

# Schutz kritischer IT-Infrastruktur

## Neue Risiken für Wirtschaft und Staat

Marit Blattner-Zimmermann

Bundesamt für Sicherheit in der Informationstechnik

1. Regionalkonferenz „Unternehmenssicherheit in Mitteldeutschland“  
3. November 2005

## Agenda

- Das BSI
- Kritische Infrastrukturen
- Bedrohungen
- Schäden
- Schutzmöglichkeiten



## Das BSI

... ist eine unabhängige und neutrale Stelle für Fragen zur IT-Sicherheit in der Informationsgesellschaft.

- Gründung 1991 per Gesetz als nationale Behörde für IT-Sicherheit
- Jahresbudget: € 52 Mio. (2005)
- Mitarbeiter: 450
- Standort: Bonn



## Zielgruppen des BSI

### Regierung und Verwaltung

- Unterstützung der E-Government Initiative (BundOnline2005)
- IT-Sicherheitsberatung
- Entwicklung von Kryptosystemen
- Lauschabwehr
- Betrieb des Regierungsnetzes



### Wirtschaft

- Nationales CERT
- IT-Grundschutz
- Zertifizierung
- Sicherheitspartnerschaften



### Bürger

- Sensibilisierungskampagnen
- BSI-Internetangebot
  - [www.bsi.bund.de](http://www.bsi.bund.de)
  - [www.bsi-fuer-buerger.de](http://www.bsi-fuer-buerger.de)
- Fachbeiträge in Zeitschriften
- Veranstaltungen, Messen, Kongresse



## Agenda

- Das BSI
- **Kritische Infrastrukturen**
- Bedrohungen
- Schäden
- Schutzmöglichkeiten



## Kritische Infrastrukturen Definition

Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden.

(2004)

## Kritische Infrastruktursektoren

- Transport und Verkehr
- Energie
- Gefahrenstoffe
- Informationstechnik und Telekommunikation
- Finanz-, Geld- und Versicherungswesen
- Versorgung
- Behörden, Verwaltung und Justiz
- Sonstiges



## KRITIS ↔ IT-Sicherheit

### KRITIS

- National/Gesamtstaatlich
  - Politisch / Strategisch
  - Interdependenzen
  - Transnationale Absprachen
- Versorgung sicherstellen
- technisch, physisch, psychologisch, organisatorisch
- Zusammenführung von
  - IT-Management
  - Sicherheitsmanagement
  - IT-Sicherheitsmanagement
- konzeptionell



### IT-Sicherheit

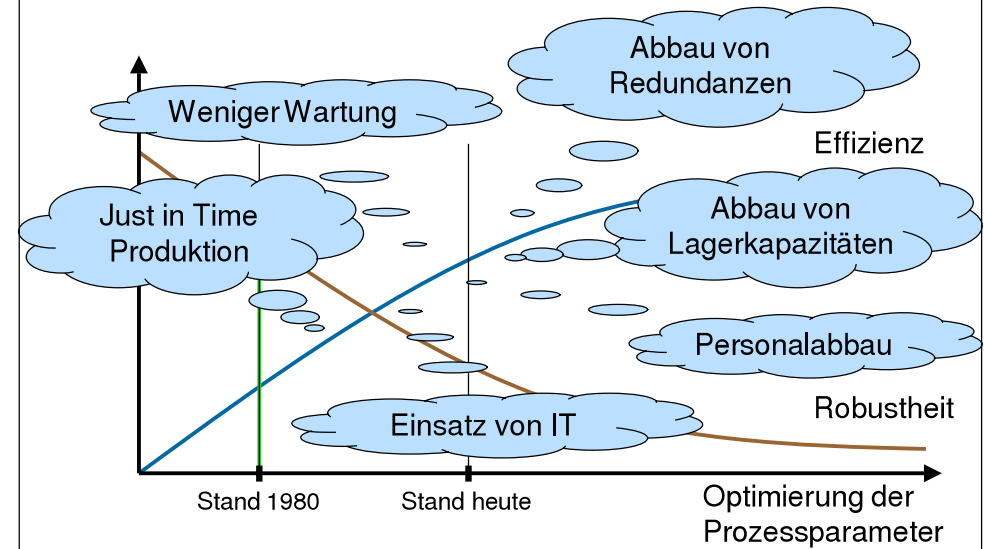
- Firmenbezug  
max. Gesamtkonzern
- Betrieb sicherstellen
- zumeist technisch, firmenorganisatorisch
- praxisorientiert

## Agenda

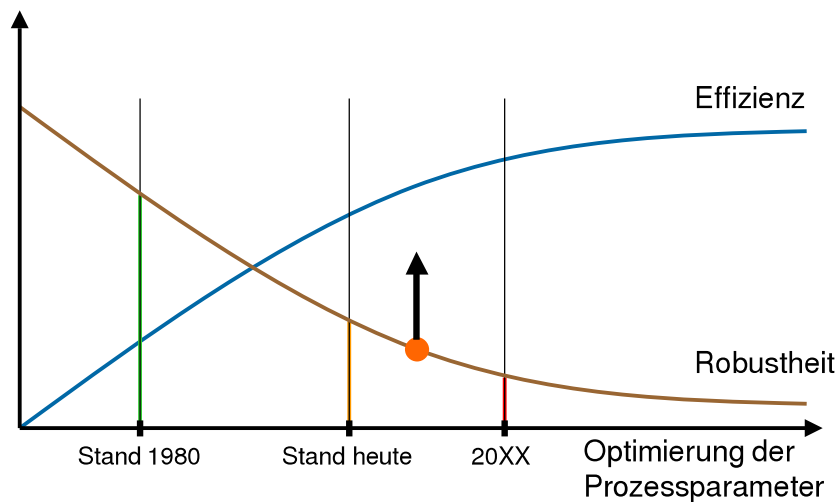
- Das BSI
- Kritische Infrastrukturen
- Bedrohungen**
- Schäden
- Schutzmöglichkeiten



## Effizienz vs. Robustheit Prozesse, Infrastrukturdienstleistungen, ...



## Effizienz vs. Robustheit Prozesse, Infrastrukturdienstleistungen, ...



## Bedrohungen Kategorien

- Höhere Gewalt
- Organisatorische Mängel
- Menschliche Fehlhandlungen
- Technisches Versagen
- Vorsätzliche Handlungen

## Organisatorische Mängel

- ❑ Fehlende Ressourcen
- ❑ Fehlende Unterstützung durchs Management
- ❑ Mangelnde Zuständigkeitsregelung,  
Kompetenzübertragung, Vertreterregelung
- ❑ Mangelnde Kommunikation / Informationsfluss
- ❑ Externe Abhängigkeiten
  - ❑ Outsourcing
  - ❑ Externe Lieferungen
  - ❑ Vernetzung („Dominoeffekte“)
- ❑ Unzureichende Umsetzung / Kontrolle der Umsetzung



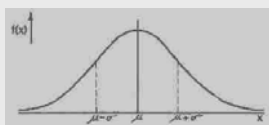
## Menschliche Fehlhandlungen

- ❑ Formen einer Fehlhandlung
  - ❑ Fehlbedienung
  - ❑ Fehleinschätzung
  - ❑ Fehlverhalten
- ❑ Gründe für Fehlhandlungen
  - ❑ Überlastung / Überforderung
  - ❑ Unwissen / Unfähigkeit
  - ❑ Langeweile / Faulheit
  - ❑ Leichtsinn / Fahrlässigkeit
  - ❑ Verführung / Social Engineering

## Unterschiede zwischen Unfall / Störungen und Vorsatz

### Unfall / Störung

- ❑ Unerwartet
- ❑ Darauf vorbereitet, da  
relativ wahrscheinlich
- ❑ Reaktion vorbereitbar
- ❑ Statistisch verteilt



### Vorsatz

- ❑ Unerwartet nach  
Vorbereitung
- ❑ Nutzer ist nicht  
vorbereitet
- ❑ Reaktion kaum  
vorbereitbar da  
Täter trickst
- ❑ Gezielt auf  
Schwachpunkt



**Kriminelle Energie**

## Vorsätzliche Handlungen (Täter)

- ❑ Script-Kiddies
- ❑ (Hack-) Aktivisten
- ❑ Hacker / Cracker
- ❑ Innentäter
- ❑ (Wirtschafts-) Kriminelle /  
Organisierte Kriminalität
- ❑ Terroristen
- ❑ Nachrichtendienste
- ❑ Militär

## Innentäter

- ❑ Berater/ Vertragspartner, Externe, Mitarbeiter
- ❑ Oft **weit gehendes Wissen**
- ❑ Grob **zwei Gruppen** :
  - a) Von Dritten Beauftragte
  - b) Innentäter, die aus eigenen Motiven handeln
- a) **Ziel:** Ausspähen sensibler Informationen.
- b) **Ziel:** Weitergabe sensibler Informationen, gezielte Manipulation von Netzwerken und Prozessen oder Vernichtung von Daten

Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors  
<http://www.cert.org/archive/pdf/insidercross051105.pdf>

## Konkurrenzausspähung (umgangssprachlich Industriespionage)

- ❑ Ausspähen sensibler Unternehmensinformationen
- ❑ Nutzung der Ressourcen von Mitbewerbern
- ❑ **Ziel:** Informationen über Preise und Angebote sowie Produktionstechnik und Marketingstrategie
- ❑ **Auswirkungen:** von unbedeutenden finanziellen Schäden bis zur Existenzvernichtung

## Konkurrenzausspähung - Beispiel -



news 30.05.2005 17:05 << Vorige | Nächste >>

### Trojaner spionierte israelische Unternehmen aus

Ein umfangreicher Fall von Industriespionage erschüttert momentan die israelische Wirtschaftswelt. Mit einem eigens entwickelten Trojaner wurden gleich mehrere große Unternehmen monatelang von Konkurrenten belauscht. Zu den Auftraggebern zählen nach Angaben israelischer Ermittlungsbehörden unter anderem die Mobilfunk-Provider Cellcom und Pelephone, der Satelliten-TV-Anbieter Yes sowie der Mineralwasserabfüller Tami-4.

In der vergangenen Woche wurden 18 Personen in Zusammenhang mit dem Fall verhaftet, darunter sieben Manager der verdächtigten Unternehmen. Es sei noch nicht absehbar, welcher Schaden entstanden ist,

- ❑ Mehrere große Unternehmen über Monate belauscht
- ❑ PCs ließen sich mit den Trojanern komplett fernsteuern
- ❑ Sensible Dokumente wurden auf FTP-Server geladen

## Wirtschaftsspionage

- ❑ Ausspähen sensibler Informationen durch **Geheimdienste / Nachrichtendienste**
- ❑ **Ziel:** Informationen über Preise, Angebote sowie Produktionstechnik und Marketingstrategie
- ❑ Verwendet werden Systemtools und selbstgeschriebene, maßgeschneiderte Programme oder Angriffswerkzeuge
- ❑ Angreifer wollen in jedem Fall **anonym** bleiben

Abwehr von Wirtschaftsspionage  
<http://www.in.zrw.de/sch517.htm>

## Lagebericht zur IT-Sicherheit in Deutschland

- Erstmaliges Erscheinen 2005, geplant als Periodikum
- Inhalt:
  - Darstellung des Sachstands
  - Überblick über anstehende Herausforderungen
  - Einordnung und Bewertung von Trends
  - Aufzeigen von Handlungsbedarf
- Ziel:
  - Information und Sensibilisierung
  - Weiterhin verlässliche Nutzung der IT zum Vorteil aller gesellschaftlichen Gruppen Deutschlands



## Agenda

- Das BSI
- Kritische Infrastrukturen
- Bedrohungen
- **Schäden**
- Schutzmöglichkeiten

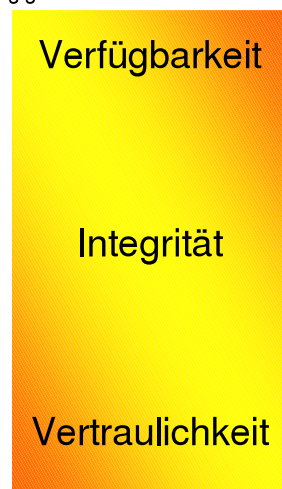


## IT-Vorfälle

### Erkennbarkeit des Verlustes



### Schadpotenzial (Abhängig von Infrastruktur-Anforderungen)



## Schadensarten

Gesetzesverstoß	Gesundheit / Leben	Ansehen / Vertrauen
Vermögenswerte	Öffentliche Sicherheit	Sachwerte

- seltenes Auftreten
- minimale Dauer
- geringstmögliche Schadensauswirkung
- beherrschbar
- isolierbar
- reparabel

- Das BSI
- Kritische Infrastrukturen
- Bedrohungen
- Schäden
- **Schutzmöglichkeiten**



- Sensibilisierung
  - Mitarbeiter
  - IT-Fachkräfte
  - Führungskräfte / Hausleitung
- Risiko- / Bedrohungsanalysen
- angemessene Schutzmaßnahmen
- Notfall- / Katastrophenpläne
- Erkennen von Abhängigkeiten
- Redundanzen / Fallback-Lösungen



### BSI-Homepage

- Grundschutz [www.bsi.bund.de](http://www.bsi.bund.de)
- KRITIS [www.bsi-fuer-buerger.de](http://www.bsi-fuer-buerger.de)
- Viren



[www.im.nrw.de/verfassungsschutz/](http://www.im.nrw.de/verfassungsschutz/)

Mittelstand  
**sicher** im Internet [www.sicherheit-im-internet.de](http://www.sicherheit-im-internet.de)

## Beispielrichtlinie

### "Aus der Praxis – für die Praxis"

- Entstanden in Kooperation mit großem Unternehmen aus dem Energiesektor
- in der Alltagspraxis bewährte IT-Sicherheitsrichtlinie; vom BSI überarbeitet
- Möglichkeit für jedes Unternehmen die Effektivität seiner eigenen IT-Sicherheitsmaßnahmen zu prüfen und ggf. anzupassen und damit zu verbessern.
- [www.bsi.bund.de/fachthem/kritis/hilfsmittel.htm](http://www.bsi.bund.de/fachthem/kritis/hilfsmittel.htm)



## Standort-Sicherheitscheck

- Auf Basis der Beispielrichtlinie entwickelt
- Audit-Materialien mit Durchführungsempfehlungen, Fragenkatalogen für Mitarbeiterinterviews, Auswertungshilfen etc.
- Hilfe zur Überprüfung der Umsetzung der Beispielrichtlinie und zur Darstellung des Status der IT-Sicherheit im eigenen Unternehmen
- [www.bsi.bund.de/fachthem/kritis/hilfsmittel.htm](http://www.bsi.bund.de/fachthem/kritis/hilfsmittel.htm)



## Basisschutzkonzept BBK / BKA

- Konzept zum präventiven Schutz Kritischer Infrastrukturen
- Erstellt in Kooperation mit der Wirtschaft
- **Analyse potenzieller Gefährdungen** wie:
  - terroristische Anschläge
  - kriminelle Handlungen
  - Naturkatastrophen
- Empfehlung baulicher, organisatorischer, personeller und technischer **Schutzvorkehrungen**
- [www.bmi.bund.de](http://www.bmi.bund.de)



## Zusammenfassung

- Die **Abhängigkeit** von der IT **wird zunehmen**.
- Die eigene IT wird von **innen und außen bedroht**.
- Das **Bewusstsein** für IT-Bedrohungen **reicht nicht aus**.
- Ein **ganzheitlicher**, nicht nur auf die Technik gerichteter Ansatz ist notwendig.
- **Prävention** stellt eine **zentrale Aufgabe** dar.
- **Kooperation** zwischen Staat und Wirtschaft ist **von zentraler Bedeutung**.

## Informationsmöglichkeiten

### KRITIS-Homepage des BSI

[www.bsi.bund.de/fachthem/kritis/index.htm](http://www.bsi.bund.de/fachthem/kritis/index.htm)

### Nationaler Plan zum Schutz der Informationsinfrastrukturen (NPSI)

[www.bmi.bund.de](http://www.bmi.bund.de)

### Studie: Internationale Aktivitäten zum Schutz Kritischer Infrastrukturen

ISBN 3-922746-54-3

### IT-Grundschutzhandbuch

[www.bsi.bund.de/gshb/index.htm](http://www.bsi.bund.de/gshb/index.htm)

### Lagebericht zur IT-Sicherheit in Deutschland 2005

[www.bsi.bund.de/literat/lagebericht/index.htm](http://www.bsi.bund.de/literat/lagebericht/index.htm)

### Weitere Publikationen des BSI

[www.bsi.bund.de/literat/index.htm](http://www.bsi.bund.de/literat/index.htm)



## Kontakt



Bundesamt für Sicherheit in der  
Informationstechnik (BSI)  
Präsident

Marit Blattner-Zimmermann  
Godesberger Allee 185-189  
53175 Bonn

Tel: +49-1888-9582-100  
Fax: +49-1888-10-9582-100

[marit.blattner@bsi.bund.de](mailto:marit.blattner@bsi.bund.de)  
[www.bsi.bund.de](http://www.bsi.bund.de)