



# **Gefährdung der Informations- und Kommunikationstechnik in Deutschland**

**19. Juni 2008**

Dr. Markus Dürig  
Referatsleiter IT 3 –  
„Sicherheit in der Informationstechnik“  
Bundesministerium des Innern



# Bedrohungslage der Informationsinfrastrukturen (1)

## ■ **Quantität** der Bedrohungen

- Vervielfachung der Zahl von Sicherheitslücken in IT-Produkten
- Vervielfachung der bekannten bösartigen Programme (Viren, Würmer, Trojaner)

## ■ **Qualität** der Bedrohung

- Einschleichen und Wirkung der bösartigen Programme ohne Zutun des Nutzers
- „Schnell“, hoch entwickelt, zielgerichtet, kaum feststellbar



# Bedrohungslage der Informationsinfrastrukturen (2)

## ■ **Veränderte Täterstrukturen**

- Trend zur arbeitsteiliger Kriminalität
- Das Opfer als Mittäter (z.B. durch Bot-Netze)

## ■ **Veränderte Motive**

- 2007 als Ende der Ära nicht kommerzieller Schadprogramme
- Gezielte Angriffe auf IT wichtiger Infrastrukturen möglich
- Gezielte Wirtschaftsspionage über das Internet





# Bedrohungslage – Beispiel: Cyber-Angriff

## Aktuelles Beispiel Estland:

- Distributed Denial-of-Service Angriffe legten die Internet Seiten der estnischen Regierung und Banken lahm
  - Email Accounts von Regierungsmitarbeitern wurden mit Mails bombardiert und „gehackt“.
- 
- Umfangreicher Angriff (Dauer und Anfragevolumen)
  - Internetverkehr zw. Estland und das Ausland musste zeitweise unterbunden werden
  - Zahlungsverkehr, Krankenhäuser, Energieversorgungssysteme, Notrufnummern wurden stark beeinträchtigt



## Bedrohungslage – Beispiel: Überlastung E-Mail-Eingang

- Internetseite stellt Möglichkeit zum Versand elektronischer Petition zur Verfügung (z.B. „Hürriyet“ am 20. Februar 2008)
- massenhafte Nutzung verursacht binnen weniger Minuten über 9.000 E-Mail-Eingänge im zentralen Postfach BMI
- Bearbeitung dieser Eingangsmenge praktisch nicht möglich
- Durch schnelle Reaktion konnte der Nachrichteneingang nach ca. 1 Std. normalisiert werden.

- Ähnliche Vorfälle sind jeder Zeit möglich
- Strafbarkeit liegt nicht vor
- Frühzeitige Erkennung und wirksame Gegenmaßnahmen notwendig!



# Gemeinsame Verantwortung für IT-Sicherheit

- Sicherheit ist ein Grundbedürfnis der Menschen

## IT-Sicherheit

- als Verantwortung des Staates
- als Verantwortung der (IT-) Wirtschaft
- als Verantwortung der Bürger



IT-Sicherheit kann nur gewährleistet sein, wenn alle Gruppen ihre Verantwortung wahrnehmen



Nationaler Plan  
zum Schutz der  
Informationsinfrastrukturen  
(NPSI)



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

# Nationaler Plan zum Schutz der Informationsinfrastrukturen

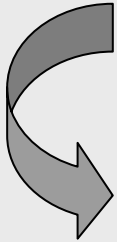
- Nationale Dachstrategie zu IT-Sicherheit
- Vom Bundeskabinett verabschiedet im Sommer 2005
- Koalitionsvereinbarung beauftragt BMI zur Umsetzung des NPSI in dieser Legislaturperiode



## Wie wird der NPSI umgesetzt?

# Nationaler Plan

zum Schutz der  
Informationsinfrastrukturen



# Nationaler Plan

Umsetzungsplan Bund



# Nationaler Plan

Umsetzungsplan KRITIS





# Herzlichen Dank für Ihre Aufmerksamkeit

Dr. Markus Dürig  
Referatsleiter IT 3 – Sicherheit in der Informationstechnik  
it3@bmi.bund.de