GLOBAL INDUSTRY CLUB

CeBIT

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

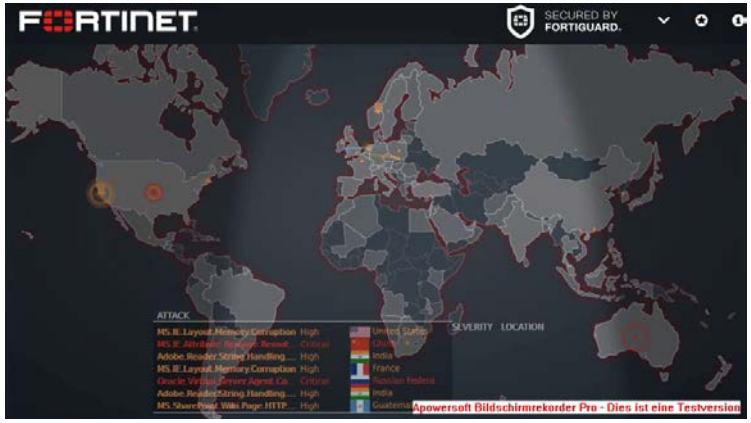
EUROPEAN CYBER SECURITY CONFERENCE

Cyber threats of tomorrow need new approaches and collaborations

Helmut Leopold

Head of Digital Safety & Security Department

AIT Austrian Institute of Technology



Hannover, March 14th, 2016

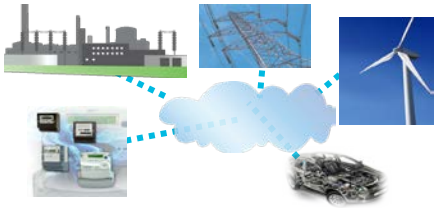
(v0.5)

ICT Platforms become Critical Infrastructures of our Society

Connected Cars

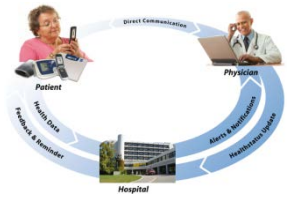
- 60% of all innovation by electronics
- Intelligent traffic-management to save CO2 and to increase traffic efficiency

Connected Utility



- Intelligent energy production, distribution and use - renewable energy – smart grid
- Energy management at home- smart home
- New energy storage

Connected Patients



- Closed loop healthcare - Telemedicine for new widespread diseases – diabetes, cardic insufficiency, overweight
- Prevention and care; Lifestyle management

Industry 4.0

- Sensor networks for production
- Cloud services
- Real-time information

Smart Digital City
Smart Environment
Public Safety

- Environmental sensors
- Smart sensors for public security
- Citizen information systems, eGovernment
- Citizen contribution

Internet of Things (IoT) – Cyber Physical Systems (CPS)

Essential ICT-Security Problem

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY

420.000 Virus signatures (malware) per day !!

Increased system complexity, dynamic behaviour → decreasing system understanding

Increased complexity of the attacks → APT Advanced Persistent Threats

The end of classical security protection.

06.05.2014 | 11:31 | (DiePresse.com) - Symantec/Norton

Increased networking and use of ICT increases the dependency → critical Infrastructure (CI)

Awareness
Market added value + cost for enterprises and society

No 100% security
Risk management

Increase the resilience
New methods in order to minimize the negative effects - encryption, Privacy&Security by Design, CAIS, CIIS

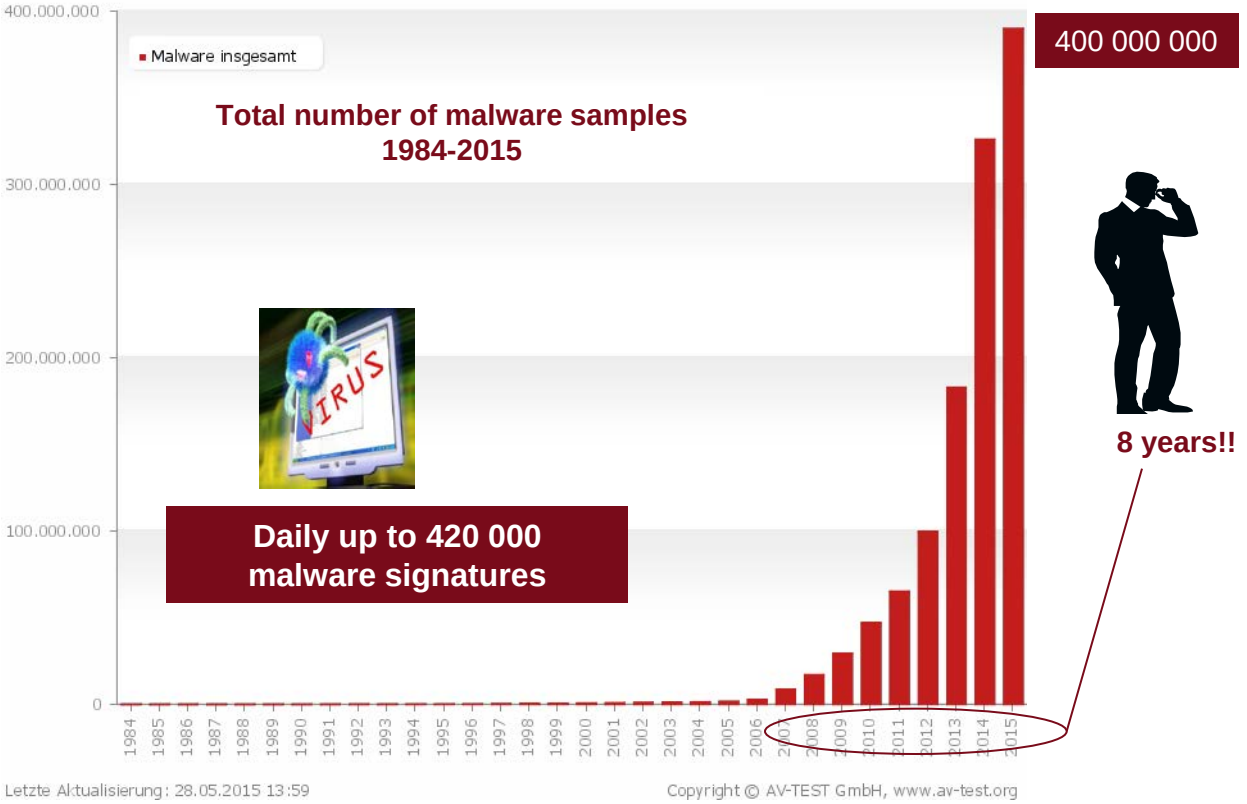
???

To allow to prohibit (Perimeter security)

Millennials Patient Cars Home Energy Environment

smart systems - M2M, CPS, IoT

Cyber Crime is in its Dimension a very young Discipline



Dimensions of „Bot networks“

- Mariposa: 12 Mio PC‘s
- Conficker: 10 Mio PC‘s
- Zeus: 3,6 Mio PC‘s

Ofcom, UK, 2014

1,658 cyber attack attempts

October - November

CERT Austria, 2014

16.000 cases – security risk

72.000 support actions for enterprises

QUELLEN:

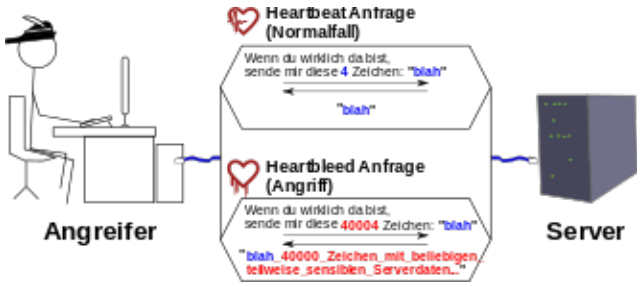
- http://www.av-test.org/de/statistiken/malware/
- http://www.trendmicro.de/media/ds/anti-malware-nss-labs-datasheet-de.pdf

Many different attack vectors

Technical vulnerabilities + **Human behaviour** + **Attacks in several steps** + **Space & time**

- **Human user - Usability**
  - Simple/well known pass words
  - USB Stick
  - Use of an email of a well known colleague or even from the boss – „CEO Fraud“
- **Phishing, Watering Hole Attacks**
  - E-mails, „*drive-by-infection*“ (manipulated Website which is waiting for a visit), online advertising „malvertising“
- **SW-Failures/Design Failures - „Vulnerabilities“**
  - Zero-Day Exploits (e.g. *heartbleed 2014)*
- **„failure“ in operation**
  - No or low level security pass words
  - Missing SW-Updates (*zero-day exploits*)
  - „Safety – Security problem“
- **Special systems**
  - Manipulated HW+SW *(„Backdoors“)*

Pishing: Spam emails for input of pers. information



90% of attacks on well known vulnerabilities, 2015 Verizon Data Breach Report

Username: admin
Pass word: admin

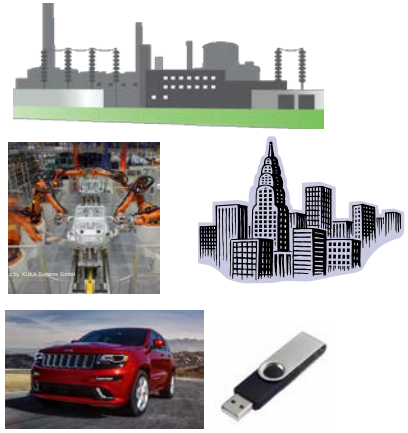
98% of Websites have vulnerabilities, it governance, 11. 6.2015

Search engines
- scan of the Internet

CloudCracker

Effectiveness – attackers versus defender

attacker:
Only 7 days in order to exploit vulnerabilities
(down to 1 day)



defender:
176 days for organisations in order to close known vulnerabilities
(up to „never“)
„Safety – Security Industry problem“

Source: it governance, Businesses dangerously slow to react to vulnerabilities, June 30, 2015 by Neil Ford.
NopSec’s 2015 State of Vulnerability Risk Management report has found that it takes cyber criminals just 7 days to successfully exploit a vulnerability. It takes 176 days for organisations to address known vulnerabilities and you have a recipe for disaster.

SW-Vulnerabilities – Business Issues

„Stagefright 2.0“ Vulnerability, 10.2015 (1)

- 1,4 Billion Android Smart phones
- Possibilities of attacks via music- and Video files (MPEG3 MPEG4 Files)

„…Bisher gibt es für das von Zimperium offengelegte Angriffsszenario noch keinen Patch. Weder von Google selbst, noch von anderen Herstellern. Ob Google im Rahmen seines monatlichen Patchday-Programms schnell reagieren wird, bleibt abzuwarten….“

- 87% of all Android Phones operate with SW with known vulnerabilities – due to missing patch management (2)

Android issue: HW - OS dependancy + complexity of the OS variations + economy of scale

Quellen: (1) www.inside-handy.de, (2) Studie Uni Cambridge http://androidvulnerabilities.org/press/2015-10-18

Advanced Persistent Threats (APT)

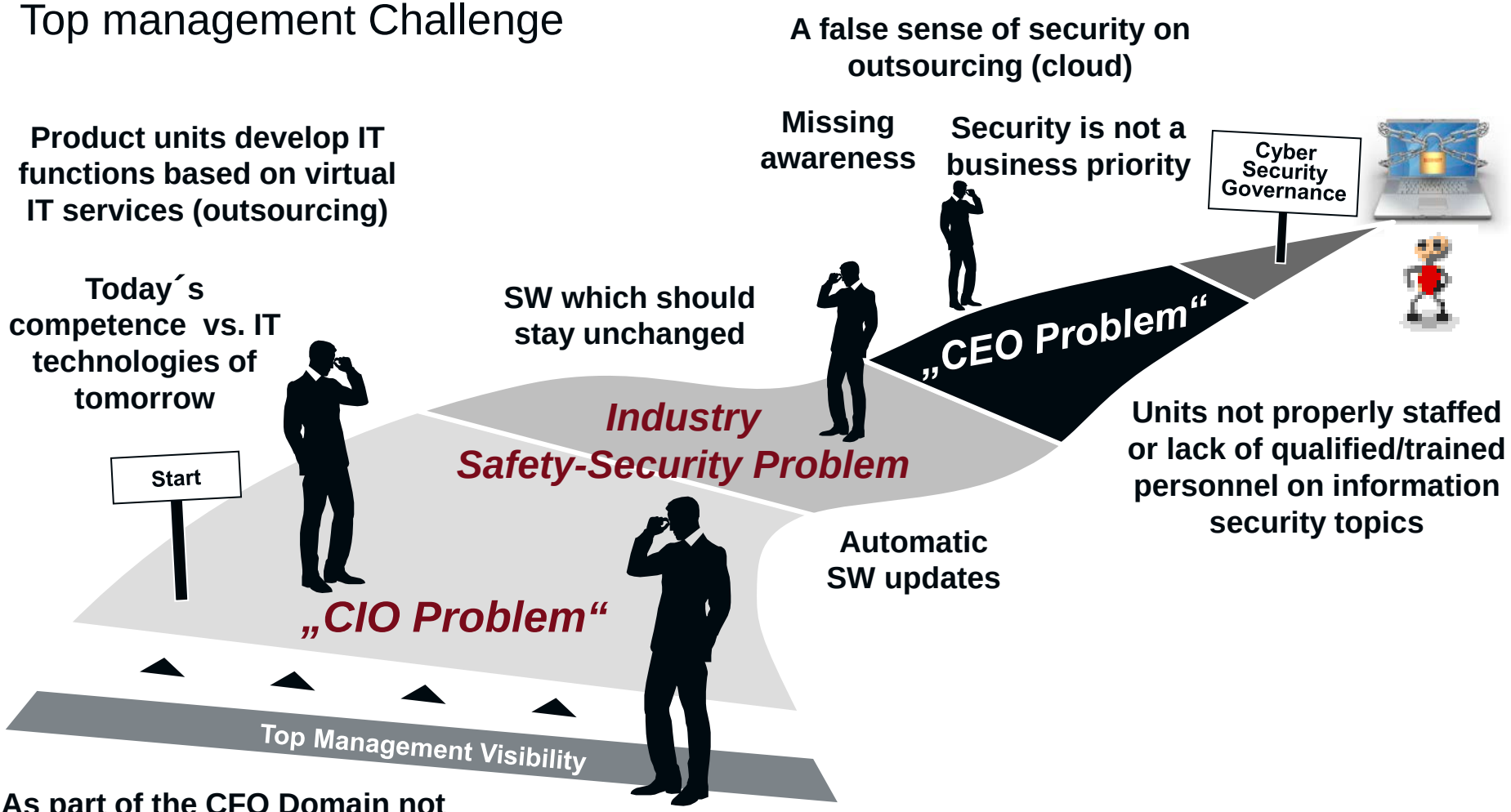
targeted attacks (“spear-phishing”) based on several steps of kind, time and space

1. **Social Engineering**
   - get access
2. **Initial Intrusion - exploit weaknesses**
   - configuration error, SW vulnerability, stolen login information, etc.
3. **Expand Access - strengthen foothold**
   - stays invisible in the system
   - access control system from within the trusted environment
4. **Gain Control**
   - send fabricated control messages

Attacks over weeks or months.
Attack well-defined for a dedicated purpose;
Basically no means to detect the attack.

Cyber Security is not at all just a technical problem

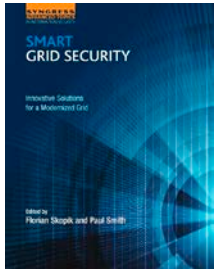
Top management Challenge



Next Gen ICT Security Research programme

AUSTRIAN INSTITUTE OF TECHNOLOGY

- Architectures, Processes for Privacy & Security for future IT systems
- IT Cloud systems
- Critical infrastructures (smart grid, Industry control systems)

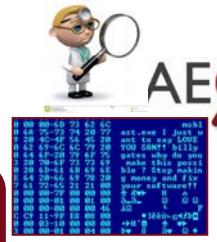


Privacy & Security by Design

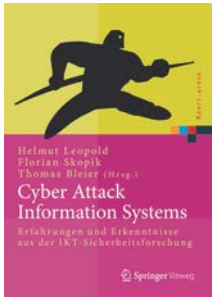
encryption

CAIS

Cyber Attack Information System



AIT patent



- Detection of the unknown unknown
- Self-learning systems
- Big Data Analytics

CIIS

Cyber Incident Information Sharing

- Trustful & secure information exchange – machine and human readable
- Processes, structures
- Cyber Situational Awareness

resilience

Risk Management

- Methodologies, models, tools
- Critical infrastructures
- National security
- Basics for specification of minimum standards for CI

IT

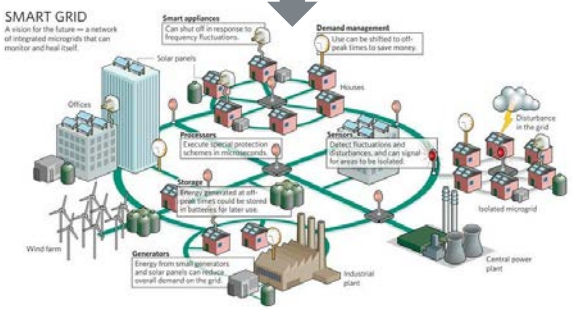
Basic protection

- Firewall, virus scan (allow/prohibit)
- Training of employees
- Processes, Info-classification
- Penetration Tests, DPI
- Vulnerability Management, SIEM
- CISO-"CEO", CERT, ISO 2700x

KMU Problem!

Security is a societal issue

AUSTRIAN INSTITUTE OF TECHNOLOGY






Digital Transport	Smart City	Connected Cars	Industry 4.0	Smart grid	eHealth

Availability of national skills, technologies

Cooperation of all stake holders on the market to achieve a critical mass of competence!

AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

Thank you for your attention!

Helmut Leopold
Head of Digital Safety & Security Department
helmut.leopold@ait.ac.at

AIT Austrian Institute of Technology