



# „Die Rolle des Staates im Bereich der IT – Sicherheit“

**14.03.2008, München**

**Horst Samsel**

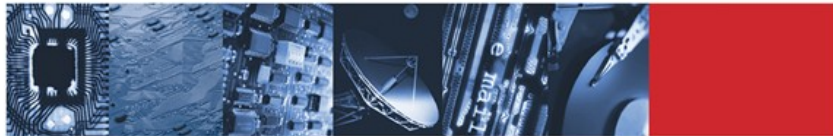
Bundesamt für Sicherheit in der  
Informationstechnik



# Das BSI – der zentrale IT-Sicherheitsdienstleister des Bundes



Sichere Informationstechnik  
für unsere Gesellschaft



Leitbild



**Prävention**

Informationsinfrastrukturen angemessen schützen



**Reaktion**

Wirkungsvoll bei IT-Sicherheitsvorfällen handeln



**Nachhaltigkeit**

Deutsche IT-Sicherheitskompetenz stärken -  
international Standards setzen

## Positionierung, Kunden:

- operativ: Bundesverwaltung
- kooperativ: Wirtschaft, Wissenschaft
- informativ: Bürger

## Kennzahlen:

- 1991 gegründet
- ca. 500 Mitarbeiter
- 64 Mio. € Jahresbudget

# Produkt- und Dienstleistungsportfolio

- ❑ Verschlüsselungsprodukte zur Sicherstellung der staatlichen Souveränität
- ❑ mitgestaltende Rolle bei Galileo, BOS-Digitalfunk, hoheitlichen Dokumenten
- ❑ Sicherheit durch Prüfung und Zertifizierung von IT-Produkten





# BSI-Dienstleistungen

## ■ ■ ■ ■ ■ Beratung

- Risiken im Internet und bei bestimmten IT-Technologien
- Sicherheit für IT-Plattformen und -Infrastrukturen für Bundesbehörden
- Penetrationstests
- Grundschatz als Methodik und Werkzeug für sichere IT-Infrastrukturen
- Risikobewertung und Sicherung Kritischer Infrastrukturen

## ■ ■ ■ ■ ■ Zentrale Serviceleistungen und Betrieb

- Schlüsselmitelherstellung/-verteilung und Root-CA (Bund)
- Warn- und Alarmdienste, CERT-Bund
- Technische Koordination des IVBB

## ■ ■ ■ ■ ■ Spezielle Technische Messungen und Abnahmen

- Abstrahlprüfungen für Kommunikationseinrichtungen
- Prüfung und Abnahme von TK-Anlagen
- Lauschabwehrprüfungen
- Prüfungen der materiellen Sicherheit

## ■ ■ ■ ■ ■ Information

- Internet-Sicherheit für alle Zielgruppen
- Spezielle Themen der Informationstechnik
- Webportal für Bürger, Wirtschaft und Verwaltung
- Veröffentlichungen von Fachthemen und Sicherheitshinweisen
- Präsentation der Arbeitsergebnisse bei Fachmessen und -kongressen

## ■ ■ ■ ■ ■ Entwicklung

- Kryptoverfahren, Biometrische Verfahren
- IT-Sicherheitslösungen (z.B. Kryptogeräte für den staatlichen Geheimschutz)
- Testwerkzeuge und Messmittel für Konformitätsprüfungen und für die Abhörsicherheit

## ■ ■ ■ ■ ■ Prüfvorschriften

- Schutzprofile für IT-Komponenten und -Produkte
- Technische Richtlinien für Komponenten in IT-Projekten der Bundesbehörden
- Schutzprofile und Technische Richtlinien von allgemeiner Bedeutung

## ■ ■ ■ ■ ■ Prüfung, Bewertung, Zertifizierung und Zulassung

- Evaluierung und Zertifizierung der Sicherheit von IT-Komponenten und -Systemen
- Zulassung von Systemen für die elektronische Verschlusssachenbearbeitung
- Abnahme- und Typmusterprüfung von IT-Sicherheitskomponenten

## ■ ■ ■ ■ ■ Akkreditierung

- Anerkennung und Qualitätssicherung von Prüfstellen und Auditoren



# Entwicklung des IT-Sicherheitsrechts

Datenschutzrecht

Signaturgesetz/-verordnung

Strafrecht

spezielle Regelungen

Verfassungsrecht



## § 9 Technische und organisatorische Maßnahmen

„ Öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.“



# Bundesdatenschutzgesetz

- Schutz des Einzelnen vor Verletzung seines Persönlichkeitsrechts aufgrund des Umgangs mit Daten, § 1 BDSG
- Normadressat: öffentliche und nicht-öffentliche Stellen
- Gebot unter Beachtung der Verhältnismäßigkeit Regelungen des Bundesdatenschutzgesetzes, insbesondere § 9 Satz 1 BDSG samt Anlage einzuhalten
  - Anlage schreibt besondere technische und organisatorische Kontrollen im Umgang mit elektronischer Datenverarbeitung vor
  - regelt u.a.: Zutritts-, Zugangs-, Zugriffs-, Weitergabe-, Eingangs-, Auftrags- und Verfügbarkeitskontrolle
- Ausführung des Gesetzes wird von Aufsichtskontrolle überwacht (§ 38 BDSG)



# Signaturgesetz und -verordnung

- **Grundlage:**

Regelungen basieren auf EG-Richtlinie 1999/93/EG und setzen Vereinbarungen in nationales Recht um

- **Zweck:**

Sicherheit und Vertrauen im elektronischen Geschäftsverkehr und in der elektronischen Verwaltung

- **Inhalt:**

Gesetz

regelt verschiedene Signaturarten mit aufsteigenden Sicherheitsmaßstäben (§ 2 SigG):

- elektronische Signatur, Nr. 1
- fortgeschrittene elektronische Signatur, Nr. 2
- qualifizierte elektronische Signatur, Nr. 3



# Strafrecht



- Verabschiedung des 41. Strafrechtsänderungsgesetzes zur Bekämpfung der Computerkriminalität durch den Deutschen Bundestag im Juni 2007
- Umsetzung des Rahmenbeschlusses des Rates der Europäischen Union über Angriffe auf Informationssysteme aus dem Jahr 2005 sowie des Europarat-Übereinkommens über Computerkriminalität aus dem Jahr 2001
- Neueinführung der § 202 b und § 202 c StGB
- Änderung bzw. Ergänzung der §§ 202 a, 303 a und § 303 b StGB



# § 202 c StGB „Hacker - Paragraph“

## § 202c Vorbereiten des Ausspähens und Abfangens von Daten

„ (1) Wer eine Straftat nach § 202 a oder § 202 b vorbereitet, indem er

1. Passwörter oder sonstige Sicherungscodes, die den Zugang zu Daten (§ 202 a Abs. 2) ermöglichen, oder
2. Computerprogramme, deren Zweck die Begehung einer solchen Tat ist,

herstellt, sich oder einem anderen verschafft, verkauft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.“



## § 202 c StGB „Hacker - Paragraph“

- § 202 c StGB setzt die Vorgabe des Art. 6 Abs. 1 a des Europarat-Übereinkommens in deutsches Recht um und stellt besonders gefährliche Vorbereitungshandlungen ausdrücklich unter Strafe (“Vorfeldkriminalisierungsvorschrift”)
- Strafbarkeit für das Herstellen, Verschaffen, Verbreiten oder Zugänglichmachen von sogenannten „Hacker-Tools“
- objektiver Tatbestand ist sehr weit gefasst
- erfasst werden lediglich böswillig programmierte „Hacker-Tools“
- nicht unter die Norm fallen hingegen Programme, die ausschließlich der Abwehr von fremden Angriffen dienen



# Verfassungsrecht

- BVerfG erklärt Vorschrift des nordrhein-westfälischen Verfassungsschutzgesetz zur Online-Durchsuchung für verfassungswidrig
- Schaffung eines Grundrechts auf „**Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme**“ als Ausfluss aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG
- Schließung der Lücken der Grundrechte des Fernmeldegeheimnisses (Art. 10 GG), der Unverletzlichkeit der Wohnung (Art. 13 I GG) und des Rechts auf informationelle Selbstbestimmung (Art.2 Abs.1 i.V.m. Art.1 Abs.1 GG)



# Entscheidung „Online-Durchsuchung“



- Grundrecht ist nicht schrankenlos gewährleistet
- Eingriffe können sowohl zu präventiven als auch repressiven Zwecken gerechtfertigt sein
- **Präventives Handeln:**  
Konkrete Gefahr für überragend wichtige Rechtsgüter wie Leib, Leben, Freiheit der Person oder Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates berühren
- in der Regel vorher Anordnung durch Richter



# Entscheidung „Online-Durchsuchung“



- Existenz eines unantastbaren Kernbereichs privater Lebensgestaltung als Ausfluss der Garantie der Menschenwürde
- Einhaltung eines zweistufigen Schutzkonzepts:
  - **1. Stufe:**  
Soweit informationstechnisch und ermittlungstechnisch möglich, soll die Erhebung kernbereichsrelevanter Daten unterbleiben
  - **2. Stufe:**  
Falls Stufe 1 nicht zu realisieren, ist sicherstellen, dass erhobene kernbereichsrelevante Daten unverzüglich gelöscht werden



# Spezielle Regelungen

## Korruptionsregister

- Meldewesen
- ePass
- Digitaler Personalausweis
- usw...



# **„Rechtsentwicklung im Bereich der IT-Sicherheit“**

## **mit drei Teilprojekten**



# Gegenwärtige Rechtslage

- keine einheitlichen Regelungen bezüglich der Verteilung der Verantwortung für IT-Risiken
- Vermögensschäden verbleiben in der Regel bei den Anwendern
- Geschädigter trägt die Beweislast für die Fehlerhaftigkeit der Software, die Kausalität zwischen fehlerhaftem Produkt und Rechtsgutverletzung sowie für den Schaden
- einseitige Verteilung des Haftungsrisikos



# IT-Sicherheitshaftungsgesetz: Regelungsansatz



## Schaffung eines IT-Sicherheitshaftungsgesetzes

### Ausgestaltung:

- Einführung einheitlicher und allgemeiner Sicherheitsanforderungen in generalklauselartiger Form  
Konkretisierung durch untergesetzliche IT-Sicherheitsstandards

### Kreis der Verpflichteten:

Hersteller und kommerzielle Betreiber von IT-Anlagen

### Betroffene Sachverhalte:

- IT-Produkte, IT-Dienstleistungen und ITManagementsysteme



# IT-Sicherheitshaftungsgesetz: Vermutungswirkung



## Regelungsansatz:

- Nachweis der Sicherheitseigenschaften von Produkten und Systemen durch Zertifikate
- Vermutung der Sicherheit für denjenigen, der Sicherheitssanforderungen einhält
- Einhaltung der Sicherheitsanforderungen grundsätzlich freiwillig
- Andernfalls Beweislast bei Abweichen
- Vermutungswirkung kann ausgedehnt werden auf Zivilrecht, BDSG, § 91 Abs. 2 AktG



# IT-Sicherheitshaftungsgesetz: Anreizstruktur



## Rechtsökonomischer Ansatz:

- Setzung von Anreizen zur Schaffung von Sicherungsmaßnahmen mit effizientem Aufwand
- Anreize zur Implementierung von Schutzvorkehrungen bestehen für Personen, die im Schadensfall haften
- Verlagerung der sicherheitsrelevanten Anforderungen auf die Personen, die die Risiken am effizientesten beherrschen können (“cheapest cost avoider”)



# IT-Sicherheitshaftungsgesetz: Vorteile der Regelung



- Anhebung des IT-Sicherheitsniveaus
- Verbesserung des Nutzerschutzes durch IT-Sicherheit
- Verbesserung der Kriminalprävention durch IT-Sicherheit
- Verbesserung des Verbraucherschutzes durch IT-Sicherheit und Stärkung der Rechtsposition
- Gewinn für die Rechtssicherheit



# Vielen Dank für Ihre Aufmerksamkeit!



Bundesamt für Sicherheit in der  
Informationstechnik (BSI)

Horst Samsel  
Godesberger Allee 185-189  
53175 Bonn

Tel: +49 (0)22899-9582-5800  
Fax: +49 (0)22899-9582-105800

[horst.samsel@bsi.bund.de](mailto:horst.samsel@bsi.bund.de)  
[www.bsi.bund.de](http://www.bsi.bund.de)  
[www.bsi-fuer-buerger.de](http://www.bsi-fuer-buerger.de)

