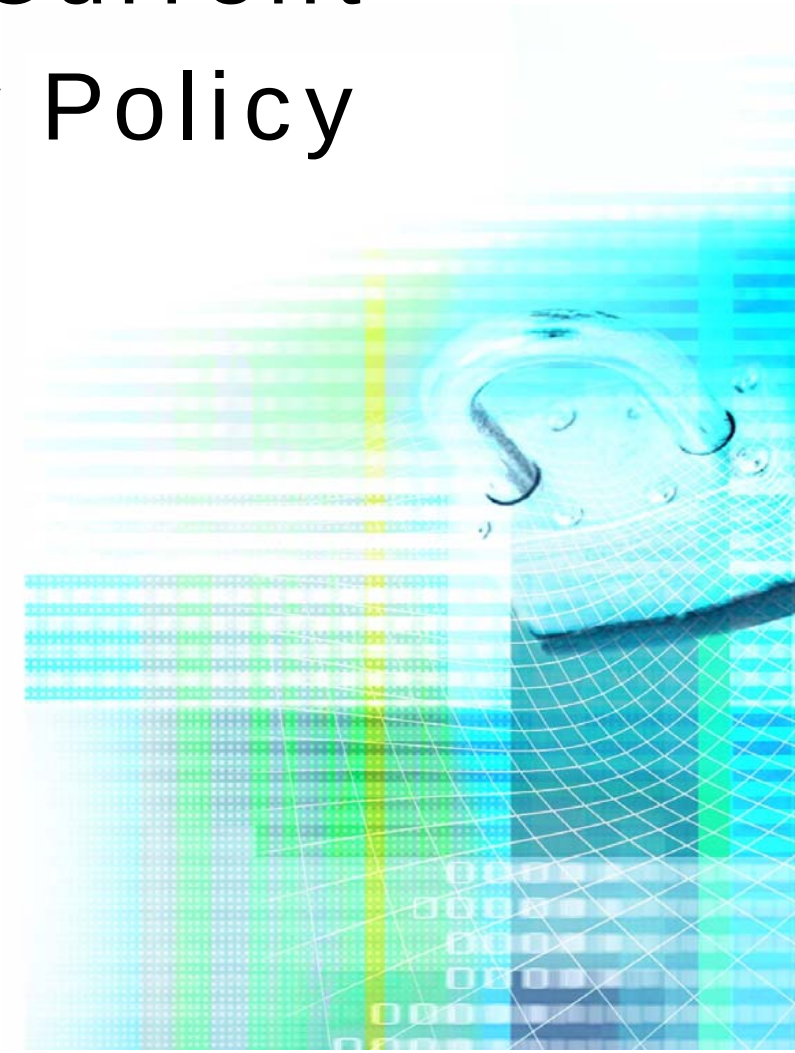
Contradictions in Current European Security Policy

Dr. Jan K. Koecher
Company Lawyer
DFN-CERT Services GmbH
koecher@dfn-cert.de



Contradictions?

- **Objective 1:**
  - Promotion of IT-security
    - Protection of critical infrastructures
    - Protection of networks
    - Protection of the integrity of IT-systems
- **Objective 2:**
  - Public security
    - IT-based measures
      - Telecommunications data retention
      - Online search on IT-Systems

Promotion of IT-Security

- **Requirements of international law:**
  - Convention of Cybercrime, signed 23.11.2001 by member states of the Council of Europe
  - Also signed by the non-member states:
    - Japan
    - United States of America
    - Canada
    - South Africa
  - Available:
    http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

Cybercrime Convention

- **States are obliged to ensure the punishability of:**
  - Illegal access to a computer system (Art. 2)
  - Illegal interception of non public transmissions of computer data (Art. 3)
  - Data and system interference by inputting, transmitting, damaging, deleting, altering or surpressing computer data without right (Art. 4 and 5)

Art. 6 is difficult

- **Article 6 – Misuse of devices**
- **States are obliged**
  - to establish as criminal offences, when committed intentionally and without right:
    - the production, sale, procurement for use, import, distribution or otherwise making available of:
      - a device, designed or adapted primarily for the purpose of committing offences (Art. 2 through 5)
      - a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed
    - with intent that it will be used for the purpose of committing offences Art. 2 through 5

Exception in Art. 6

- **IT-security aspects:**
  - This article shall not be interpreted as imposing criminal liability where the production..., or otherwise making available or possession
    - ➔ is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the **authorised testing or protection of a computer system**.

German implementation

- **Difference between:**
  - Hacker tools
    - Important for the qualification:
      - → Intended use: committing offences
  - Dual use tools
    - Not intended for committing offences, but applicable for misuse
      - Informations about zero-day exploits?
      - Tools for account probes?
      - → ??? - Intent of the user!
- **Not implemented: Exception Art. 6, IT-sec.**

Problems in practice

- **Punishability of pentesting?**
  - Solutions for the problem:
    - Prior written consent of the owner
    - Documentation
- **Punishability of password security checks?**
  - Solutions for the problem:
    - Stipulation in the provider agreement

    or
    - Acceptance by the user

Problems in practice

- **Punishability of exchange of informations about vulnerabilities?**
  - No punishability if the aim of the activity is the protection of computer systems (exception)
  - Indicated by:
    - Profession (IT-security professionals)
    - Objectives (white hat)
  - Additional recommendation:
    - Agreement between the parties of information exchange > Only use for legal purposes!

Public Security – Telco-data

- **Telecommunications data retention**
  - Stated by the Directive 2006/24/EC
    - Also planned in the USA
  - Obligation for access providers:
    - Collecting data about telecommunication (phone, internet, e-mail)
      - Persons, time, ip-adresses...
      - Except the content of conversations and communications
    - Storage time at least 6 month
    - On demand: forwarding to security authorities
    - No use for own (providers) purposes allowed

Pros / Cons of data retention

- **Pros**
  - Additional chance of identifying criminal offenders in the Internet
  - Chance to find and monitor potential terrorists
- **Cons**
  - Applys on the communication data of nearly all citizens
    - Costs / effectiveness?
    - Negative effects for civil rights

IT-security and data retention

- **Vast amounts of stored data in database**
  - Risk of fraudulent use by the providers
  - Attractive target for attacks
    - Risk: law contains no unique guidelines for security concepts of data storage
- **Alternative solution:**
  - Storage by a central institution of the security authorities
  - Logging of demands
  - Supervision by parliament (checks and balances)

Secret infiltration of IT-systems

- **Part of the anti-terrorism legislation in:**
  - Germany
  - Latvia
  - Slowenia

- **Secret infiltration on IT-systems by authorised security agencies**
  - Live search and observation
  - Without house search and physical control
  - Without knowledge of the owner

IT-security aspects

- **Problem: implementation**
- **Necessary: backdoor penetration that allows the unnoticed access to data files**
  - Accomplished by installation of backdoor software
    - By specially designed vulnerabilities
    - By using specially designed backdoors in commercial software
    - By using not published zero-day exploits

Contradiction:

- **Objective of promotion of IT-Security**

and

- **Secret infiltration: Governmental interest in vulnerability of IT-systems**
  - Danger of misuse by criminals for cyberattacks!
    - Backdoors in commercial software
    - Informations about unpublished zero-day exploits
- **Solutions:**
    - Manual installation
    - Special designed vulnerabilities

Conclusions

- **Contradictions between the objectives**
  - IT-security <> public security
    - Solution: more considerateness by legislator
- **Contradictions inside the objective IT-security**
  - Pentesting
  - Password security checks
  - Informations about vulnerabilities
    - Solution: measures to mitigate the risk of punishability

Thanks for your attention!

Questions?

Dr. Jan K. Koecher, Company Lawyer DFN-CERT
WWW: https://www.dfn-cert.de/
Mail: koecher@dfn-cert.de