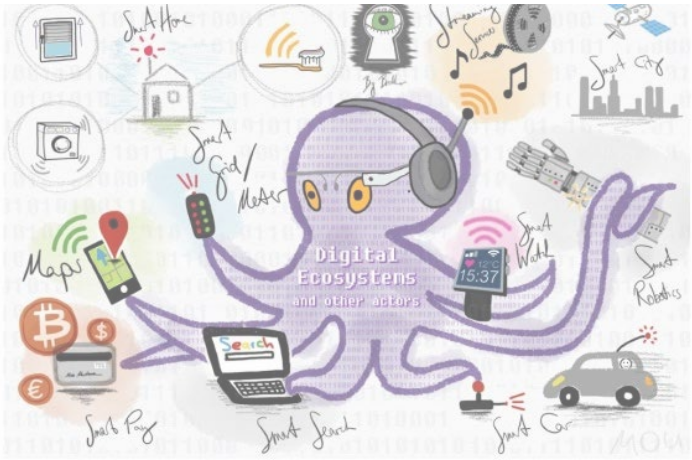
Prof. Dr.-Ing. Jochen H. Schiller
Arbeitsgruppe Technische Informatik
Fachbereich Mathematik und Informatik

Freie Universität Berlin



Grafik: Oliver Ullmann. Deutsche Bank Research.
Quelle: Dapp, T. (2014). Big Data – die ungezähmte Macht. Deutsche Bank Research. Frankfurt am Main.

Sicherheit in einer IP-basierten Welt

© REUTERS

... und es ist doch „Neuland“!

Alles – sofort – immer – überall – jederzeit – 24/7/365

vs.

Realität – Kostendruck – Komplexität – OK – Altlasten

Jochen H. Schiller

Univ.-Prof. Dr.-Ing.

- Seit 2001 Professur für Technische Informatik an der Freien Universität Berlin
- Mitglied des Zukunftsforums Öffentliche Sicherheit e.V.
- Gründung des Forschungsforums Öffentliche Sicherheit
- Leiter des Innovationszentrums Öffentliche Sicherheit bei Fraunhofer FOKUS
- CIO der FU Berlin
- Schwerpunkte im Bereich Mobilkommunikation, Öffentliche Sicherheit, eingebettete Systeme, robuste Kommunikationssysteme, Vernetzte Sicherheit

Innovationszentrum Öffentliche Sicherheit

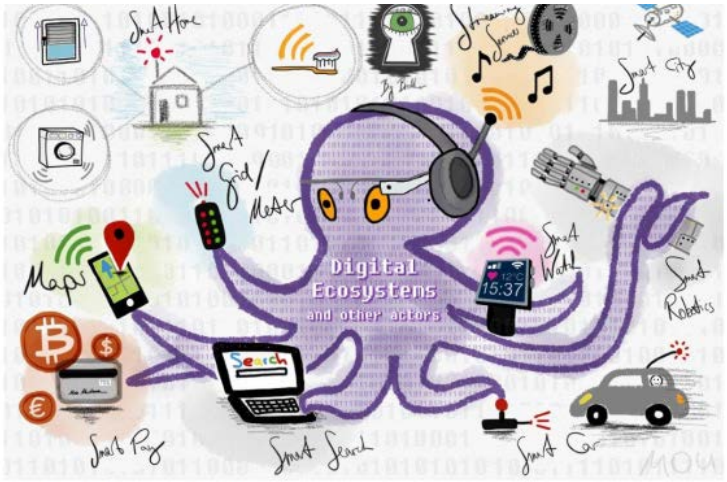
Fraunhofer FOKUS

Forschungsforum Öffentliche Sicherheit

Kein (vertieftes) Thema

Angriffswerkzeuge

- Turbine (Angriffe auf Rechner), Hammerchant/ -stein (VoIP, Skype), Quantumsky/-copper (Dateien blockieren/verfälschen), Unitedrake (Übernahme Computer)...
- Siehe z.B. www.heise.de/thema/NSA



Grafik: Oliver Ullmann. Deutsche Bank Research.
Quelle: Dapp, T. (2014). Big Data – die ungezähmte Macht. Deutsche Bank Research. Frankfurt am Main.

Schutz der Privatsphäre

- Chancen, Risiken, ökonomischer Wert, Vertrauensverlust...
- Siehe z.B. Big Data – die ungezähmte Macht, Deutsche Bank Research, www.dbresearch.de

Konkrete Sicherheitsverfahren/-protokolle/-systeme

- Siehe Vorlesungen

Juristische, politische, wirtschaftliche Aspekte

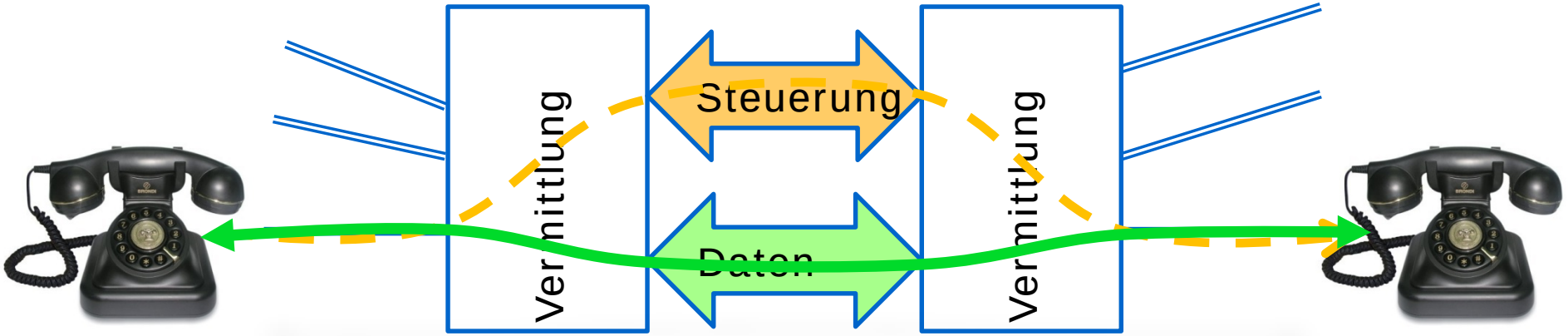
- z.B. „lawful interception“, unterschiedliche Gesetzgebung etc.

Etwas Historie ist wichtig für das Verständnis

Historie der Kommunikationsnetze 1

Klassisches Telefonnetz

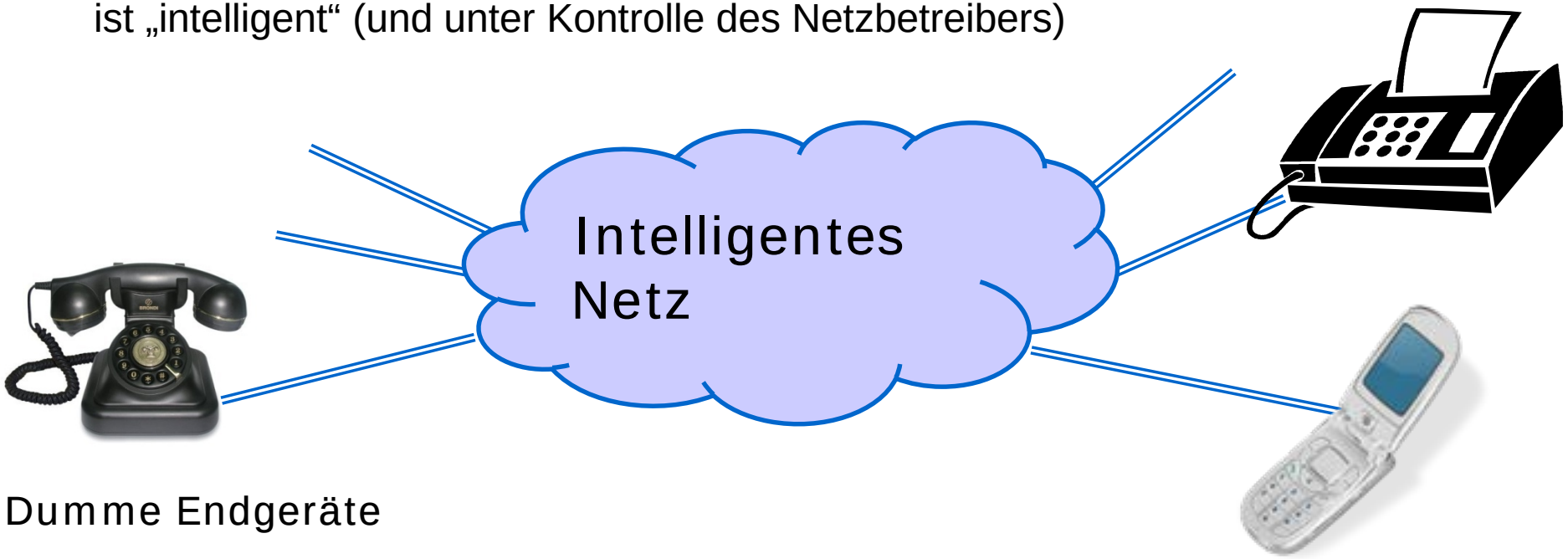
- Hoheitlich betrieben, meist Monopol
- Nur Sprache, zunächst analog, dann digital (ISDN)
- Strikte Trennung von **Steuerung** des Netzes und Übertragung der **Nutzdaten**
- Energieversorgung über Telefonleitung („Amtsbatterie“)



Historie der Kommunikationsnetze 2

Intelligentes Telefonnetz

- Grundlage für 0800/0130-Nummern, Televoting über 0137
- Viele neue Dienste wie Konferenzschaltung, Callcenter, Anrufweiterleitung, Voicebox, Bezahldienste, …
- Grundphilosophie: Endgeräte (Telefon, Handy, Fax) sind eher „dumm“, das Netz ist „intelligent“ (und unter Kontrolle des Netzbetreibers)



Historie der Kommunikationsnetze 3

Mobilfunknetz

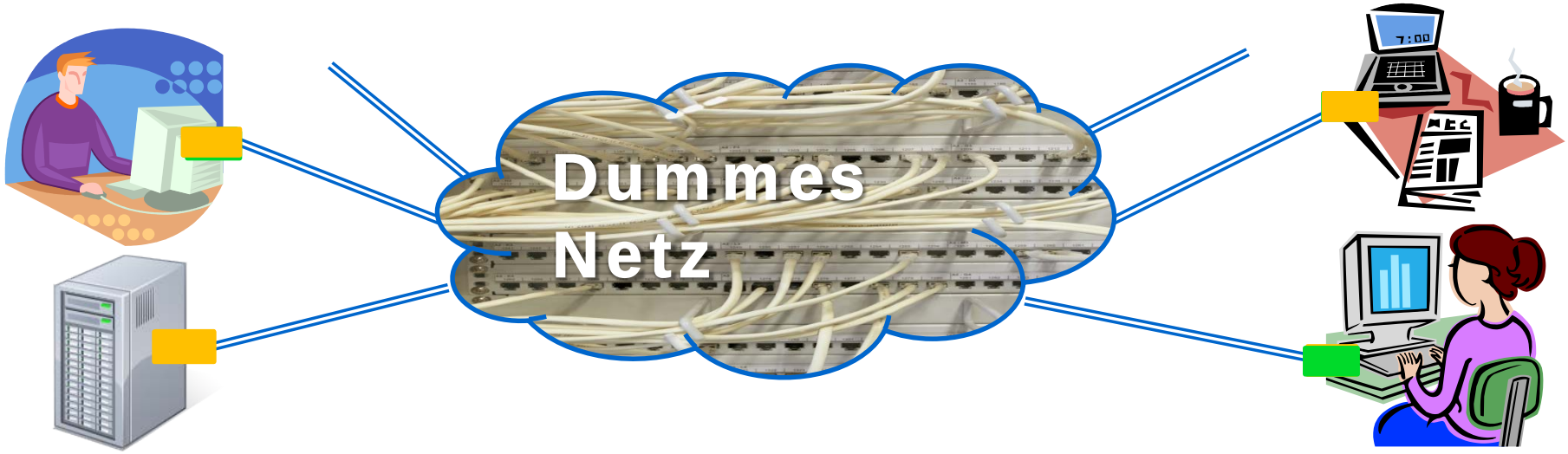
- Weiterentwicklung von digitalem Telefonnetz, Intelligentem Netz plus Funk („ISDN + Funk + Datenbanken“)
- Hochkomplexe Netzsteuerung, am Anfang „dumme“ Handys
- DAS erfolgreichste Kommunikationssystem mit 8 Milliarden Teilnehmern (Stichwort GSM, UMTS, LTE…)




Historie der Kommunikationsnetze 4

Internet

- Grundphilosophie: Endgeräte (Computer, Server) sind „intelligent“, das Netz ist eher „dumm“ (transportiert einfach Daten, egal welchen Inhalts: **Steuerung** und **Nutzdaten**!)
- Keine Monopole, Zusammenschluss von verschiedenen Netzen auf „einfacher, robuster Basis“ (Internet Protokolle)
- Anfänglich nur für „unkritische“ Aufgaben (Email, WWW…)



Intelligente Endgeräte

Intelligente Endgeräte

Kostendruck und Fortschritt

Internet kann auch Sprache übertragen (Voice over IP)

- Technisch gesehen ist Sprache auch nur eine Bitfolge = Daten
- Allerdings klassisch keine Dienstgüte verfügbar

Klassische Kommunikationsnetze sind hochkomplex

- Verhindern neue Geschäftsmodelle am Rande des Netzes
- Bieten aber qualitativ hochwertige Dienste

Deregulierung der Telekommunikationsmärkte

- Viele neue Akteure, Dienstanbieter, Betreiber etc.

Verschmelzung der Netzarten in Richtung Internet

- Eine Infrastruktur hoher Leistungsfähigkeit
- Massive Kosteneinsparungen

Kommunikationsnetze heute

Praktisch keine analogen Netze mehr, alles digital

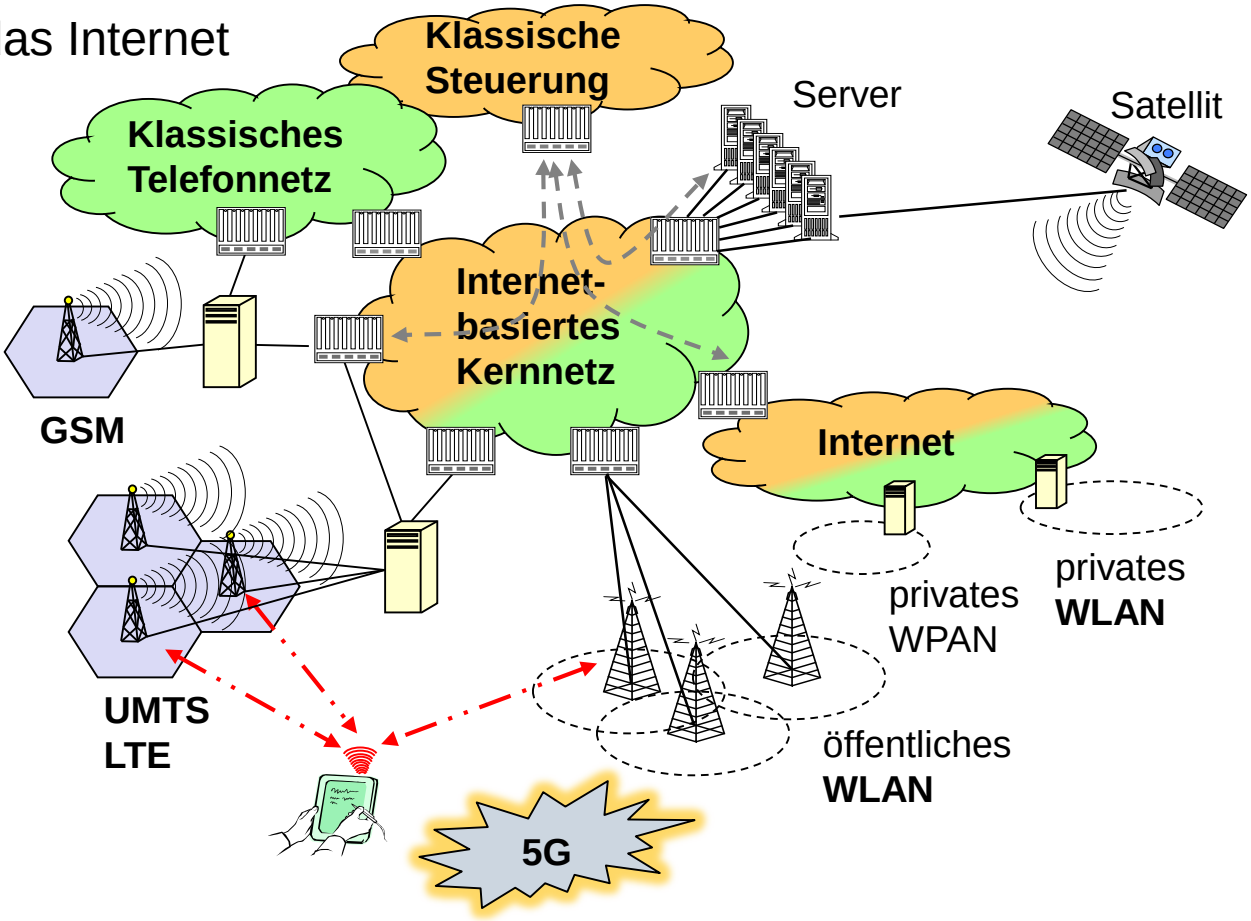
Dominiert von Mobilfunk (riesige Infrastruktur)

Immer mehr Telefonie über das Internet

- Direkt über Computer
- Indirekt über DSL-Anschluss
- Unbemerkt netzintern

Komplett von direkter Stromversorgung abhängig

„Alles hängt mit allem zusammen“



Aktueller Trend – Internet der Dinge

Quelle: The Telecare Blog, thetelecareblog.blogspot.de, 24.10.14

Auch kritische Infrastrukturen werden IP-basiert sein

Smart Grid, Smart Metering, Energiewende, dezentralisierte Energieerzeugung

- Mehr und mehr vernetzte Erzeuger und Konsumenten
- Vielzahl ferngesteuerter Kraftwerke (PV, Wind, Block…)
- Flexible Anpassung von Erzeugung und Verbrauch

E-Energy: auf dem Weg zum Internet der Energie

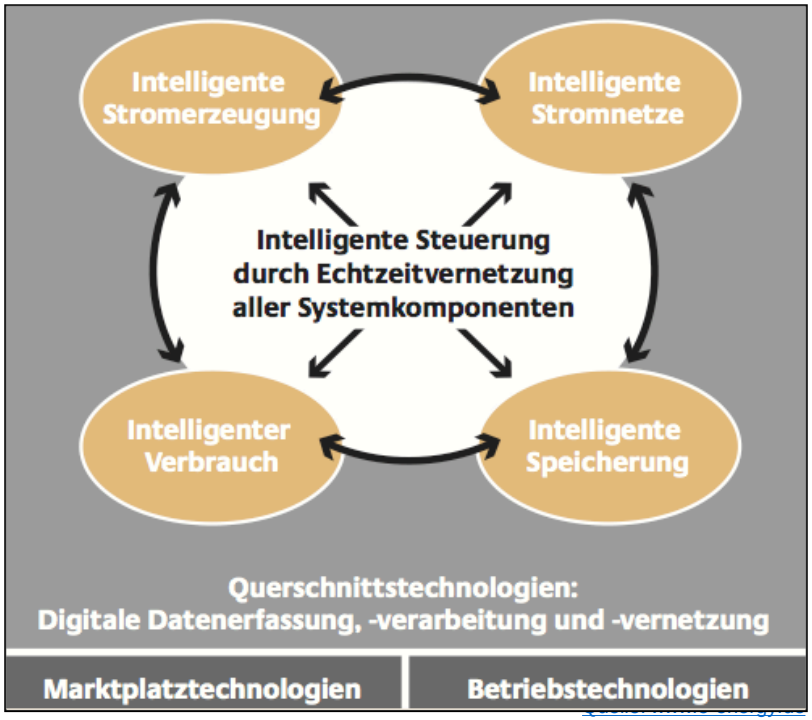
- IKT ist der Schlüssel zur Restrukturierung der Energieerzeugung

➔ Keine Energie ohne IKT und umgekehrt

Plus: keine Kreditkarten, kein Einkaufen, keine Heimpflege, keine Abwasserbehandlung, …

Was ist mit dem Internet der Dinge?

- Batteriebetrieben, ok – aber DNS, Infrastruktur, Cloud-Dienste, Konfigurationsserver, …



Einschub:
Massive Auswirkungen auf die Verfügbarkeit

Klassische (analoge) Telefone praktisch verschwunden, kaum ISDN mit Notstrom

Umstieg auf VoIP-Systeme auch zu Hause z.B. via DSL-Router

Ohne Strom kein Telefon!

- Ortsvermittlungsstellen:
  15min bis 8h Notstrom
- Fernvermittlungsstellen:
  8h bis 4 Tage Notstrom
- Münsterland, 2005:
  88% der Festnetzanschlüsse tot

Bild: dpa

Mobiltelefone

- Basisstation: 15min bis 8h Notstrom
- Privilegierter Zugriff für Behörden, Versorger, Notrufe, Netzbetreiber – falls Strom vorhanden
- Behördenfunk (TETRA): z.Zt. nur 2h Notstrom
- Münsterland 2005: 73% der Handys tot

Was passiert bei Softwarefehler

Systeme sind hochkomplex
- Nicht einfach Leitungen plus Schalter/Stecker/Relais/…

Softwarefehler passieren
- Auch bei sorgfältigster Entwicklung
- Oft aufgrund nicht überschaubarer Wechselwirkungen, vieler neuer Möglichkeiten, kurzer Innovationszyklen

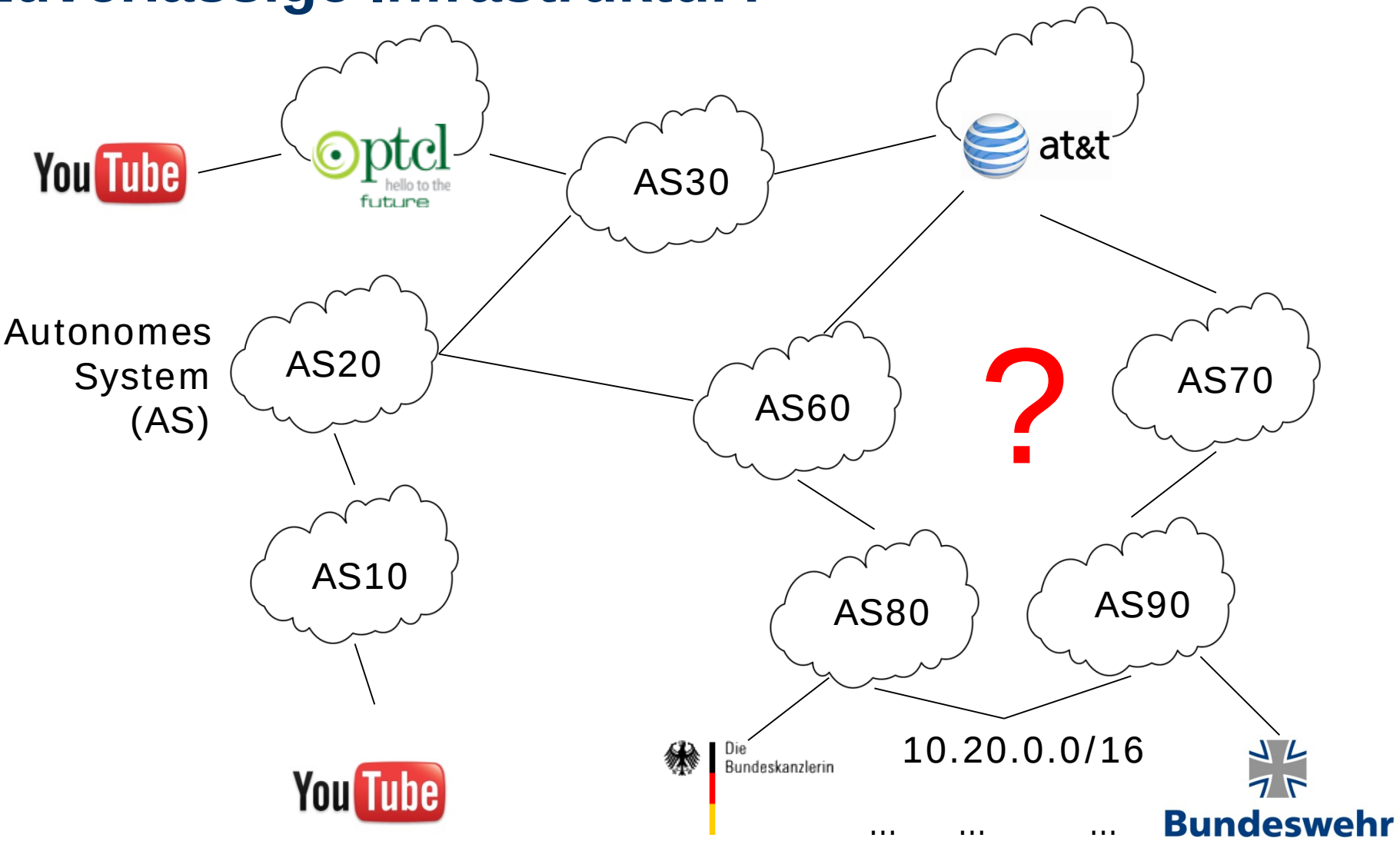
Bild: www.heise.de

Häufig nur ein bzw. wenige Hersteller
- Fehler wirken sich schnell auf alle Systeme aus

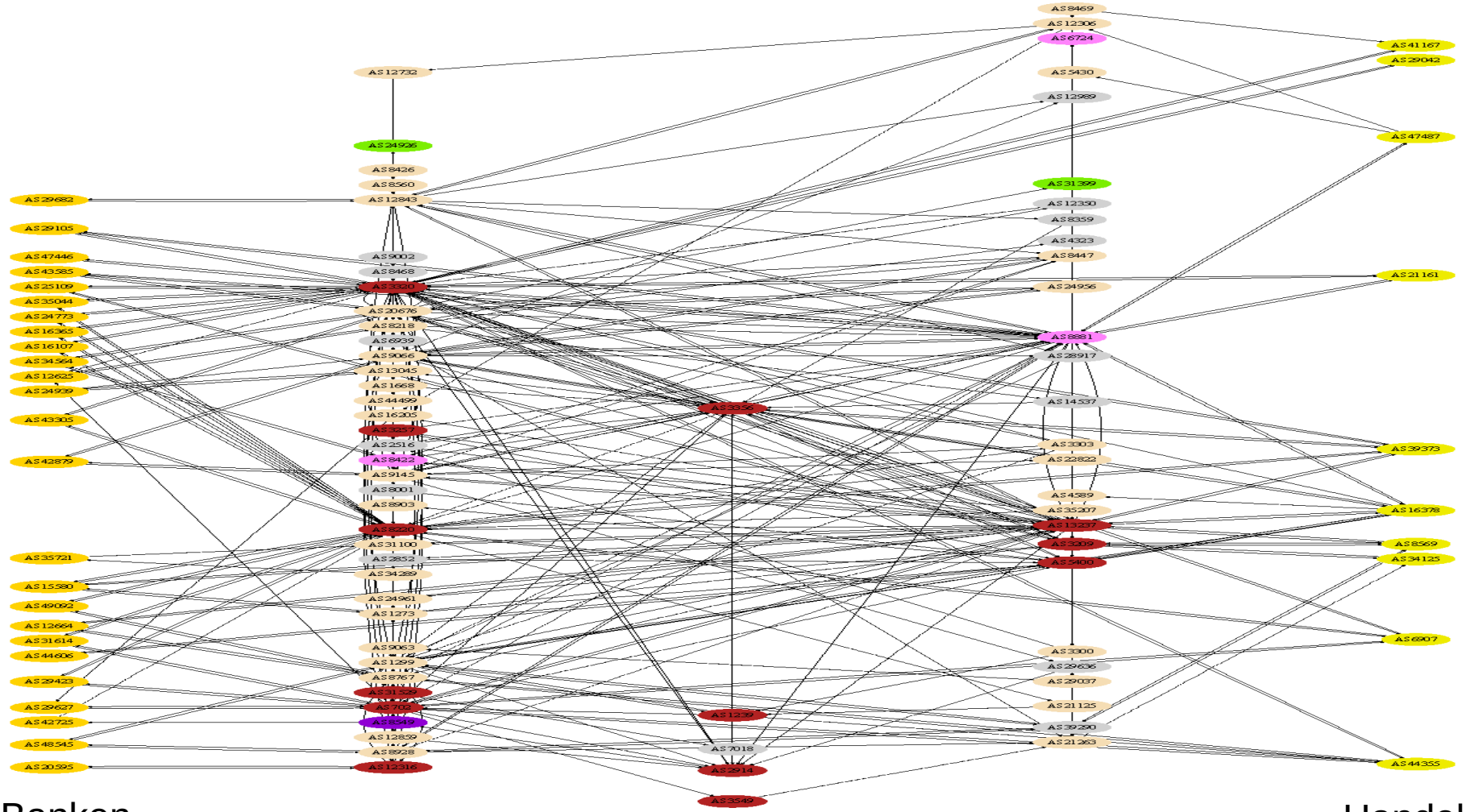
Fazit: Sehr schnell sind Millionen Nutzer betroffen
- Z.B. Systemaktualisierung bei Telekom legt 40 Mio. Nutzer lahm
- Fehler in Internet-Komponenten lassen komplette Netze wegbrechen

Klassische Hochverfügbarkeit? Notrufe? Redundanz?

Zuverlässige Infrastruktur?



Beherrschbare Komplexität?



Banken

Handel

Wenige kennen sich im Notfall wirklich aus!

„The Internet is not Enterprise in Star Treck, but rather an 18th century sailing ship with a small crew pulling the ropes.“

- Aussage eines Insiders einer Sicherheitsberatungsfirma

Bild: www.soic.se

- Allgemein geht man davon aus, dass weltweit nur etwa 1000 Menschen wirklich in der Lage sind z.B. in Notfällen im Internet einzugreifen und es wieder „in Gang zu bringen“

- Störungen hervorrufen können leider sehr viele...

…und jetzt auch noch Angriffe

Auch jenseits staatlicher/hochprofessioneller Angreifer gilt es viel abzuwehren

- Geschätzter Schaden durch Cyberangriffe: 300 Mrd. US$ / Jahr
  - Wie immer Vorsicht bei Schätzungen!
- Im Wesentlichen Industriespionage

Ouroboros. Zeichnung von Theodoros Pelecanos aus Synosius, einem alchemistischen Traktat (1648)

Verbreitung von Angriffswissen nimmt zu

- Hochprofessionelle Angriffswerkzeuge (oft staatlicher Herkunft, z.B. Uroburos) landen mit der Zeit als Virenbaukästen „auf der Straße“
- Cybercrime ist längst einfach buchbare Dienstleistung

Massiver Anstieg von Angriffen

- Insbesondere durch massive Verbreitung von mobilen Geräten
- ... denn hier sind wir im „Neuland“!

Neuland – auch für IT-affine Personen/Firmen

Vielen denken noch im Schema Computer = PC

- Klassische Denkweise der 80er des letzten Jahrhunderts
- Für viele nur Schlagwörter:
  - Smartphone, Phablet, Tablet, Cloud, Fog, smart grid, smart city, smart xy, Internet der Dinge, BYOD (Bring Your Own Device) etc.
  - Ohne zu verstehen, was wirklich dahinter steckt!

ABER

- Vollständiger Computer (mit Betriebssystem, Speicher, Prozessor, E/A,...) steckt in vielen „Dingen“
  - Drucker, BIOS, USB-Stick, Leuchtmittel, Akkumulator, Tastatur, Kopfhörer, Brille etc.
- „Always on“ – es gibt keinen Ausschalter mehr
  - Ständige Verbindung zum Internet bzw. zur Umgebung möglich
- Vielfältige Schnittstellen – auch unbekannte!

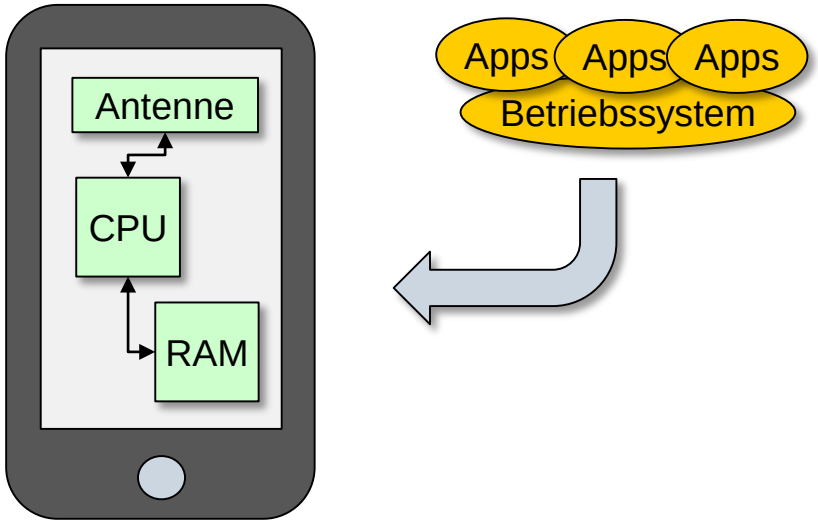
„Klassisches“ Beispiel Mobiltelefon

Smartphones (in allen Ausprägungen) immer weiter verbreitet

- Sicherheitsdiskussion dreht sich meist um Betriebssysteme (Android, iOS, Windows Mobile) bzw. Anwendungen (Apps) und deren Datenhunger/Fehler
- Diverse Firewalls und Antivirensoftware wird angeboten

Smartphone wird oft analog zu einem klassischen PC gesehen

- Prozessor arbeitet Betriebssystem ab
- Auf dem Betriebssystem laufen Anwendungen
- Prozessor entscheidet, was gemacht wird, was gesendet wird etc. – hat also die Kontrolle über das Gerät
- Achtung: 80er-Denke!



Schon das Mobiltelefon ist hochkomplex

Bereits das klassische Mobiltelefon bekam einen zweiten „Computer“ über das SIM

- Prozessor mit kleinem „Betriebssystem“
- Ausführen einfacher Programme
- Unter der Kontrolle des Netzbetreibers
- Zugriff auf diverse Funktionen des Mobiltelefons
- Programmierbarkeit „über die Luft“ (OTA, over-the-air)
- SIM Application Toolkit

Beispiel (Standard 3GPP TS 31.111)

- 4.5 Call control by USIM [UMTS SIM]
  When this service is activated by the USIM, all dialed digit strings […] are first passed to a USIM application before the ME [Mobile Equipment] sets up the call [...]. The USIM application has the ability to allow, bar or *modify* the call [...].

Ein Smartphone ist viel mehr als ein PC

Mehrere Prozessoren mit Speicher und Betriebssystem

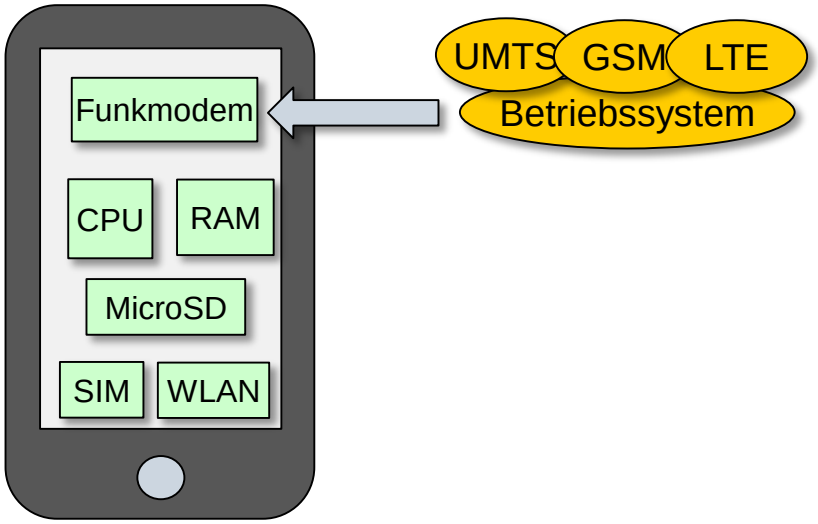
- Prominent: Hauptprozessor mit z.B. iOS, Android, Windows Mobile
- Weniger bekannt: Funkmodem
  - Komplett eigenes Betriebssystem, Kontrolle über das Smartphone
- Hinzu kommen MicroSD-Karte, Grafik-Coprozessor, Ortungssystem, SIM etc. – mit eigenem Speicher, Prozessor, Software

Alle nicht wirklich abschaltbar

- Nur durch echtes Entfernen des Akkus

Betriebssysteme mit „allem drum und dran“ sind sehr klein – passen überall hinein

- Beispiel: RIOT OS
  - für das Internet der Dinge
  - 1,5 kByte RAM, 5 kByte ROM
  - http://www.riot-os.org



Wo ist das Problem?

Funkmodem

- Proprietäres Betriebssystem, nicht offengelegt, veraltete Sicherheitsphilosophie
- Hochkomplex durch umfangreiche Standards, vielfältige Fehler enthalten
- Sicheres Handy-Betriebssystem, Antivirensoftware, Firewall wirken hier nicht, da Funkmodem „außerhalb“ des Prozessors!
- Zugriff von außen möglich

www.nuand.com

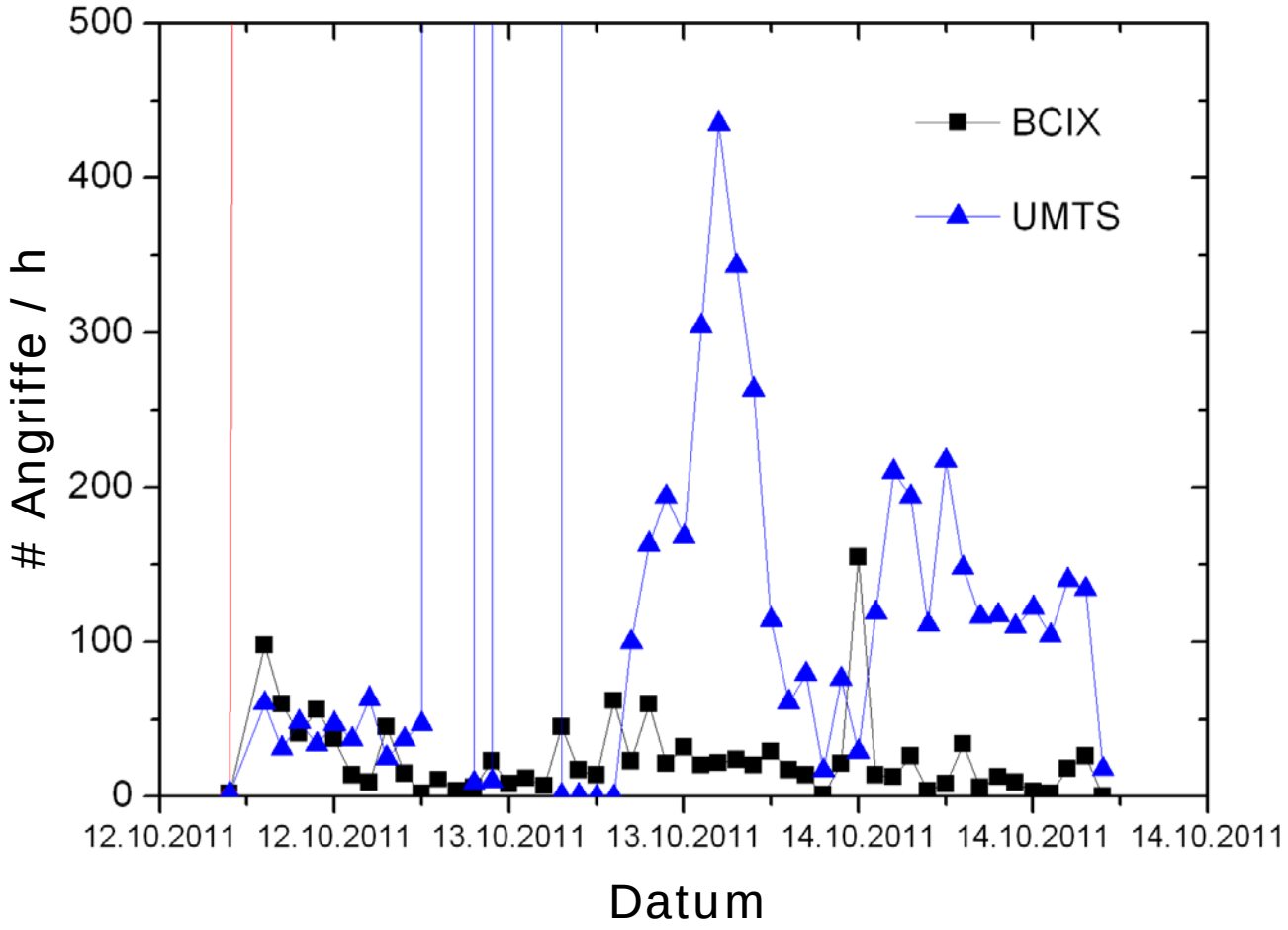
Klassisch

- Kein größeres Problem, da nur Netzbetreiber Zugriff hatte

Heute

- Problematisch, da Netzinfrastruktur billig für jeden erhältlich
- z.B. können gefälschte Basisstationen alles abgreifen
- Zusätzlich „offene“ Hintertüren (z.B. Fernzugriff auf den Speicher, siehe www.replicant.us)

Angriffe im Mobilfunknetz



Was passiert, wenn das Netz angegriffen wird?

Vernetzungsgrad steigt
- Alles mit allem vernetzt
- Immer mehr Bereiche vernetzt

Abhängigkeit wächst
- Keine Produktion ohne Kommunikation
- Kein Geldtransfer ohne Kommunikation
- Rettungsdienste, Kraftwerke …

Fast alles „irgendwie“ Internet-basiert
- Einfacherer Zugang, bekannte Schwachstellen

Viele Motive für einen Angriff
- Politisch, finanziell, aus Spaß
- Sehr hohes Erpressungspotenzial

Fazit: Deutlich erhöhtes Bedrohungspotenzial
- Z.B. Industriespionage, Blockieren des Notrufs…

Bild: REUTERS/Kacper Pempel

Zwischenfälle

McAfee Labs

Bad Program Logic Amplifies Baofeng Attack

By McAfee on May 26, 2009

Gefällt mir 0 Share 0 +1 0 Tweet 0

a domain registrar coupled
work outages in parts of China

200 million users and seve
ws boots and connects to
to DNS servers to get the
use of its massive numbe

USCC.gov

244

minutes on April 8, 2010, China Telecom advertised
rk traffic routes that instructed U.S. and other for-
ffic to travel through Chinese servers.* Other serv-
world quickly adopted these paths, routing all traf-
ercent of the Internet's destinations through serv-
ina. This incident affected traffic to and from U.S.
government (".gov") and military (".mil") sites, including those for the Senate, the army, the navy, the marine corps, the air force, the office of secretary of Defense, the National Aeronautics and Space Administration, the Department of Commerce, the National Oceanic and Atmospheric Administration, and many others. Certain commercial websites were also affected, such as those for Dell, Yahoo!, Microsoft, and IBM.[116]

Although the Commission has no way to determine what, if anything, Chinese telecommunications firms did to the hijacked data, incidents of this nature could have a number of serious implications. This level of access could enable surveillance of specific users or sites.† It could disrupt a data transaction and prevent a user from establishing a connection with a site. It could even allow a diversion of data to somewhere that the user did not intend (for example, to a "spoofed" site). Arbor Networks Chief Security Officer Danny McPherson has explained that the volume of affected data here could have been intended to conceal one targeted attack.[117] Perhaps most disconcertingly, as a result of the diffusion of Internet security certification authorities,‡ control over diverted data could possibly allow a telecommunications firm to compromise the integrity of supposedly secure encrypted sessions.§

tive DNS serv
a player, all onli
sponses previc
queries floodec
ers in parts of
rgeted a speci
ers in China, s
y the attack.

Baofeng Attack:
475 Millionen Nutzer
9 Stunden vom
Internet getrennt

Industriesteuerungsanlagen

Angreifbarkeit der IKT-Infrastruktur

- analog zum „normalen“ Internet, gleiche Technologie
- >95% aller Computer sind integrierte Steuerungssysteme

- Angreifbarkeit der Steuersysteme
  - Smart Meter zu Hause, SCADA (supervisory control and data acquisition) im Kraftwerk
  - Viele Steuerungssysteme sind offen!
    - Nie mit Vernetzung geplant!
    - en.wikipedia.org/wiki/SCADA#Security_issues
  - Bereits einfacher Zugang verfügbar, z.B. Shodan
- Beherrschbarkeit der Komplexität
  - z.B. Bangkok geschätzt 14 Mio. Knotenpunkte zum ansteuern/überwachen

Bild: pacetoday.com.au

Und noch einmal...

- ... ohne Strom geht keine IKT - wie soll die IKT dann die Energieversorgung steuern?

Warum sind wir nicht verunsichert?

Sehr viel, sehr gute Ingenieursleistung schafft Gefühl der Sicherheit
(plus natürlich echte Sicherheit!)

- Bevölkerung ist hohe Versorgungssicherheit gewohnt, kennt hohe Sicherheitsstandards
- Gefühl kann trügerisch sein gerade mit zunehmender Robustheit und geringerer Störanfälligkeit eines Systems

Verletzlichkeitsparadoxon

- „In dem Maße, in dem ein Land in seinen Versorgungsleistungen weniger störanfällig ist, wirkt sich jede Störung umso stärker aus.“ [www.bmi.bund.de]
- Verstärkung durch immer weiter gehende Abhängigkeit

Trends zusammengefasst

Verschmelzung der Techniken
- Internet als Grundlage, eine Netztechnik für viele Dienste
- Kostendruck und Fortschritt lassen Redundanzen verschwinden
- Erhöhtes Bedrohungspotenzial durch einheitliche Technologie und hohe Wertschöpfung

Internet
- Verwundbar durch seine Konstruktion
  - Zusätzlich zu hacking, DDoS, Viren, Trojaner, ...
- Erste Schritte zur Absicherung dieser Kritischen Infrastruktur werden unternommen

Mobilfunksystem
- DER Zugang zum Internet - höherer „Wert“ der Endsysteme für Angreifer

Eingebettete Systeme/Steuerungsanlagen
- >95% aller Computer - oft ohne Vernetzung und Sicherheit geplant

Komplette Abhängigkeit von Energieversorgung
- ...und Energieversorgung mehr und mehr von IT

Achtung: Wir denken oft noch in der Welt der analogen Telefone!

Wie überall so auch im Internet

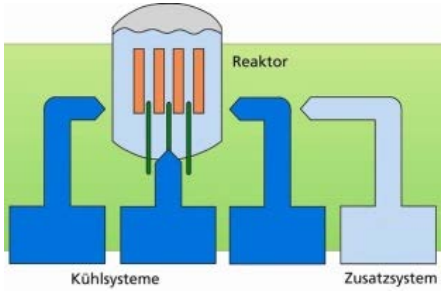


Bild: www.kkw-gundremmingen.de

Redundanz/Reserve vs. Kosten
- Keine Sicherheit ohne Redundanz/Reserve
  - Altbekannt vielen Bereichen
    - Doppelte Bremssysteme, verschiedene Zulieferer, Lagerhaltung ...
  - Aber auch oft vernachlässigt
    - Alles über einen Internet-Anschluss, ein Zulieferer aus Komplexitätsgründen, Monopole mit einer Technologie, just-in-time Lieferungen ...
- Redundanz kostet zusätzlich
  - Totes Kapital

Sicherheit vs. Bequemlichkeit
- Ein Passwort für alles, festes Passwort, kein Passwort
  - Auch in Industriesteuerungsanlagen
- Alles mit allem vernetzen für einfachen Zugriff
  - Vom Handy ins Kraftwerk

Es sollte zumindest eine bewusste Entscheidung sein!

Zu spät? Alles verloren?

Ansatz: Kontrollverlust entgegenwirken wo möglich, Versagen einplanen

- Rein technische Ansätze wirken nur eingeschränkt
  - Z.B. Security Information and Event Management (SIEM) wie Splunk
  - Wirkt nur gegen einfache Angreifer/Angriffe, seltener gegen Profis
  - Gesamtsystem oft nicht verstanden, siehe Mobiltelefon/BYOD/Firmennetze/neue und unbekannte Schnittstellen
- Nur machen, was man versteht
  - Lieber weniger Funktionalität, aber sicher (z.B. eigene Cloud bei Springer-Verlag)
  - Weniger, dafür einfache und klare Schnittstellen (z.B. VPN-Box statt Software-Client)
- Bekanntes auch nutzen
  - Verschlüsselte Dateisysteme, Smartcard statt simples Passwort, Mehrwege-Authentifizierung
  - Vielfältige Best Practices existieren – müssen aber eben auch gelebt werden!
  - Siehe BSI IT-Grundschutz-Kataloge, Zertifizierung etc.

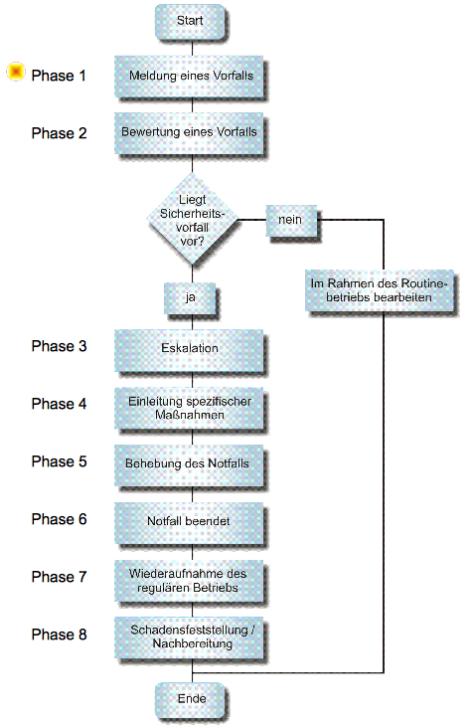
Organisatorische Maßnahmen wichtig

Was tun bei Angriffen von außen oder von innen?

- „klassischer“ Cyberangriff, gekündigter Administrator, kompromittierter Rechner...

Im Vorfeld – Beispiel Freie Universität

- IT-Sicherheitsrichtlinie der Freien Universität Berlin
- Richtlinie Cloud-Datenablage
- Handlungsleitfaden zur Behandlung von IT-Sicherheitsvorfällen an der Freien Universität Berlin
- Handlungsleitfaden: Realisierung von IT-Projekten
- Datenschutz-Richtlinie der Freien Universität
- Handlungsleitfaden: Einbindung des IT-Beauftragten
- IT-Organisationsrichtlinie der Freien Universität Berlin



„under attack“

- Abarbeitung des Notfallplans (der vorab erstellt wurde!)
  - Meldung, Bewertung, Eskalation, Behebung, Nachbearbeitung

Fazit

Bewusst sein, dass teilweise wirklich Neuland betreten wird und nicht alles klar ist

- Wir denken oft noch in alten Strukturen und merken gar nicht, wo Gefahren lauern

Gelebte Sicherheitskultur wichtiger als rein technische Maßnahmen

- Motivation durch Komfortgewinn, transparentere Prozesse
- Es bleibt aber noch einiges zu tun, um Sicherheit überall „komfortabel“ zu gestalten bzw. akzeptierbar (Schlüssel für Türen sind akzeptiert)

Kein wirklicher Schutz gegen hochbezahlte Profis möglich

- Das sind aber auch nur selten die Angriffe des Alltags
- Hier helfen eher juristische/politische Maßnahmen, da OK oder Staaten

Aufklärung und Vorbereitung hilft gegen Ohnmacht und Kontrollverlust

© Andreas Rentz/Getty Images

© REUTERS

Eigene Forschung im Bereich der Sicherheit

KRITIS
IoT
Cloud
Smart Grid, Car, Home, …
4G/5G
Fog
SCADA
M2M
VoIP

Monokulturen
Malware
Kostendruck
Komplexität
Altlasten
Bequemlichkeit
Organisierte Kriminalität

- Vernetzte Sicherheit
- Robustes Kommunikationsminimum
- Ad-hoc-Strukturen
- Sichere SW & HW
- Redundanz
- Gelebte Sicherheit
- Resiliente Systeme
- Schulung, Aufklärung
- Gesetzgebung
- …

Geschäftsmodell für sichere, robuste Systeme?

Beispiel Vernetzte Sicherheit

Nicht-Technische Herausforderungen

Neue Prozesse passend zum technologischen Wandel erforderlich

Training/Schulung/Ausbildung

- Komplett anderes Niveau verglichen mit klassischen Sicherheitstechnologien

IP-Ökosystem

- Andere Interaktionen und Gefahren

Testen, Simulationsumgebung, Resilienz, Zusammenspiel

- Technisch, wie rechtlich – bis zur Entscheidungsebene

Passen hierzu Tarife, Karrierewege, Gesetzgebung?

Das ist ja schön, aber …

- Wer soll das umsetzen, wer hat die Verantwortung?
  - Rollen, Verständnis, Bereichsfürsten vs. cloud
- Wie sieht meine Angriffsfläche aus?
  - Technisch, Mitarbeiter/-innen, …
- Wie sollen die Sicherheitsmaßnahmen getestet, überwacht werden?
  - Pen-Test, Code review, Werkzeuge
- Wann, wie, wer soll Verfahren aktualisieren?
  - Schneller technologischer Wandel
- Wie soll die Aufklärung stattfinden?
  - Schulungen, permanent „subkutan“, Bewusstseinskampagnen
- …