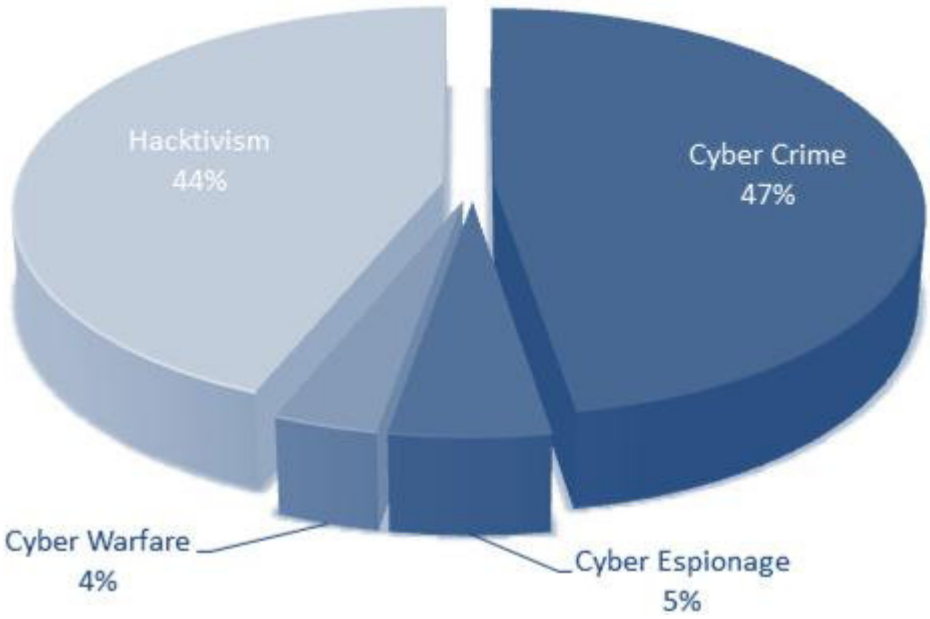
Quelle: hackmageddon.com

Motivation

Analyse der Motivation von Cyber-Angriffen

Die wichtigsten Motivationen:

- Soziale Orientierung
- Technische Ambitionen
- Politische Orientierung
- Finanzieller Profit
- Regierungsauftrag



Achtung

Die Aussagekraft der verfügbaren Statistiken ist begrenzt!

Quelle: hackmageddon.com

Bedrohungslage

Analyseergebnisse Cyber-Crime

- 5.428 befragte Unternehmen weltweit (Deutschland 1.166)
- jedes zweite deutsche Unternehmen ist betroffen
- häufigste Arten: Veruntreuung, Betrug, Industriespionage
- ermittelter Schaden in Deutschland: 4,3 Mrd. €
- Durchschnittlicher Schaden pro Vorfall 1,6 Mio. €
- Die Hälfte der wirtschaftlichen Delikte ist Mitarbeitern zuzuordnen
- Täter: 20% Senior Management, 25% Mittleres Management

PWC

- 64% der Unternehmen waren in den vergangenen 3 Jahren selbst Opfer eines Angriffs
- Schadenshöhe bis zu 85 Mio. €
- Viele Vorfälle wären mit einer höheren Sensibilität des Managements vermeidbar gewesen
- Täter: zu 84% Mitarbeiter

KPMG

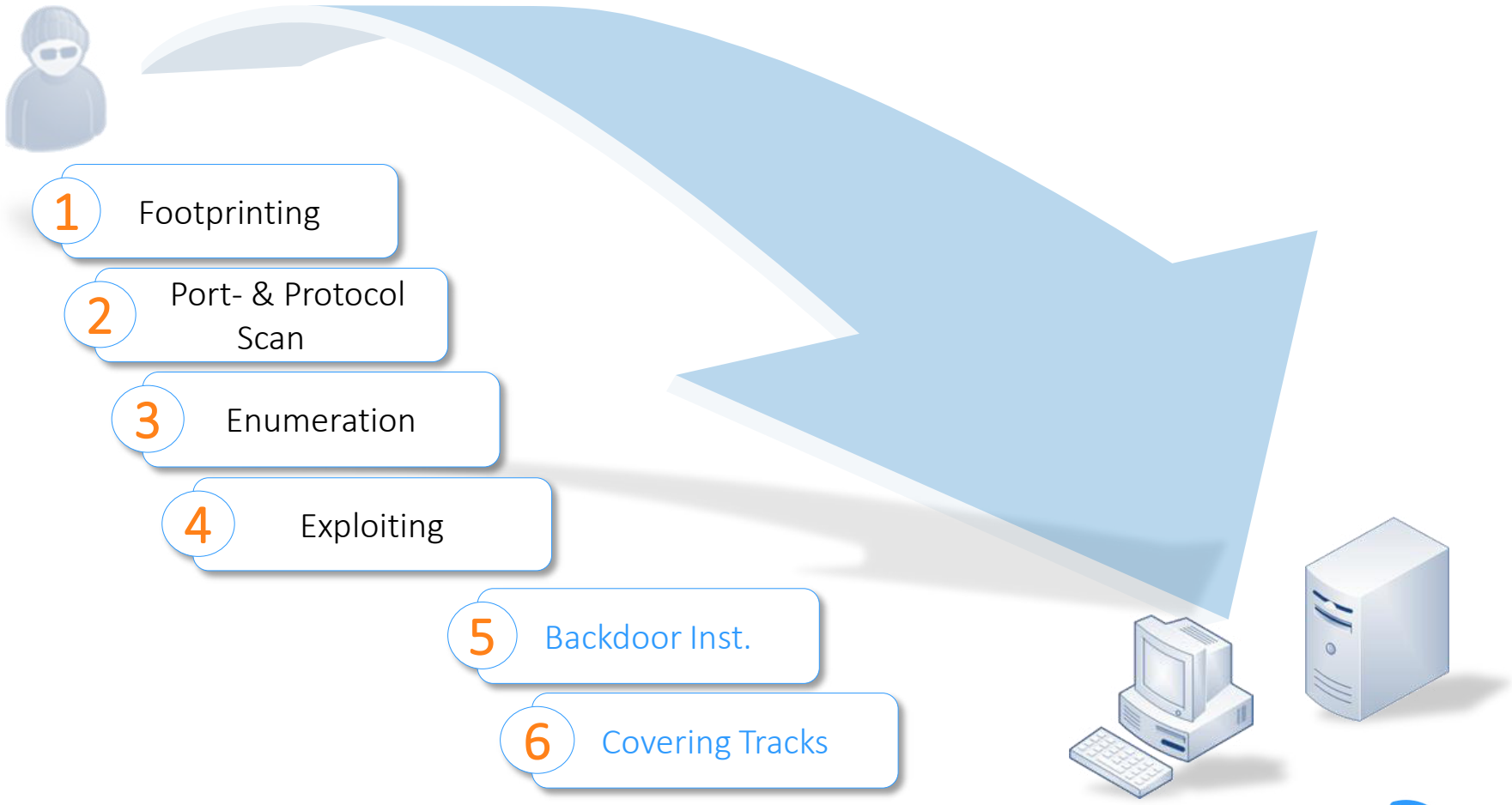
"Ist nur für andere ein Problem …"

- Schadenshöhe: 8,3 Mrd. €
- "Der Feind im eigenen Lager "
- Top Managers als Insider

Ernst & Young

Systemangriffe

Typische Phasen eines Cyber-Angriffs



sure it .de
Stefan Rieber consulting

Angriffsziele

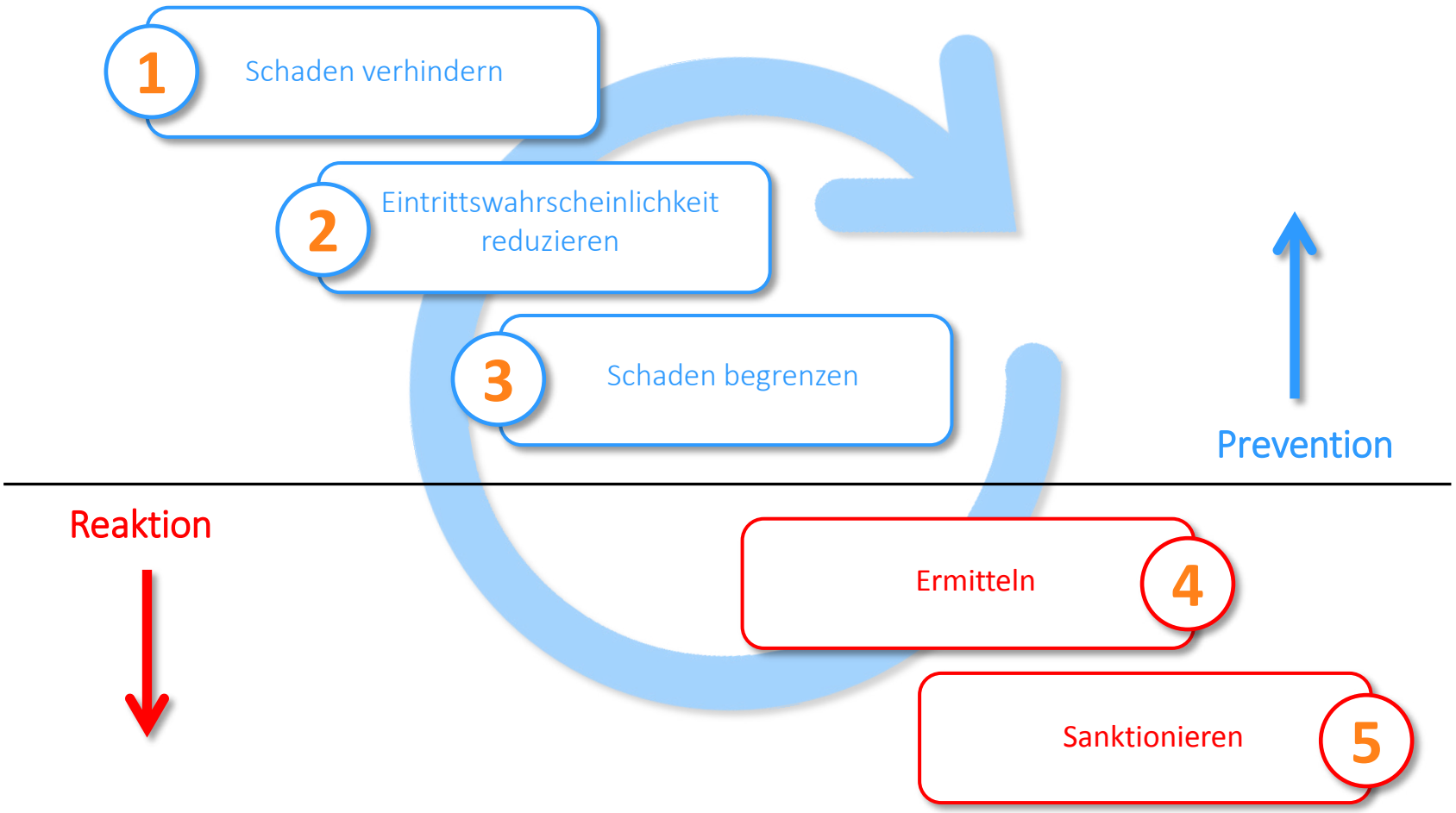
Wertvolle Daten / Ziele für Industriespionage

- Forschungsergebnisse
- Entwicklungs-Strategie
- Produkt Informationen
- Produktionstechnologie/ -prozesse (Know-how)
- Designstudien/ Produktideen
- Ergebnisse von Qualitätsaudits
- Ersatzteillisten
- Geschäftsstrategien
- Expansions- und Investitionsplanungen
- Kooperationen/ Partnerschaften/ Fusionspläne
- Kostenaufstellungen und Budgetplanungen
- Marketing-Informationen und Wettbewerbsstrategie
- Kundendaten
- Preisberechnungen/ -informationen und Controlling-Informationen

Quelle: Verfassungsschutz

Informationssicherheit

Ebenen der Gefahrenabwehr



sure it .de
Stefan Rieber consulting

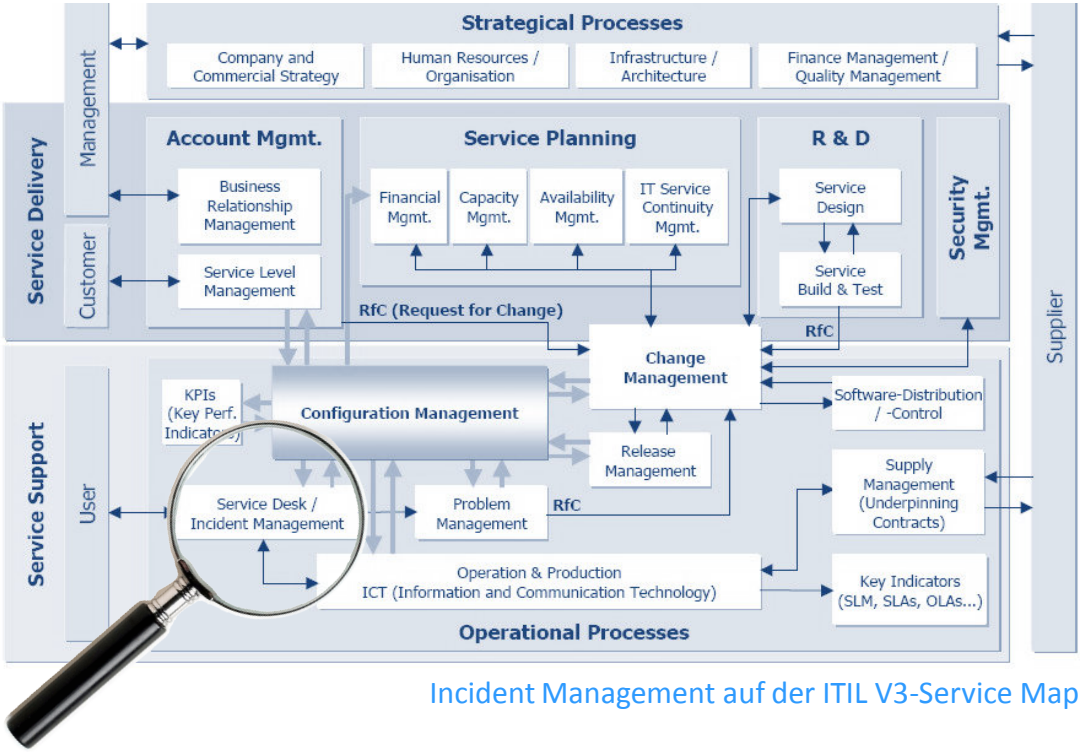
Identifikation von Cyber-Angriffen

Security Incident vs. (operational) Incident

Von entscheidender Bedeutung ist die Fähigkeit, zwischen einem Sicherheitsproblem und einer Betriebsstörung zu unterscheiden.

Für die Unterscheidung müssen geeignete Kriterien gefunden werden!

- Gefahr in Verzug
- Vorsatz
- betrügerische Absicht
- …



Incident Management auf der ITIL V3-Service Map

sure it .de
Stefan Rieber consulting

Identifikation von Cyber-Angriffen

Merkmale/ Anzeichen eines Angriffs

Netzwerk	- ungewöhnlich hohes Datenvolumen, Firewall droppings, …
IDS	- Alarm, Policy dropping, auffällige Einträge in Logfiles, …
Server	- unbekannte Prozesse, User (neue Accounts) oder (neue) Dateien, Veränderungen von Dateigrößen oder Metadaten, fehlende oder veränderte (Log) Dateien, Schreibversuche auf Systemdateien, ungewöhnliche Systemauslastung, beendete Prozesse/ Services, Denial of Service, unerklärliche Systemabstürze, ungewöhnliche Logins (Zeiten oder abgewiesene Versuche), sichtbare Veränderungen (z.B. Defacement), …
Extern	- Warnungen von Dienstleistern (z.B. CERT), Beschwerden über Malware von Kunden oder Partnern, Information von Behörden, Presseinformationen, Informationen aus Intrusion Mapping Systemen, …

Gestohlene Güter vs. kopierte Daten

Computer-Straftaten werden häufig weder bemerkt noch reportet …

… weil sie nicht offensichtlich sind!

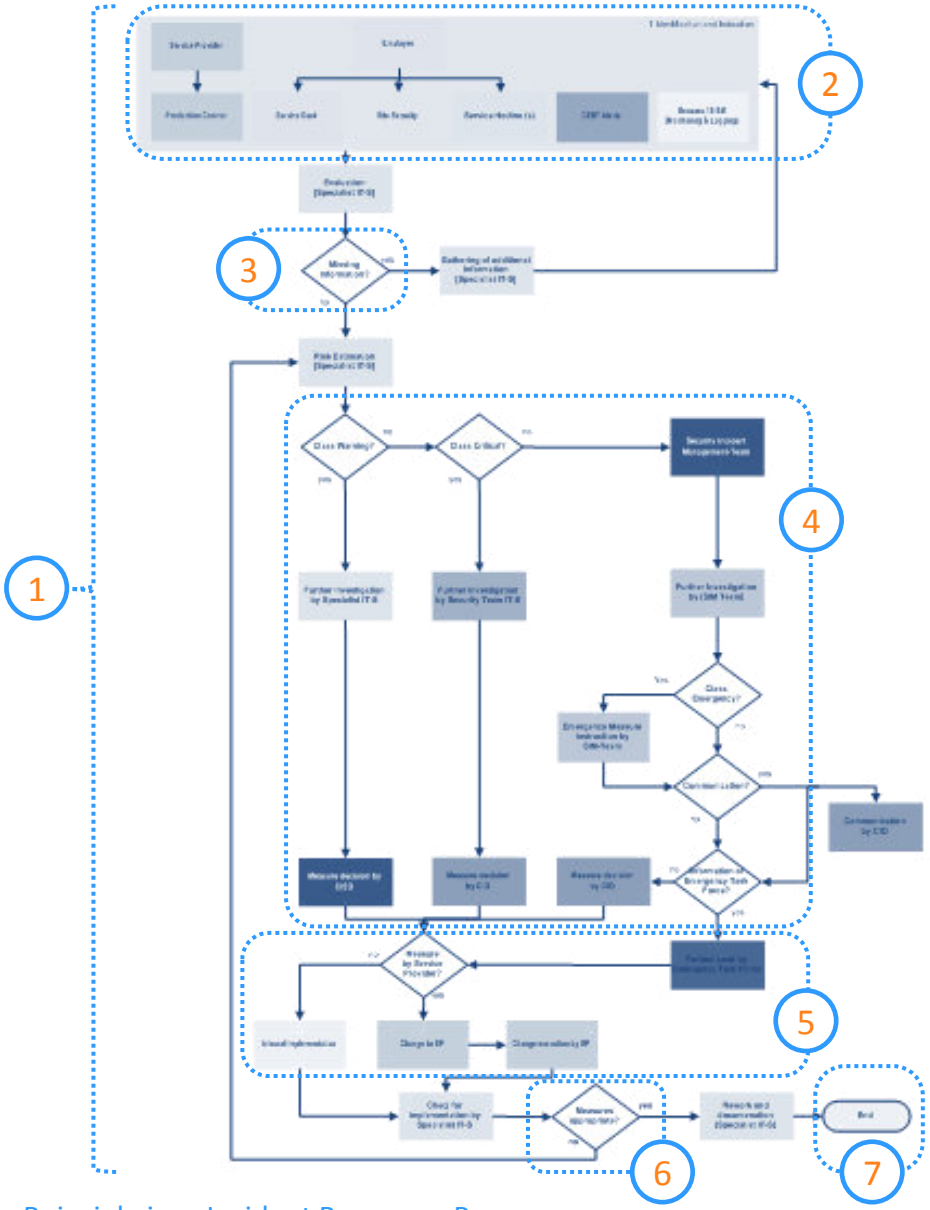
Incident Response

Organisieren Sie den Ernstfall

„Information Security Incident Management“

Kernelemente

1. Vorbereitung/ Test
2. Anzeige eines Vorfalls
3. Klassifikation
4. Initialisierung der Response (Datensicherung, Ermittlung, Maßnahmenentscheidung, Koordination, Reporting, Kommunikation, ...)
5. Rückkehr zum Normalbetrieb
6. Beobachtung
7. Lessons learned



Beispiel eines Incident Response-Prozesses

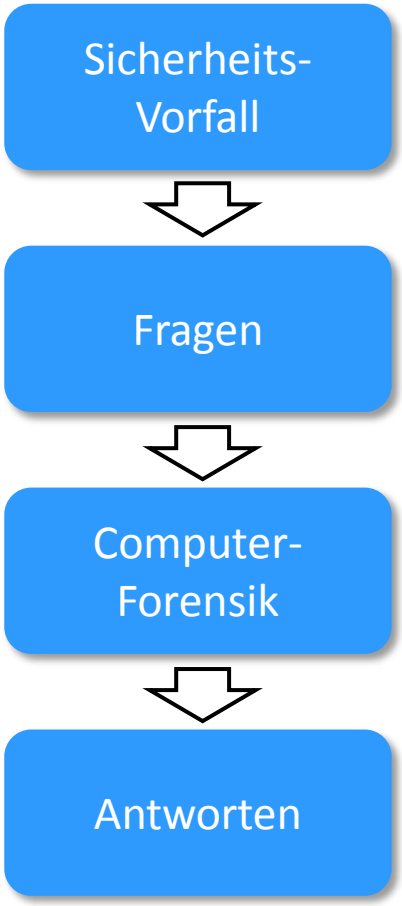
Incident Response

Typische Fehler

1. Response-Plan nicht vorhanden/ bekannt
2. Vorfall wird unterschätzt
3. Keine zeitnahe Meldung
4. Unzureichende Information der Entscheidungsträger
5. Unvollständige Dokumentation
6. Unzureichender Schutz der Beweise

Computer-Forensik

Suche nach Antworten



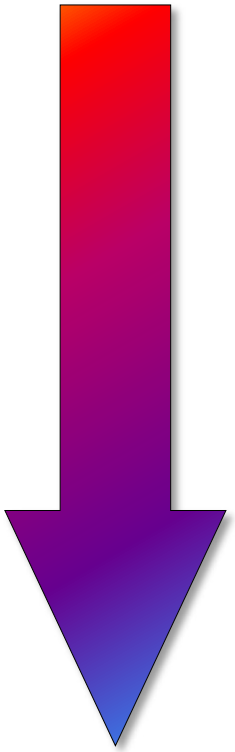
- Fragen nach einem Sicherheitsvorfall sind Fragen nach Manipulation
- Die Antworten werden für einen sicheren Weiterbetrieb benötigt
- Die wichtigsten Spuren sind i.d.R. flüchtig oder fragil
  - Flüchtig - RAM: Netzwerkverbindungen, Prozesse, Speicher, …
  - Fragil - Festplatte: gelöschte Dateien, Auslagerungsdateien, Eventlogs, …
- Am betroffenen Gerät sind Spuren in Gefahr
  - Flüchtige Spuren werden durch Ausschalten vernichtet
  - Fragile Spuren werden durch Anlassen vernichtet
  - Beide Arten von Spuren werden durch Aktivitäten am Gerät vernichtet

Quelle: HiSolution AG, 2. BSI GS-Tag

Computer-Forensik

First und Life Response - Reihenfolge der Datensicherung

Die Halbwertzeit der Informationen bestimmt die Sicherungsreihenfolge

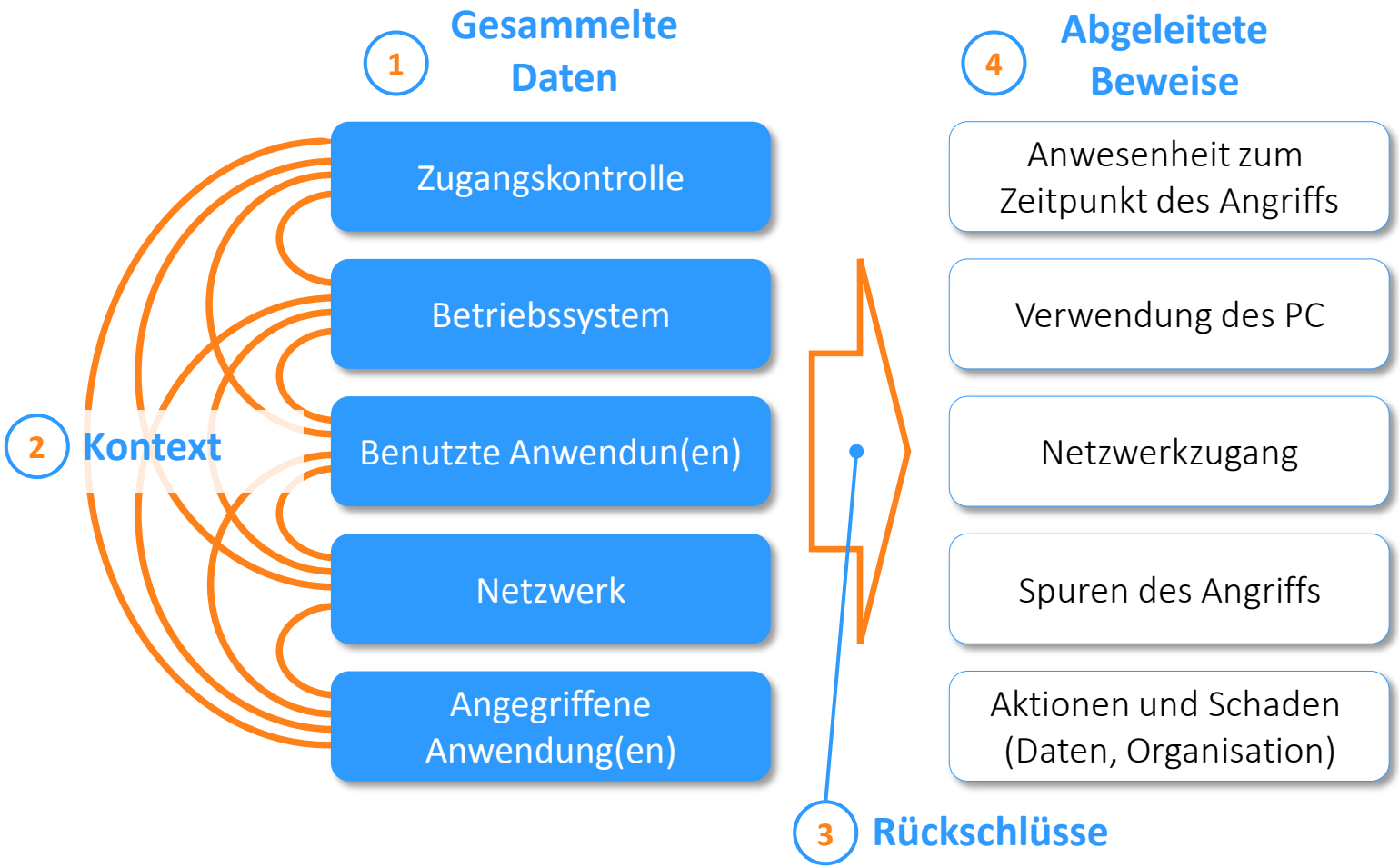


- Routingtabellen, ARP-Cache, Prozessliste, angemeldete User, Netzstatus, Kerneldaten, Hauptspeicherinhalt, Prozesse, …
- Temporäre Dateisysteme, SWAP-Bereiche, lokale Logdateien, …
- Inhalt der Datenträger
- Relevante Logdaten auf zentralen Log-Servern
- Physische Konfiguration und Netzwerktopologie
- Archivierte Medien
- …

Quelle: RFC 3227

Computer-Forensik

Zusammenhänge herstellen



Fazit

1. **Incident Response ist wichtig!**
2. Schnelligkeit ist oberstes Gebot (First Response)!
3. Live Response ist ohne Expertenwissen (selber) machbar!
4. Den Ernstfall vorbereiten – und üben!