IT Security

Vorlesung an der Hochschule Karlsruhe - Technik und Wirtschaft
im Sommersemester 2024

Michael Fischer und Georg Magschok

mf@wanulator.de gio@eglikoe.de

Die Vorlesung im Web:

http://pl.attitu.de/vorlesungen/netsecman/

Roter Faden

- Überblick
- Safety
- Badaboom
- Security

[root@netsec]>

Wegweiser

Überblick

Überblick:Ursachen (Wieso?)

- Unbeabsichtigte Ereignisse => Safety
  - höhere Gewalt, technische Fehler, Defekte, Bedienfehler
- Beabsichtigten Angriffe => Security
  - Aktive Angriffe (Manipulation von Daten, Störung der Übertragung oder Speicherung, Verbreitung von Malware)
  - Passive Angriffe (Abhören (Sniffing)), Analyse von Kommunikationsbeziehungen

Überblick: Ziele (Was?)

- Verfügbarkeit: IT Dienste sind für befugte Nutzer zugänglich und funktionsfähig
- Integrität: Daten dürfen nur von berechtigten Nutzern verändert werden
- Vertraulichkeit: Daten dürfen nur von Berechtigten Nutzern interpretiert werden
- (Zurechenbarkeit:) Man kann jederzeit feststellen, wer welchen Prozess ausgelöst hat
- (Rechtsverbindlichkeit:) Man kann jederzeit sicherstellen, dass Daten oder Vorgänge dritten gegenüber rechtskräftig nachgewiesen werden können.

Überblick: Methoden (Wie?)

	Redundanz (HA)	„Firewall“++	Krypto-graphie	Policies (Faktor Mensch)
Verfügbarkeit	X	X		X
Integrität		X	X	X
Vertraulichkeit		X	X	X
Zurechenbarkeit			X	X
Rechtsverbindlichkeit*			X	

* (Besondere Mechanismen notwendig)

Überblick: Rechtliche Grundlagen IT-Sicherheit

- Sorgfaltspflicht bei Unternehmen (Nachweispflicht insbesondere bei AGs) (HGB/AktG)
  - Risikomanagement mit Ziel Geschäftskontinuität
  - Aufbewahrungspflicht für steuerlich- /bilanzrelevante Daten
- Datenschutz (BDSG / DSGVO) betrifft Erhebung und Verarbeitung personenbezogener Daten.
  - Bestellung eines Datenschutzbeauftragten
  - Nachweispflicht des ordentlichen Betriebs/Protokollierung/Löschung
- Schutz des Fernmeldegeheimnisses (TKG)
  - Nicht bei rein Dienstlicher Nutzung
  - Maßnahmen müssen AN bekannt sein, keine vollständige Überwachung erlaubt.
  - Viren Mails dürfen gefiltert werden (Abwägung der Schutzinteressen)
- Branchenspezifisch
  - Z.B Banken, Pharmaunternehmen

Überblick: Rechtliche Grundlagen IT-Sicherheit II

- Haftungs- Ordnungs- und Strafrecht
  - Vorsatz / Fahrlässigkeit bei Nichteinhaltung rechtlicher Verpflichtungen
  - Verletzung des Post/Fernmeldegeheimnisses (!!! Unterdrücken/Filtern von SPAM)
  - Computerbetrug
  - Urkundenfälschung
  - Datenveränderung
  - Computersabotage
  - Störung von Telekommunikationsanlagen
  - §202c „Vorbereiten des Ausspähens und Abfangen von Daten“
  - Uvm.

Überblick: IT Sicherheit Standards

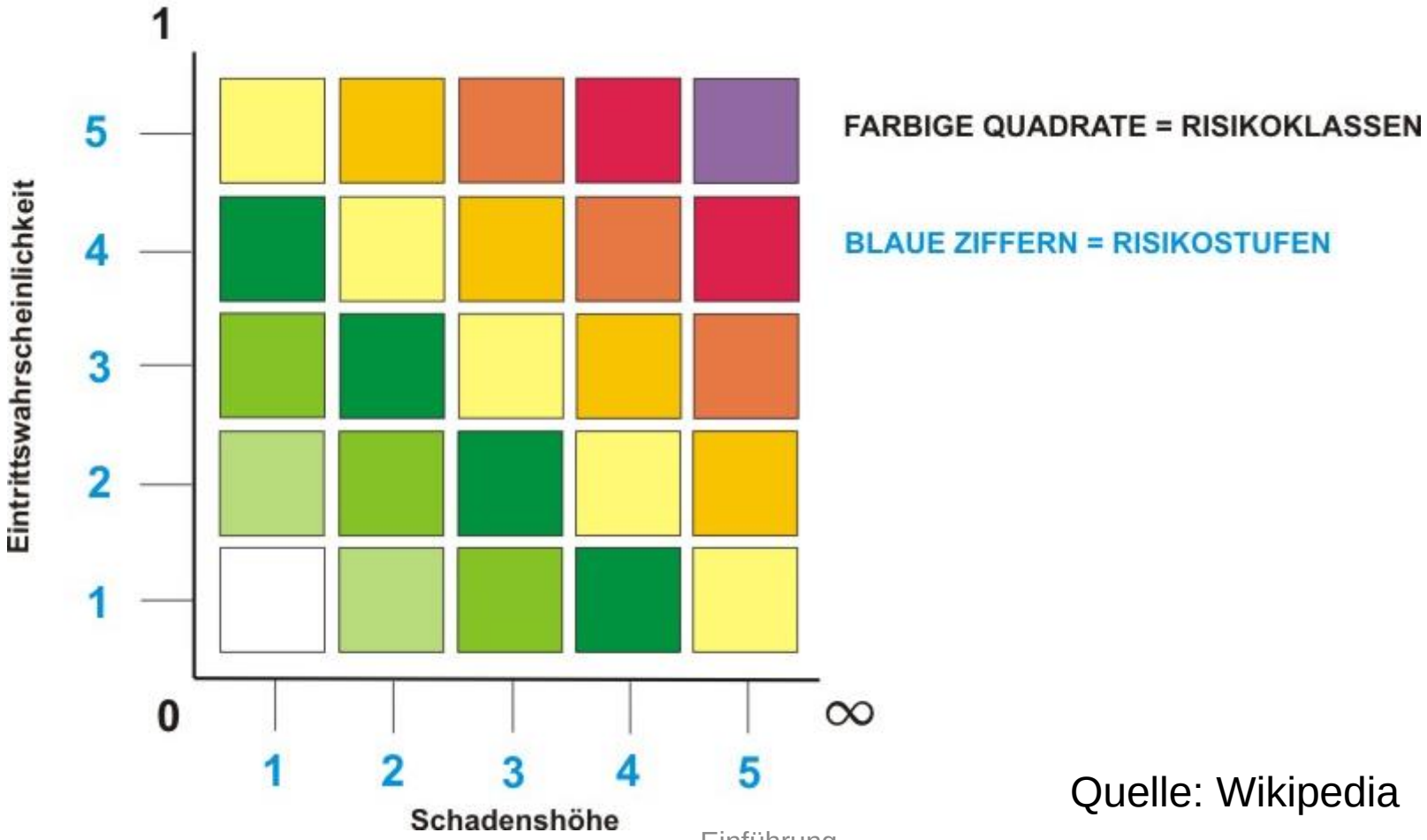
- Orange Book (Trusted Computer Evaluation Criteria TCSEC) (DoD) Erster Standard von 1983
- Common Criteria (ISO 15408)
  - aus Internationalen Erfahrungen
  - Zertifizierung verschiedener Evaluierungsstufen (EAL 0 – EAL7)
- IT Grundschutz Katalog (BSI)
  - IT Grundschutzhandbuch (GSHB)
  - „Einfach“ zu verwenden
  - Zertifizierbar (via Selbsterklärung und Audits)
- ISO 27001/2

[root@netsec]>

Exkurs: Risiko

- Je nach Fachdisziplin unterschiedlich definiert
- ISO: Eintrittswahrscheinlichkeit x Schadenshöhe
- Häufig als finanzielle Größe

Risikomatrix nach Nohl



Quelle: Wikipedia

Anwendung

- Übliche Vorgehensmodell z.B. bei ISO 27001
  - Bedrohungsanalyse
  - Bewertung => Risikowert bestimmen
  - Lösungen finden:
    - Maßnahmen
    - Übertragung (Versicherung)
    - Vermeidung
    - Akzeptanz
- Risiko Management im Unternehmen => Compliance
- Versicherungen
- Projektmanagement
- …

[root@netsec]>

Wegweiser

Soviel zum allgemeinen Überblick

Nun kommt:

Safety

Ausfallsicherheit/Redundanz: Definition

- 1. Überreichlichkeit, Überfluß, Üppigkeit. 2. (Sprachw.) a) ... mehrfache Kennzeichung derselben Information ... b) stilistisch bedingte Überladung ... Pleonasmus, Tautologie 3. ...Informationstheorie, Nachrichtentechnik ... weglaßbare Elemente einer Nachricht..." (Duden, Fremdwörterbuch)

- Bezeichnung für die Anteile einer Nachricht, die keine Information vermitteln, also überflüssig sind. (Duden Informatik)
  - Ziel: Verständlichkeit bei ungenauer Übertragung

- Bezeichnung für den Aufwand, der für den Normalbetrieb eines Systems nicht benötigt wird, der aber beim Ausfall von Komponenten oder des ges. Systems automat. die Funktionsfähigkeit sicherstellt (z.B.Notstromaggregat, doppelt ausgelegte Hydraulik im Flugzeug). (Universal Lexikon)
  - Ziel: Verfügbarkeit, Ausfallsicherheit

Redundanz: Motivation

- Erhöhung der **Verfügbarkeit**: Maximierung der Zeit, die ein System funktionsfähig ist, über einen Betrachtungszeitraum.
- Erhöhung der **Zuverlässigkeit**: Maximierung des Zeitintervalls in welchem ein System fehlerfrei arbeitet.

- Veeam Availability Report (n ~1000):
  - Server mit mindestens 1 Ausfall im Jahr: 27%
  - Durchschnittlicher Schaden bei Business kritischen Anwendungen: $108.000/h
  - Durchschnittliche Länge eines ungeplanten Ausfalls: 85 Minuten

Ursachen für Systemausfälle

36%: Software
34%: Bedienung / Administration
25%: Hardware Fehler
3% : Stromausfall
2% : Elementarschäden: Feuer / Wasser…

Redundanz: Beispiele

- Flugsteuersystem: Ausfallswahrscheinlichkeit einer sicherheitskritischen Komponente: 10^{-9} D.h. Ein Ausfall bei einer Milliarde Flugstunden.
  - erreicht durch: diversitäre Techniken im Aufbau, Hard- und Softwareentwurf
  - z.B. 3-fach Abstimmung beim Slat-Flap Control System im Airbus
- Marketing „five-nines“
- Internet Shop
- Krankenhaus OP-Räume oder lebenserhaltende Maßnahmen

Redundante Auslegung von Systemen:

- **Symmetrische Redundanz (n+m):**
  - Für N Komponenten existieren m Ersatzkomponenten
  - Spezialfall 1:1 wird auch Doppelung genannt. Bei dem Ausfall von >1 Komponenten, steht das gesamte System nicht mehr zur Verfügung.
- **Asymmetrische Redundanz:**
  - Die Komponenten sind nicht identisch implementiert.

- **Statische Redundanz (aktive, funktionsbeteiligt, Fault Tolerance):**
  - Mehrere redundante Systeme führen zeitgleich die selbe Funktion aus.
  - Z.B.: N-fach modulare Redundanz (NMR) – Die Ergebnisse von N Komponenten werden einem „Voter“ vorgelegt, der eine Mehrheitsentscheidung trifft.
  - Üblicherweise wird N ungerade gewählt.
  - Bei 2n+1 eingesetzten Komponenten können n Ausfälle toleriert werden
  - Keine Unterbrechung der Verfügbarkeit bei Ausfall.
  - Erhöhung der Zuverlässigkeit durch asymmetrische Redundanz
  - Problem: „Voter“
  - Nachteil: hoher Implementierungsaufwand

Redundante Auslegung von Systemen:

- **Dynamische Redundanz (Standby, Hot Sparing):**
  - Nur eine Komponente führt eine Funktion aus (d.h ist aktiv oder „hot“)
  - Wenn ein Fehler festgestellt wird, übernimmt eine Reservekomponente (standby) die Funktion.
  - Bei n redundanten Komponenten können n-1 Ausfälle toleriert werden.
  - Spezialfall: Loadbalancing – die redundanten Komponenten führen ebenfalls Funktionen aus. Ein Ausfall macht sich durch einen Leistungsabfall des Gesamtsystems bemerkbar.
  - Problem: Fehlererkennung (aktiv, passiv), Fehlerfortpflanzung, Konvergenzzeit, Zustandssynchronisation
- **Hybridredundanz:**
  - Kombination aus statischer und dynamischer Redundanz

Definition Verfügbarkeit

- Wahrscheinlichkeit des Betrieb eines Systems (t_a Ausfallzeit, t_b Betriebszeit):

$$q = W(B) = \frac{t_b}{t_b + t_a}$$

- Wahrscheinlichkeit für den Nichtbetrieb eines Systems

$$p = W(NB) = \frac{t_a}{t_b + t_a}$$

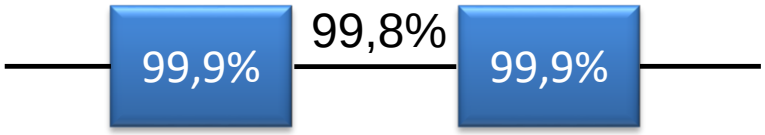
- Es gilt p+q=1
- Verfügbarkeitsstufen bezogen auf die maximale Ausfallzeit pro Jahr:

99,0%	3,7 Tage	Üblich
99,9%	8,8 Stunden	Verfügbar
99,99%	52,6 Minuten	Hochverfügbar
99,999%	5,3 Minuten	Fehlerunempf.
99,9999%	32 Sekunden	Fehlertolerant

Berechnung von Verfügbarkeit eines Systems

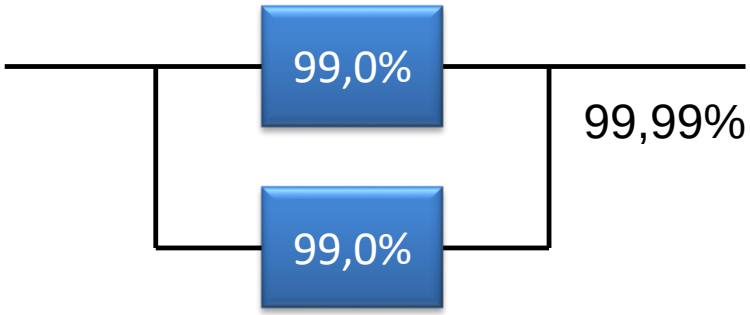
- Serienschaltung (q Betriebswahrscheinlichkeit, p Ausfallwahrscheinlichkeit):

$$q_{sys} = \prod_{i=1}^{n} q_i \qquad p_{sys} = 1 - \prod_{i=1}^{n} (1 - p_i)$$

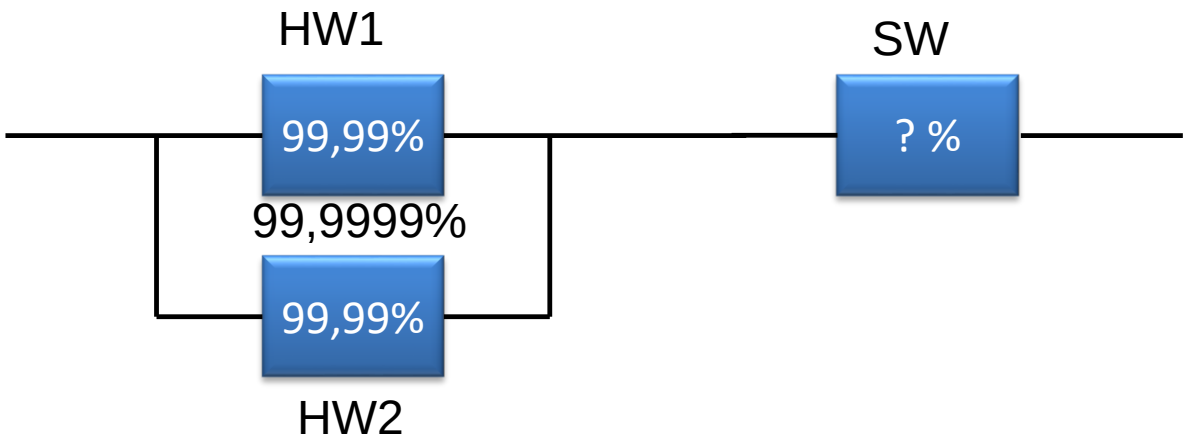


- Parallelschaltung (1:1 Redundanz):

$$q_{sys} = 1 - \prod_{i=1}^{n} (1 - q_i) \qquad p_{sys} = \prod_{i=1}^{n} p_i$$



Beispiel: HW vs. SW:



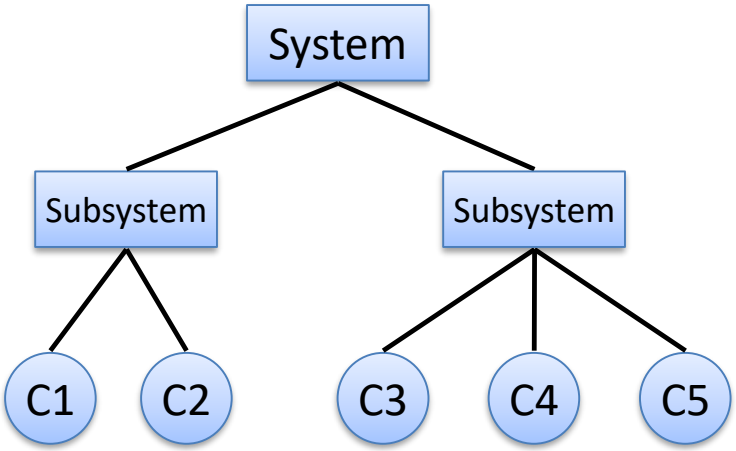
- Um eine hohe Verfügbarkeit zu erreichen müsste die SW Komponente eine utopische hohe Verfügbarkeit aufweisen. Nur asymmetrische Redundanz möglich da sonst die Wahrscheinlichkeit für das gleiche Verhalten der SW Komponente zu groß ist.

Fehler Ursachen

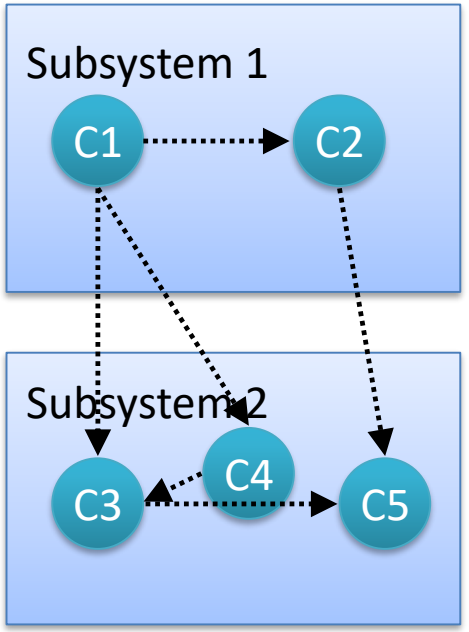
- Systemfehler
- Physikalische Fehler (äußere Einflüsse)
- Verschleiß
- Bedienungsfehler
- Wartungsfehler

System Analyse

- Hierarchisches vs. Relationales Modell:



Composed of



Uses

Ausfallsicherheit im Netzwerkbereich

- Dabei zu betrachtende Komponenten:
  - Stromversorgung
  - Hardware
  - Software
  - LAN Infrastruktur
  - WAN Infrastruktur
  - Naturkatastrophenwahrscheinlichkeit
  - Klima
  - Wasserversorgung
  - (Security)
    - Terroranschlagswahrscheinlichkeit
    - Gebäudesicherheit
- Zur Berechnung der Verfügbarkeit zu betrachten sind auch:
  - Bootzeiten
  - Konvergenzzeiten

Stromversorgung:

- Zur Statistik, in den USA:
  - 15 Durchschnittliche Anzahl der Stromausfälle pro Jahr in einem IT-Department.
  - 90% der Ausfälle < 5 Minuten
  - 99% der Ausfälle < 60 Minuten
  - Verfügbarkeit: 99,98%
- Redundanz durch:
  - Unterbrechungsfreie Stromversorgung (USV) (kurze Zeiträume)
  - Generatoren (längere Zeiträume)
  - Üblicher Fehler: USV aber keine 2 Netzteile (siehe HW)

Hardware:

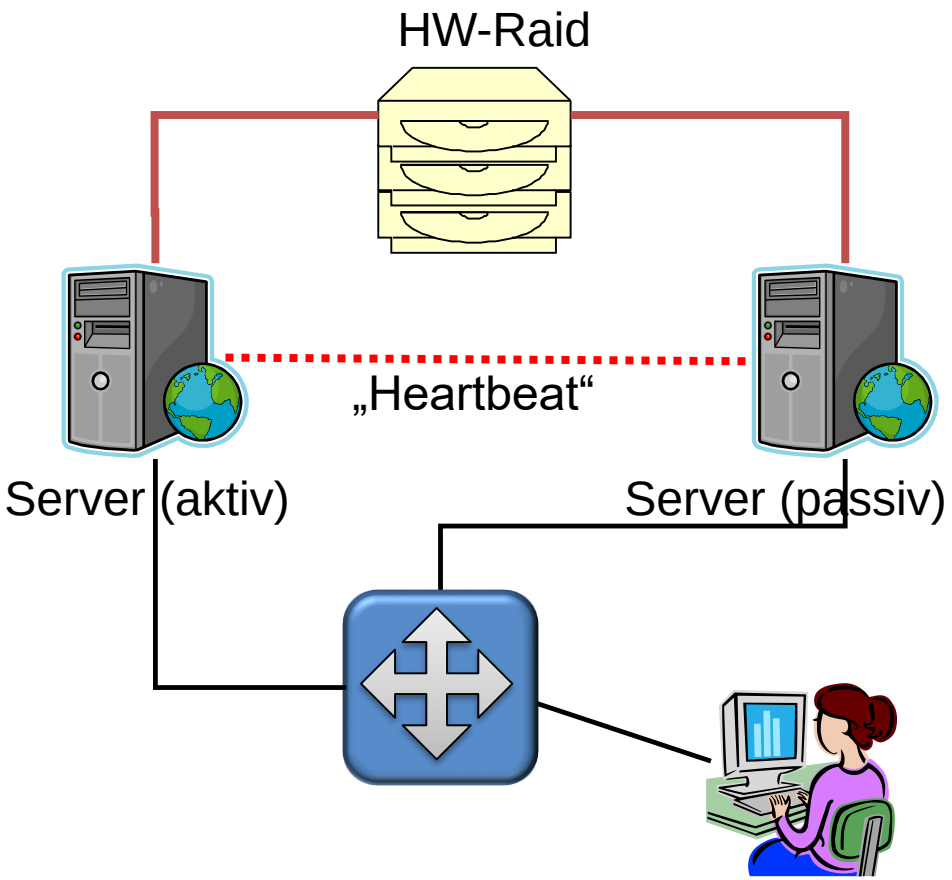
- Verschiedene Ebenen von Rechenzentrum bis „Chip“
- Berechnung der Verfügbarkeit ist schwierig wegen der Komplexität und da nicht alle Bauteilehersteller Angaben machen.
- Statistisch verlässliche Angaben sind erst nach 2 Jahren nach der Markteinführung zu erwarten.
- Redundanz durch:
  - Parallelisierung im HW betrieb
  - Problem: Fehlererkennung, eventuelle Umschaltzeiten, Aufwand

Software:

- Berechnung der Verfügbarkeit ebenfalls schwierig
  - Abschätzung durch Analyse der Qualitätsstandards des Herstellers, Lines of Code, Statistische Information
- Redundanz durch:
  - Siehe HW
- Verbesserung der Verfügbarkeit auch durch:
  - Schnellere Bootzeiten
  - SW/HW Watchdogs
  - Methodik (Einsatz sicherer Betriebsysteme, Sprachen, SW-Entwicklungs Methoden)

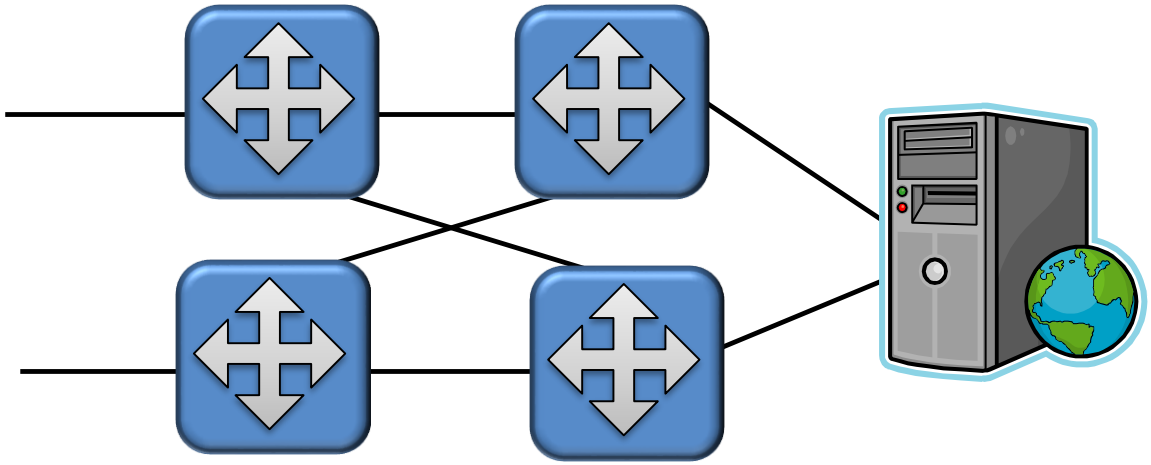
HW/SW Redundanz Beispiel::

- Zugriff auf gemeinsamen Datenbestand
- Übernahme der „Services“ durch;
  - MAC Address takeover
  - IP Address takeover
  - DNS reconfiguration
  - Anwendungsumschaltung



LAN/WAN Infrastruktur:

- Redundanz durch:
  - Mehrfachauslegung von Komponenten
  - Intelligente Verkabelung
  - Anschlüsse an mehrere ISPs
  - Wahl geeigneter Protokolle



[root@netsec]>

Wegweiser

Das war Safety

Der Rest der Vorlesung handelt von

Security

Badaboom

- http://www.caida.org/research/security/code-red/newframes-small-log.gif
- Maps
  - http://www.digitalattackmap.com/
  - http://threatmap.fortiguard.com/
  - https://threatmap.bitdefender.com/
- https://www.ibm.com/reports/threat-intelligence
- https://nvd.nist.gov/general/visualizations/vulnerability-visualizations/cvss-severity-distribution-over-time
- https://www.ibm.com/reports/data-breach
- https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/istr-24-cyber-security-threat-landscape
- https://www.exploit-db.com/exploit-database-statistics/