Bundesamt
für Sicherheit in der
Informationstechnik

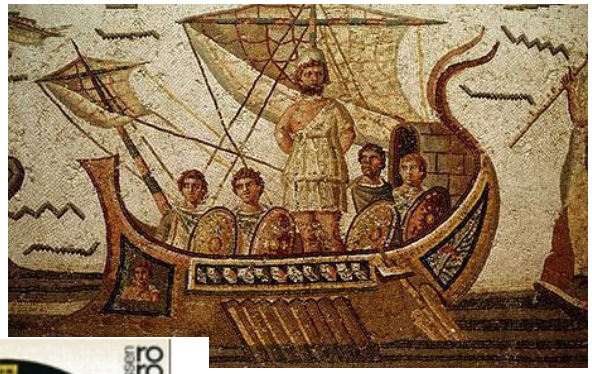
Cyber-Sicherheitsarchitektur für Deutschland

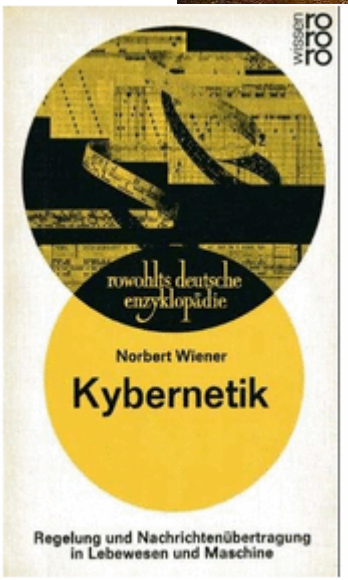
Dr. Günther Welsch
Bundesamt für die Sicherheit in der Informationstechnik

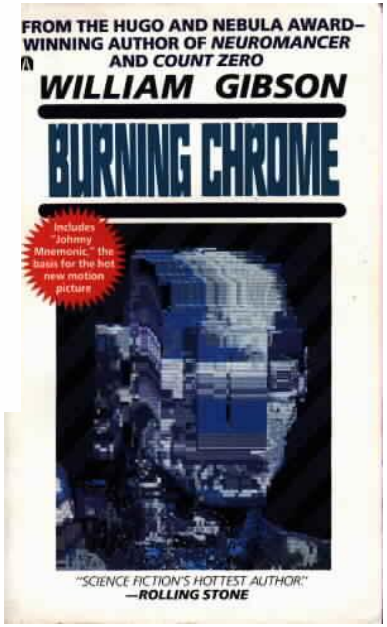
27. November 2013

Die Cyber-Welt (1)

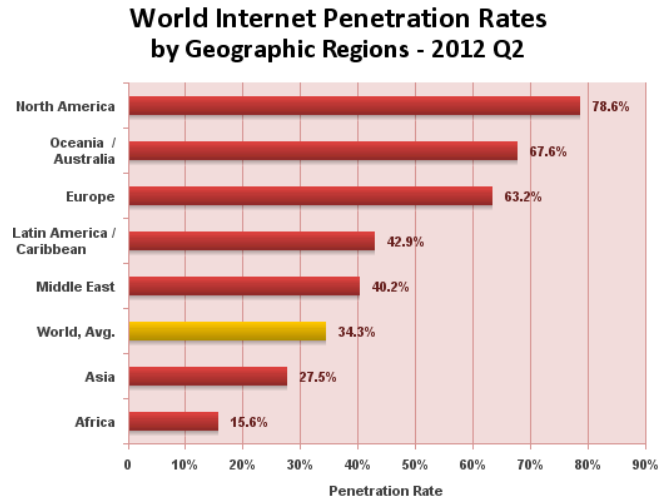
- „Cyber“: Altgriechisches Präfix : „Steuerung“, ursprünglich die „Steuerkunst des Seefahrers“ (Quelle: Wikipedia)
- 1948: Norbert Wiener: „Kybernetik – Regelung und Nachrichtenübertragung in Lebewesen und Maschinen“
- 1982: William Gibson: Burning Chrome
- 1991: Die erste WWW-Seite am CERN
- 2007: Cyber-Warfare in Estland
- 2012: Mobiles Internet: Penetration 50%
- 2012: Cloud-Computing: ca. 1 Mrd € Umsatz in Deutschland

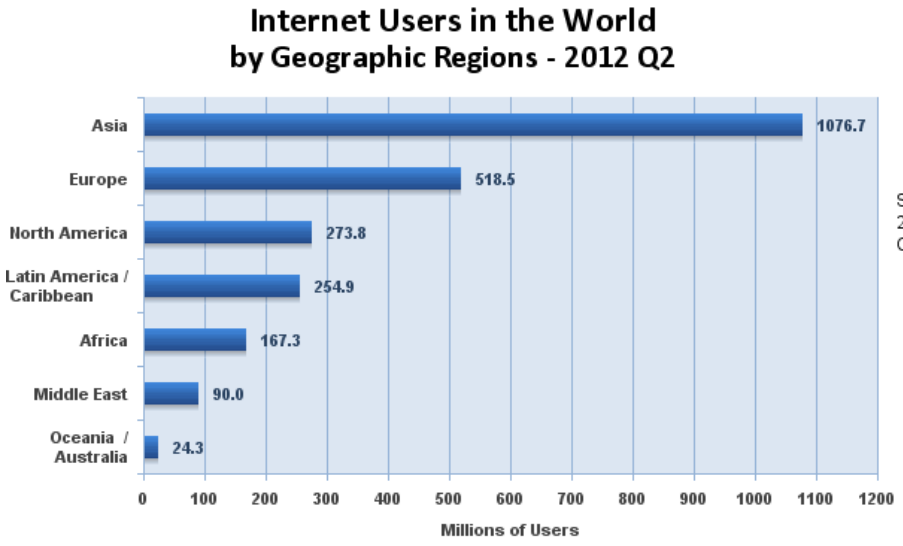




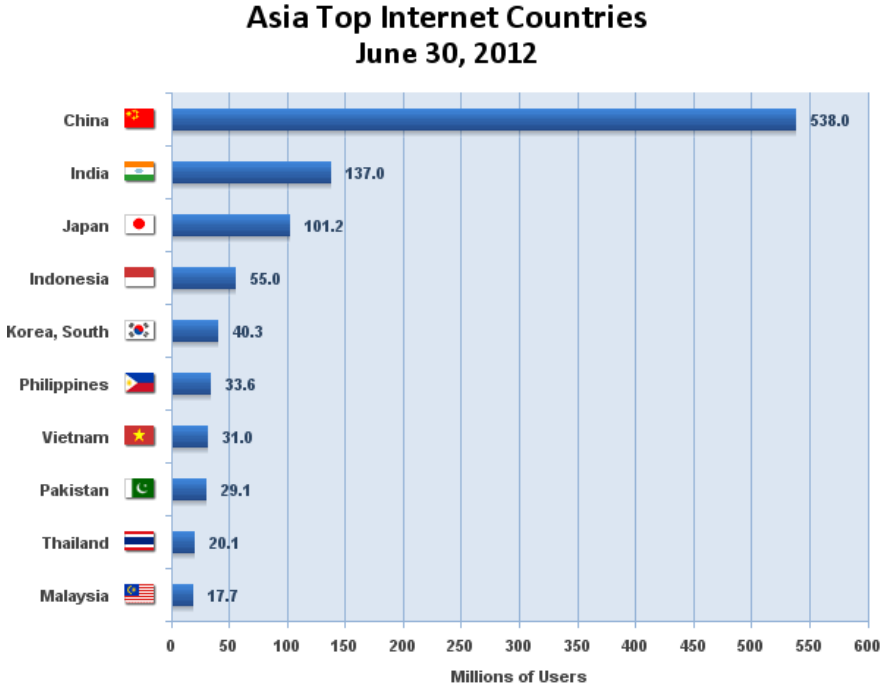


Die Cyber-Welt (2)





Source: Internet World Stats - www.internetworldstats.com/stats.htm
2,405,518,376 Internet users estimated for June 30, 2012
Copyright © 2012, Miniwatts Marketing Group



Source: Internet World Stats - www.internetworldstats.com/stats3.htm
2,405,518,376 Internet users in the World estimated for June 30, 2012
Copyright © 2012, Miniwatts Marketing Group

- 7,0 Mrd. Menschen
- 2,4 Mrd. Nutzer im Cyber-Raum
  - 34 % aller Menschen
  - 45 % der Nutzer in Asien

Die Cyber-Welt (3)

Wertschöpfung mit Cyber-Technologien:

- Klassische Geschäftsmodelle werden ergänzt
- Neue Geschäftsmodelle entstehen
- Alte Industrien werden transformiert (digitalisiert)
- Hohe gesellschaftliche Akzeptanz
- Quelle zukünftigen Wohlstands
- Schritt in den Cyber-Raum unvermeidlich!

Chancen / Risiken:

- Effektivität..... ↑
- Effizienz ..... ↑
- Technologiefortschritt..... ↑
- Neue Geschäftsmodelle..... ↑
- Ökologische Wertschöpfung.. ↑↓
- Digital Divide ..... ↑
- Verlässlichkeit der Systeme... ↓
- Beherrschbarkeit..... ↓
- Missionskrit. Abhängigkeiten. ↑
- Kritische Abhängigkeiten..... ↑

Entwicklung von Sicherheitsarchitekturen

Steinzeit

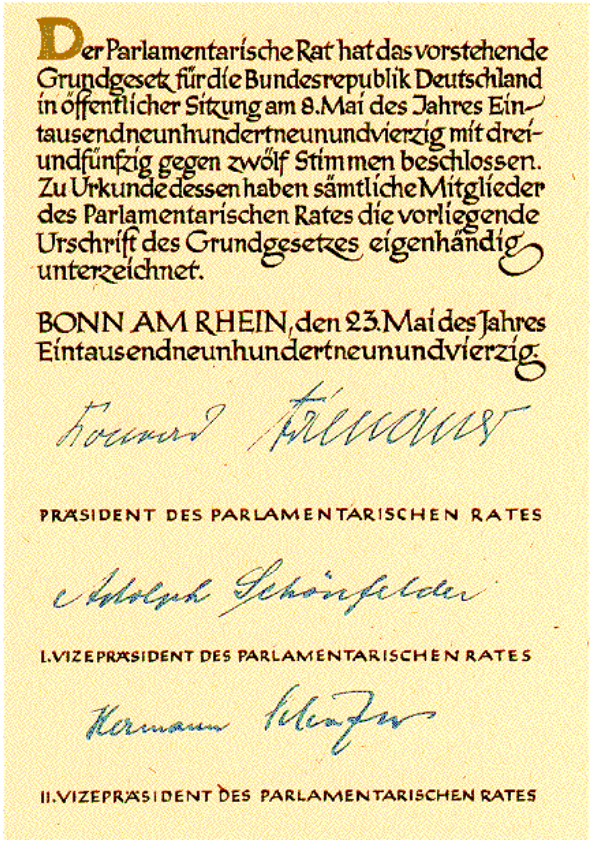
Mittelalter

Absolutismus

U.S.A.

Revolution

1919



1949

Deutschlands Sicherheitsarchitektur

Verfassung

- Deutschland als föderaler Bundestaat
- Gewaltenteilung der Organe: Legislative, Exekutive, Judikative
- Trennung von
  - innerer und äußerer Sicherheit
  - Polizei und Nachrichtendiensten
  - Kirche und Staat
- Verwaltungsgesetze regeln und begrenzen
  - Aufgaben und Befugnisse der Behörden
  - Eingriffe in die Freiheit des Einzelnen
- Bürgerrechte
  - Rechtsmittel gegen staatliches Handeln

Rolle und Aufgaben des Staates

- Freiheits- und Ausgleichsfunktion
- Schutz- bzw. Gewährleistungsfunktion
- Angebots- und Innovationsfunktion

- Wohlstand
- Zukunftssicherheit
- Soziale Sicherheit
- Soziale Gerechtigkeit
- Bildung
- Forschung

„Sicherheit“ und „Risiko“

- Sicherheit: Ein Zustand, der frei von unvertretbaren Risiken der Beeinträchtigung ist oder als gefahrenfrei angesehen wird.
  (Quelle: Wikipedia)

- Sicherheit beziehbar auf:
  - Einzelne Individuen
  - Gesellschaft von Individuen, Staaten
  - Reale Objekte und Systeme
  - Abstrakte Gegenstände, z.B. den Cyber-Raum

- „Risiko“: Maß für den Eintritt und die Auswirkung eines schädigenden Ereignisses.

- In der IT-Sicherheit: Produkt aus Eintrittswahrscheinlichkeit eines Ereignisses und des potentiellen Schadens

- Risikomanagement
  - Transparenz
  - Vermeidung
  - Reduzierung (Maßnahmen)
  - Transfer, Überwälzung
  - Akzeptanz

„Scheinsicherheit“

- Risiken werden nicht transparent
- Ungeeignete Maßnahmen führen zu leicht überwindbarer Sicherheit.
- Effektivität von Maßnahmen ist nicht immer *per se* ersichtlich.
- Maßnahmen erzeugen Kosten, reduzieren aber nur scheinbar das Risiko.
- Nutzer fühlen sich „sicher“, sind es aber faktisch nicht.

- In der IT ist Scheinsicherheit manchmal schwierig zu erkennen!

Unsichere Informationstechnologie

- **Technologisches Umfeld:**
  - Hohe Flexibilität und Vielseitigkeit von Informationstechnologie
  - Schnelle Innovationszyklen
  - Periodische Leistungssprünge
- **Kundenumfeld**
  - (Bislang) geringe Erwartungshaltung an Softwarequalität und Sicherheit
  - Schnelligkeit und Einfachheit vor Sicherheit
- **Wettbewerbsumfeld**
  - Globalisierung
  - Funktionalität und Ergonomie
  - Effizienz- und Kostendruck

Grundsätzliche Rahmenbedingungen für Technikentwicklung und Innovation:

- **Nützlichkeit und Effektivität:** Prognostizierter Nutzen muss notwendige Aufwände und verbundene Nachteile überwiegen.
- **Rentabilität und Effizienz:** Prognostizierte Einkünfte müssen Ausgaben übertreffen.
- **Kompatibilität mit Werten:** Nur Techniken, die kulturell, sozial oder rechtlich akzeptiert werden, lohnen den Aufwand der Verwirklichung.

Bundesamt
für Sicherheit in der
Informationstechnik

Technische Sicherheitslage

Betroffene Systeme

- Betriebssysteme
- Programme (Applikationsebene)
- Mobile Plattformen
- Web-Plattformen
  - Mobile App-Märkte
- Industriesteuerungen
  - Industry Control Systems (ICS)
  - SCADA

Häufige Probleme (u.a.):

- Schwaches Identitätsmanegement
- Kein IT-Sicherheitsmanagement
- Wiederholung gleicher Fehler
- Adaption „schlechte“ SW
- Konsumenten IT
- Erosion des Perimeterschutzes

Technische Sicherheitslage

Verwundbarkeiten:

- ca. 10.000 neu in 2012
- 20% kritisch ausnutzbar
- 90% remotefähig
- 49% Web Applikationen
- 50% ungepatched in 365 Tagen

Schadprogramme:

- Alle zwei Sekunden ein neues Schadprogramm
- 21.000 Webseiten täglich mit Schadprogrammen infiziert
- Zahlreiche Spionageangriffe täglich allein auf die Bundesverwaltung

Qualität von Cyber-Angriffen

Ungerichtete Angriffe

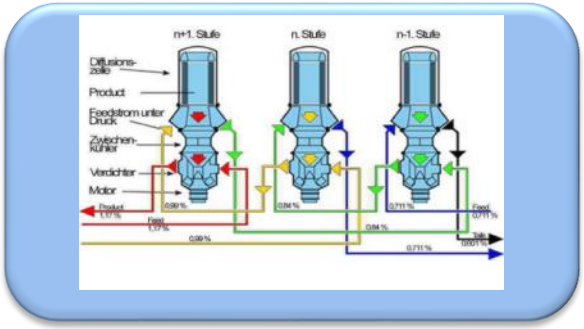
- Sabotage, Betrug, etc.
- Unspezifische Zielgruppen
- **SPAM, Viren, Würmer, Trojaner, Drive-by-Downloads**

Gezielte Angriffe

- Spionage und Sabotage
- Spezielle Zielgruppen
- **Social-Engineering und Trojaner**

Skalpellartige Angriffe

- Sabotage spezieller IT-Systeme (und Infrastrukturen) mit großem Schadausmaß
- Komplexe , langwierige Vorbereitung
- **Zero-Day-Verwundbarkeiten**
- **Fälschung von Zertifikaten**



Cyber-Angriffe und Werkzeuge

Gegen Deutschland

Rank	Country	Percentage
1	United States	40%
2	Russia	32%
3	Germany	16%
4	China	3%
5	United Kingdom	1%

Weltweit

Rank	Country	Percentage
1	United States	46%
2	China	12%
3	South Korea	5%
4	Germany	4%
5	United Kingdom	3%

Quelle: Symantec Security Report

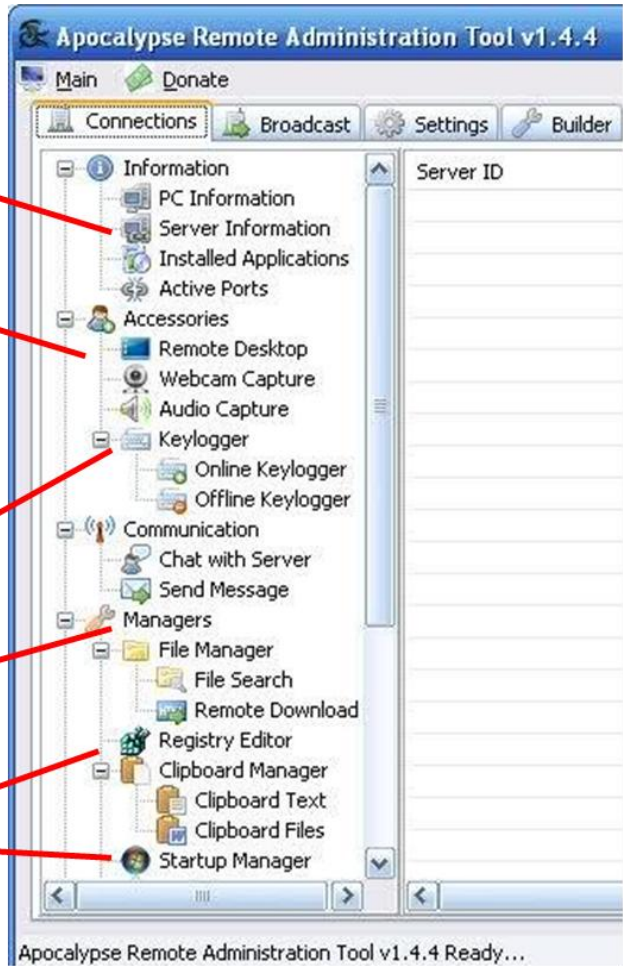
Konfiguration

Fernzugriff
- Bildschirm
- Webcam
- Mikrofon

Keylogger

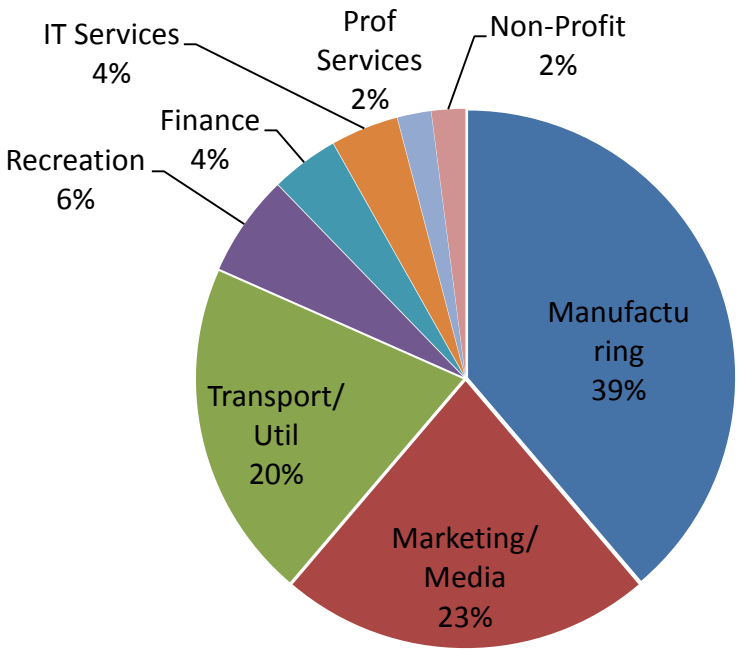
Datenabfluss
- Dateidownload

System-modifikation

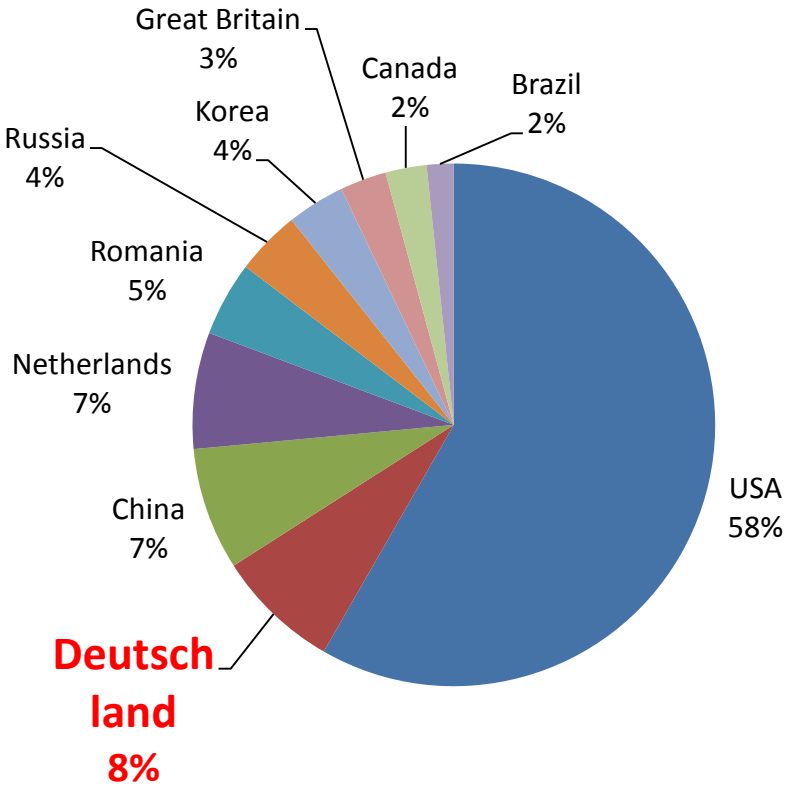


Gezielte Angriffe auf Deutschland

Opfer gezielter Angriffe



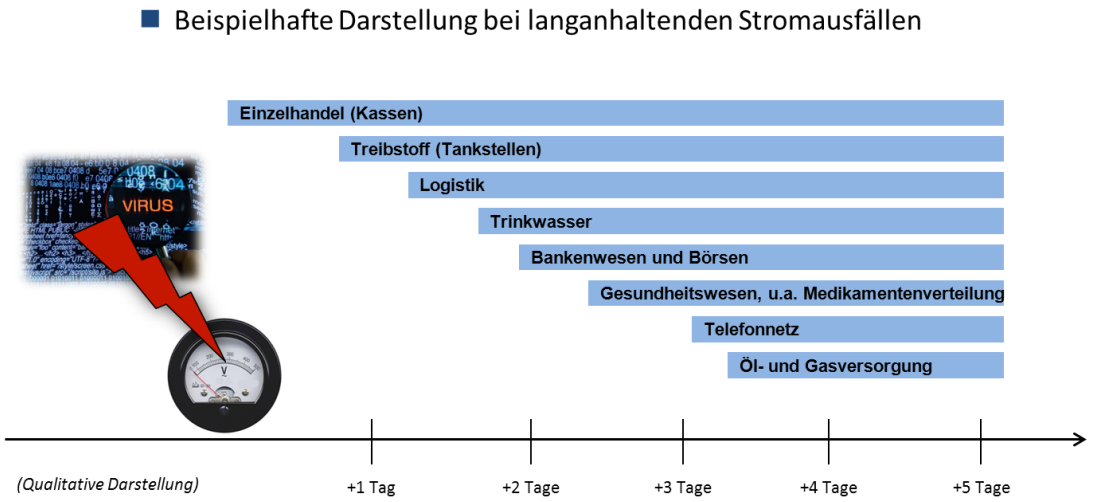
Verteilung von C&C Servern



- Quelle: Symantec Security Report

(Missions-) Kritische Infrastrukturen

KRITIS: Infrastrukturen mit wichtiger Bedeutung für das staatliche Gemeinwesen, deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere, dramatische Folgen bewirken.



- Digitalisierung und Vernetzung in allen Lebensbereichen, auch in KRITIS!
- Schlüsselbedingungen:
  - Verfügbare und
  - verlässliche IT und Energie

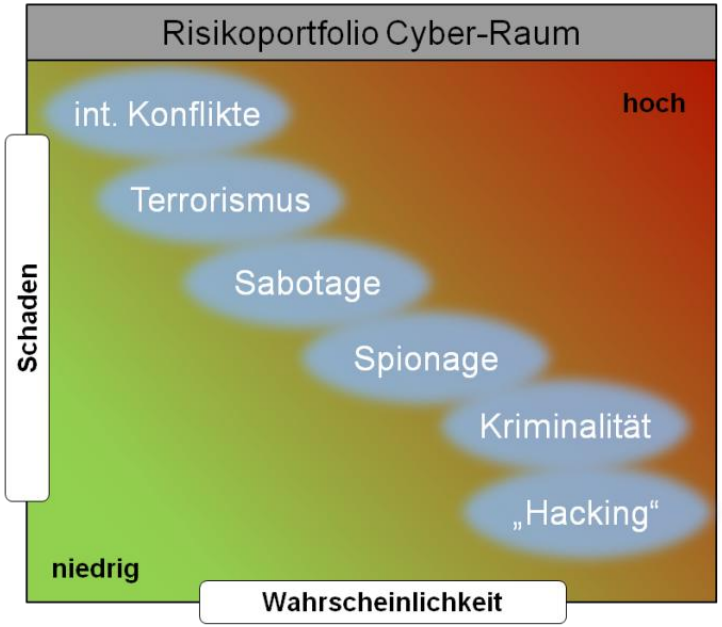
Folge: Neue Kritikalitäten in Bezug auf IT entstehen in allen Wirtschafts- und Lebensbereichen.

Advanced Persistent Threats (APT)

Angriff	Opfer	Entdeckung (Dauer)	Ziele
Duqu	6 Organisationen in 8 Ländern	10/2011 (11 Monate)	Diebstahl von Zertifikaten, IDs, etc.
Stuxnet	5 iranische Organisationen	07/2011 (1 Jahr)	Sabotage von Steuerungsanlagen
Downbot “Shady RAT”	71 Organisationen: Verteidigungsindustrie, IT-Industrie, UN, IOC	07/2011 **(5 Jahre)**	Spionage von Datenbanken, E-Mail, Verschlusssachen, etc.
RSA-Angriff	EMC/RSA, Lockheed Martin	03/2011 (2 Monate)	Diebstahl von SecurID informationen
Hydraq “Aurora”	>20 Organisationen Google, Rackspace, Adobe, Juniper	01/2010 (6 Monate)	Diebstahl von Source Code, IP, Spionage von Gmail Konten

Quelle: Symantec

Risikoportfolio



Angreifer	Anteil
Hacker	31 %
Kriminelle	19 %
Aktivisten	13 %
ND	10 %
Unbekannt	27 %

Quelle: BSI

Kriminalstatistik

Cyber-Kriminalität 2012 (BKA):

- ca. 64.000 gemeldete Fälle (+7,5%)
- Schäden ca. 42,5 Mio. €
- Wenige hochspezialisierte Täter
- Zunahme von international arbeitsteilig wirkenden Kriminellen

Schätzung der EU:

- 1 Mio. Menschen pro Tag betroffen
- 290 Mrd. € Schäden p.a. weltweit

Bundesamt
für Sicherheit in der
Informationstechnik

„Cyber“-Sicherheitsarchitektur

Fortschreibung und Weiterentwicklung mit Blick auf Cyber-Risikosituation:

- Schutz der demokratischen Verfassung, der demokratischen Werte und der freiheitlichen Wirtschaftsverfassung
- Schutz des individuellen Persönlichkeitsrechts (informationelle Selbstbestimmung, Datenschutz)
- Schutz des Agierens und Handelns im Cyber-Raum
- Schutz der Offenheit und Freiheit des Cyber-Raums

- Schutz des Wirtschaftsraums
- Schutz vor Cyber-Warfare
- Verfolgung von Cyber-Kriminalität
- Schutz vor Spionage und Sabotage durch Staaten, Konkurrenten, kriminelle Organisationen

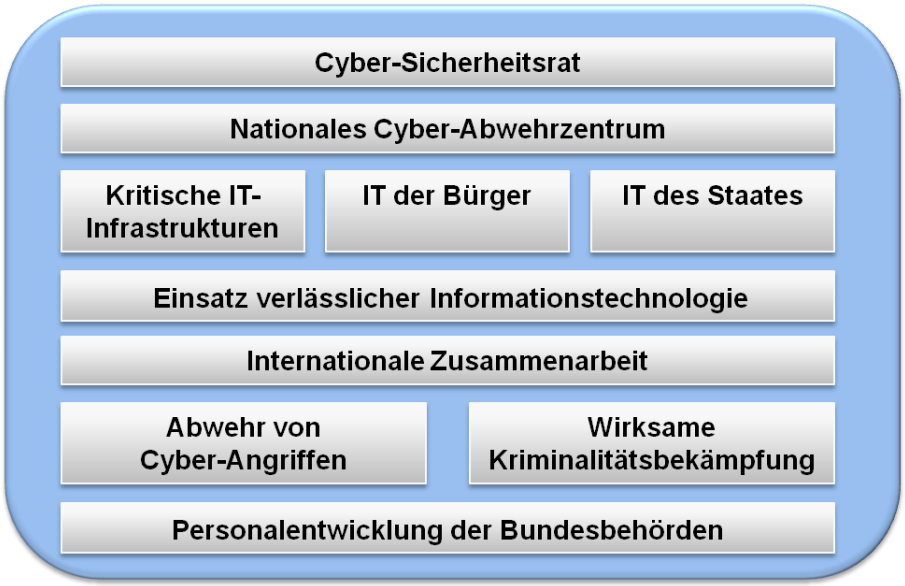
Bundesamt
für Sicherheit in der
Informationstechnik

Die Cyber-Sicherheitsstrategie für Deutschland

Feb
23
2011

Beschluss des Bundeskabinetts am 23. Februar 2011:

„ Ziel der am 23.02.2011 beschlossenen Cyber-Sicherheitsstrategie für Deutschland ist es, Cyber-Sicherheit auf einem der Bedeutung und der Schutzwürdigkeit der vernetzen Informationsinfrastrukturen angemessenen Niveau zu gewährleisten, ohne die Chancen und den Nutzen des Cyber-Raums zu beeinträchtigen.“



Kritische Informationsinfrastrukturen

Zielrichtung

- Systematischer Ausbau der Zusammenarbeit im UP KRITIS
- Intensiver Informationsaustausch
- Prüfung Erforderlichkeit, Notwendigkeit neuer Verpflichtungen
- Zusätzlicher Befugnisse bei konkreten Bedrohungen
- Harmonisierte Regelungen zur Aufrechterhaltung der Verfügbarkeit in IT-Krisen

Aktivitäten

- Organisatorische/inhaltliche Weiterentwicklung des UPK
- Strategische Ausweitung des Teilnehmerkreises UPK
- Definition sektorspezifischer Mindestsicherheitsanforderungen
- Festigung/Ausbau von Melde- und Alarmierungsprozessen
- Evaluierung der aufsichtsrechtlichen Grundlagen

Bundesamt
für Sicherheit in der
Informationstechnik

Sichere IT-Systeme in Deutschland

De
De-Mail

Anti-Botnet
Beratungszentrum

Zielrichtung

- Sicherheitsbewusstsein und Sensibilisierung verbessern
- Gemeinsame Initiativen mit gesellschaftlichen Gruppen
- Zielgerichtete Bündelung von Informations- und Beratungsangeboten

BÜRGERCERT
Ins Internet - mit Sicherheit

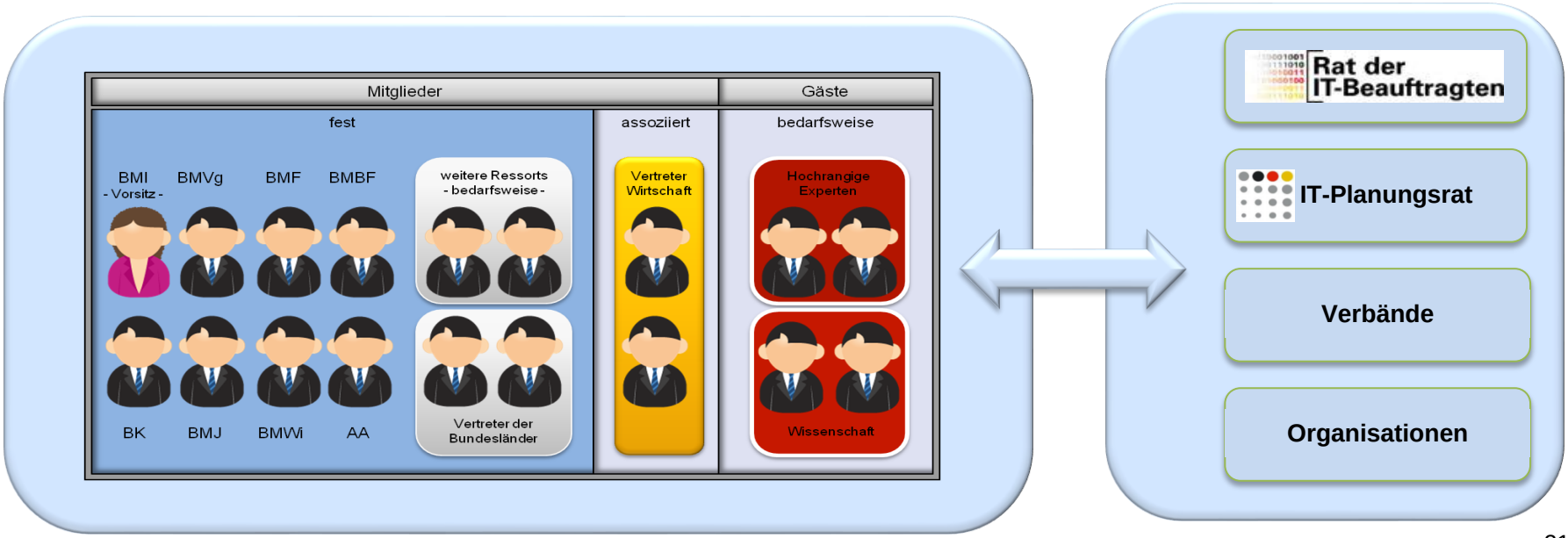
Aktivitäten

- BMWi Task Force „IT-Sicherheit in der Wirtschaft“
- Allianz für Cyber-Sicherheit
- Vorbereitung eines IT-Sicherheitsgesetzes
  - Mindestanforderungen an TK-Provider und Befugnisse zur Erkennung von Schadaktivitäten (SPAM/Botnet-Schutz)
  - Etablierung von Meldewegen für erkannte skalierende IT-Vorfälle
  - Einführung Mindeststandard Nutzerinformation und Sicherheitswerkzeuge für Nutzer

Nationaler Cyber-Sicherheitsrat

Zielrichtung und Aufgaben

- Identifikation und Beseitigung struktureller Krisenursachen
- Koordinierung präventiver Instrumente & übergreifender Politikansätze
- Beratung Handlungsempfehlungen des Cyber-Abwehrzentrums



Bundesamt für Sicherheit in der Informationstechnik

Nationales Cyber-Abwehrzentrum

Nationales Cyber-Abwehrzentrum

Zielrichtung

Staatliche Stellen

- Optimierung operativer Zusammenarbeit
- Koordinierung Schutz- und Abwehrmaßnahmen

Informationsaustausch

- Schwachstellen, Verwundbarkeiten, Angriffsformen und Täterbilder
- IT-Vorfälle analysieren und Handlungsempfehlungen abstimmen
- Empfehlungen an Cyber-Sicherheitsrat
- Berichte an Krisenstab

Cyber-Abwehrzentrum

Bundesamt für Sicherheit in der Informationstechnik

Bundesamt für Verfassungsschutz

Bundesamt für Bevölkerungsschutz und Katastrophenhilfe

- Kernbehörden BSI, BfV, BBK
- Erweiterter Kreis: BKA, BND, BPOL, Bundeswehr, ZKA
- Berücksichtigung der Interessen der Wirtschaft zum Schutz vor Kriminalität und Spionage
- Für alle Akteure gilt:
  - Strikte Wahrung der Aufgaben und Befugnisse
  - Umsetzung in eigener Verantwortung

BKA

BUNDESPOLIZEI

ZKA ZOLLKRIMINALAMT

Bundesnachrichtendienst

Wirksame Kriminalitätsbekämpfung

Zielrichtung

Fähigkeiten der Sicherheitsbehörden und Wirtschaft

- Verbesserte Bekämpfung
  - IuK – Kriminalität
  - Spionage und Sabotage

Zusammenarbeit mit Wirtschaft

- Know-how Austausch in gemeinsamen Einrichtungen mit der Wirtschaft
- Institutionalisierte PPP
- BDI-DIHK-BMI Wirtschaftsschutz

Internationale Zusammenarbeit

- Förderung strukturschwacher Partnerländer
- Prüfung weiterer Übereinkommen in Vereinten Nationen
- Harmonisierung Strafrecht auf Grundlage der **Convention on Cybercrime**

Bundesamt
für Sicherheit in der
Informationstechnik

Effektives Zusammenwirken für Cyber-Sicherheit in Europa und weltweit

Zielrichtungen

Europa

- Aktionsplan zum Schutz kritischer Informationsinfrastrukturen
- Verlängerung und maßvolle Erweiterung Mandat ENISA
- Bündelung von IT-Zuständigkeiten in EU-Institutionen
- EU Strategie „Innere Sicherheit“ und „Digitale Agenda“

Internationale Organisationen

- Cyber-Kodex: Kodex für staatliches Verhalten im Cyber-Raum
- Botnetz-Abwehr

NATO

- Strategisches Konzept
- Fundament der transatlantischen Sicherheit
- Einheitliche Sicherheitsstandards als Best-Practice für zivile Infrastrukturen (auch KRITIS)

Bundesamt
für Sicherheit in der
Informationstechnik

Einsatz verlässlicher und vertrauenswürdiger Informationstechnologie

Zielrichtungen

Innovative Schutzkonzepte

- Verbesserte IT-Sicherheit
- Forschung für IT-Sicherheit und Schutz Kritischer Infrastrukturen
- Technologische Plurarität bewahren
- Zertifizierung in sicherheitskritischen Bereichen

Common Criteria

Strategische IT-Kernkompetenzen

- Technologische Souveränität und wissenschaftliche Kapazität stärken
- Politische Strategien entwickeln und weiterentwickeln
- Kräfte mit Partnern und Verbündeten (insb. in Europa) bündeln

Instrumentarium zur Abwehr von Cyber-Angriffen

Gesamtstaatliche Sicherheitsvorsorge

Plan

- Geeignete Schutzmaßnahmen planen (Maßnahmenplanung)

Do

- Schutzmaßnahmen umsetzen
- Übungsprozesse mit allen Akteuren etablieren
- Bedrohungslage regelmäßig prüfen

Check

- Monitoring der Zielerreichung (Cyber-Sicherheit)
- ggf. Bedarf weiterer gesetzlicher Befugnisse auf Bundes-/Landesebene evaluieren

Act

- Abstimmung und Komplettierung des Instrumentariums

Bundesamt
für Sicherheit in der
Informationstechnik

Organisationen und Einrichtungen mit Cyber-Sicherheitsbezug

BMI
- Lagezentrum
- IT-Krisenstab*
- Cyber-Sicherheitsrat
- UP BUND
- UP KRITIS
- BSI (zugleich als Nationale Cyber-Abwehrbehörde NCDA)
- BKA
  - IPPP
- BfV
- BBK
- BPOL

Länder
- LKA, LfV, LfDI, Verwaltungs-CERT-Verbund

Bundeskanzleramt
- BND

BMVg
- CERT-Bw
- KSA
- MAD

BMWi
- TF IT-Sicherheit in der Wirtschaft

BMF
- ZKA

BMELV

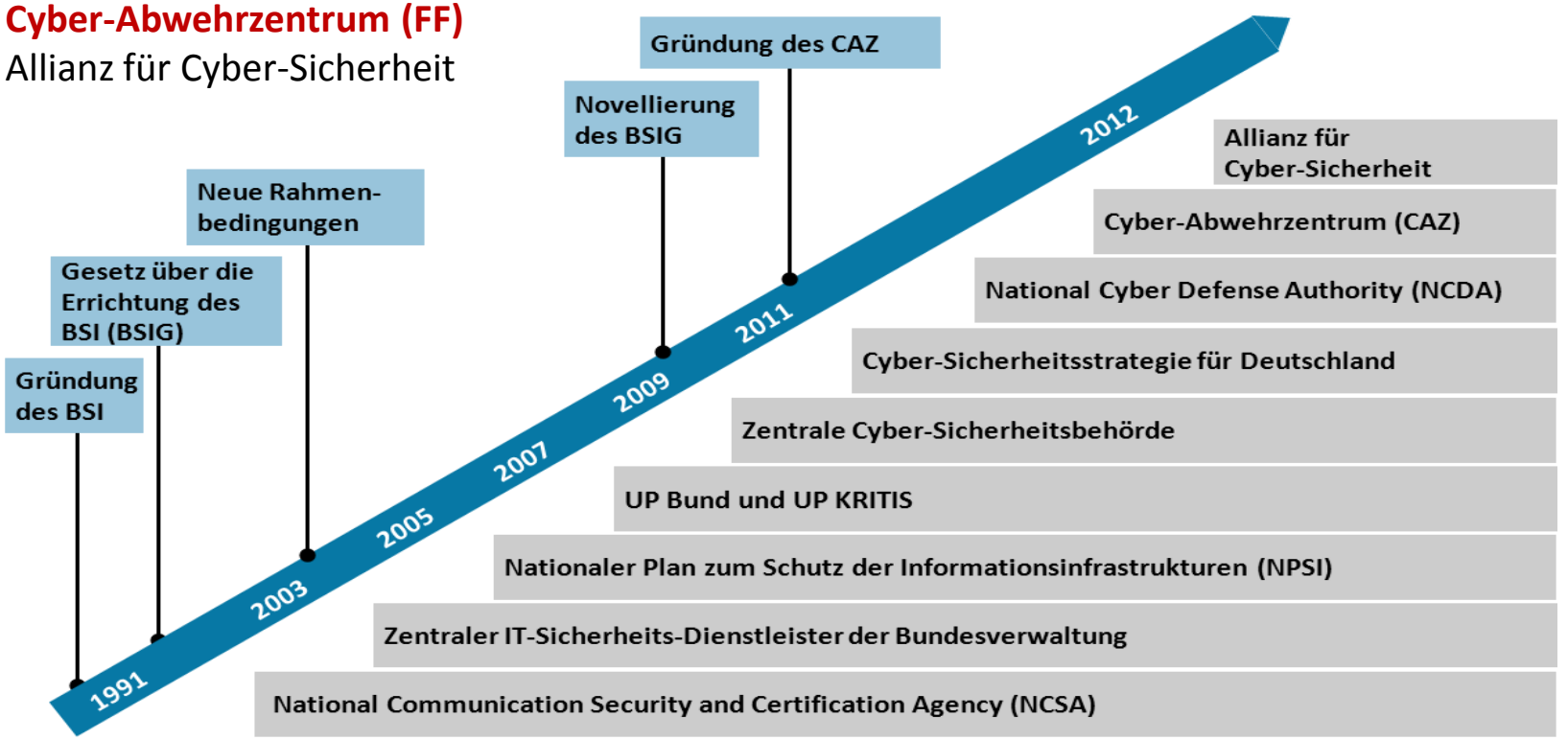
BfDI

Wirtschaft
- ASW
- DSiN
- Teletrust
- NIFIS
- BITKOM
- eco
- CERT-Verbund
- BDI – DIHK – BMI Nat. Strategie Wirtschaftsschutz

Das BSI als Cyber-Sicherheitsbehörde

BSI (zugleich National Cyber Defense Authority)

- CERT-Bund
- IT-Lagezentrum
- IT-Krisenreaktionszentrum*
- **Cyber-Abwehrzentrum (FF)**
- Allianz für Cyber-Sicherheit



Bundesamt
für Sicherheit in der
Informationstechnik

Entwurf für ein IT-Sicherheitsgesetz

Mär
18
2013

- Wahrnehmung staatlicher Verantwortung für Infrastrukturen mit Bedeutung für das Gemeinwohl (Fokussierung auf KRITIS-Bereiche)
- Erwartung der Bürger, Anwender und Nutzer nach stärkerer Rolle des Staates.

Anforderungen an die Verwaltung

Einrichtung der zentralen Meldestelle im BSI für Bundesverwaltung und Kritische Infrastrukturen (§8b)

Erstellung Lagebild und Unterrichtung betroffener KRITIS Betreiber

Jährliche Berichtspflicht des BSI zur Sensibilisierung (§13)

Anforderungen an die Wirtschaft

Mindestanforderungen IT-Sicherheit

- Kritis-Betreiber („Stand der Technik“)
- Branchenspezifische Mindeststandards
- Nachweis der Einhaltung durch Audits

Telemedien Anbieter

- Technischen Schutz gegen unerlaubten Zugriff gewährleisten

Meldepflicht für IT-Sicherheitsvorfälle

- Einrichtung Warn- und Alarmierungskontakte
- Meldung schwerwiegender Beeinträchtigungen

TK Anbieter

- Unerlaubte Zugriffe und Beeinträchtigungen an BNetzA melden
- Unterrichtung von Nutzern, die Störungen verursachen
- Hinweis auf technische Hilfsmittel zur Beseitigung

EU-Cybersicherheitsstrategie

Feb
7
2013

Cybersicherheitsstrategie der EU:
"ein offener, sicherer und geschützter Cyberraum“

Digitale Agenda
(= EU-Binnenmarkt)

(1) Widerstandsfähigkeit gegenüber Cyberangriffen

Inneres
(= Innere Sicherheit EU)

(2) Eindämmung der Cyber-Kriminalität

EU-Außen- und Sicherheitspolitik

(3) Cyberverteidigungs-politik/kapazitäten

(4) Industrielle und technische Ressourcen für die Cybersicherheit

(5) Cyberraumstrategie der EU auf internationaler Ebene

Die Grundwerte der EU

Richtlinien Vorschlag der EU Kommission
zu Netzwerk- und Informationssicherheit (NIS)

Bundesamt
für Sicherheit in der
Informationstechnik

Zukünftige Herausforderungen

Weltpolitisch

- Verteilungskämpfe um begrenzte Ressourcen
- Cyber-Raum wird 5. Gefechtsfeld des Militärs
- Dominanz U.S.A. , China , Indien (?)
- Zunahme der Asymmetrie
- Wegfall innerer- & äußerer Sicherheit

Politisch

- „Race to the Bottom“
- „Computer Crime Havens“
- Unbegrenzte ND-Aufklärung
- Verschiedene Demokratie & Sicherheitsbegriffe weltweit
- Kollision von Werten in westl. Staaten
- Zunahme Abhängigkeit von IT

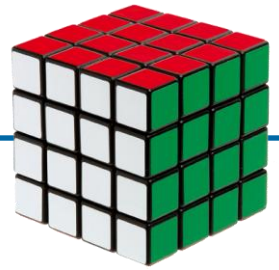
Wirtschaftspolitisch

- Informationsmonopole bei Unternehmen (Entzug demokratischer Kontrolle)
- Verwundbarkeit Cyber-Geschäftsmodelle
- Transformation in Cyber-Industrie
- „Zwang“ zur Vernetzung & Datenpreisgabe bei Teilhabe
- Deutsche IT-technologische Souveränität schwindet
- Smarte Produkte & Fabrik der Zukunft
- Missionskritische Abhängigkeiten

Technologisch

- Cloud Computing
- Big Data Analytics
- Virtualisierung
- Gestaltung intelligenter Netze

Ausklang



Der Cyber-Raum:

- Globale Vernetzung zwischen Systemen, Prozessen, Personen & Institutionen
- Viele neue Potenziale und Chancen, begleitet durch neue Gefahren
- Cyber-Sicherheit bedingt vernetztes Sicherheitsdenken auf technischer, organisatorischer, sozialer, wirtschaftlicher, rechtlicher und politischer Ebene

Komplexitätszunahme:

- Jede Maßnahme hat häufig komplexe Wirkungen und Rückwirkungen
- Mit den Worten Carl-Friedrich von Weizsäcker:

„Einige Dinge hängen enger zusammen, alles hängt mit allem zusammen. Da wir aber den Zusammenhang von allem mit allem nicht zu denken […] vermögen, denken wir Einzelnes. Unsere Schwäche ist, dass wir Einzelnes isoliert denken und nicht in seinem Zusammenhang. Dann stoßen wir darauf, dass das doch falsch ist...“ („Große Denker: C.F.v.W.“ , M.Drieschner (S.101))

Kontakt:

Dr. Günther Welsch
Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 183-189
53175 Bonn

Tel: 0228 / 99 9582 5900
E-Mail: guenther.welsch@bsi.bund.de