AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

Critical Infrastructure Cyber Security

Andrea Nowak
Head of Business Unit Information Management
Deputy Head of Safety & Security Department
AIT Austrian Institute of Technology GmbH

Cyber Security Incidents 2013 …

PANASONIC **SPARKASSE** **THYSSENKRUPP** **AFCLC**

RENAULT **NASA** **APPLE** **BURGER KING**

TURKISH GOVERNMENT **MICROSOFT** **NBC** **ADOBE**

US GOVERNMENT **VODAFONE GERMANY** **BANKS SOUTH AFICA**

NEW YORK TIMES **AIRPORT ISTANBUL** **POLICE SOUTH AFRICA**

US ENERGY MINISTRY **PEUGEOT** **TURKISH MINISTRY OF FINANCE**

WASHINGTON POST **EGYPT GOVERNMENT** **FERRARI**

The provider of the well-known antivirus protection Norton evokes the end of classic anti-virus solutions . New methods of attackers require new measures.
06.05.2014 | 11:31 | (DiePresse.com) - Symantec/Norton

QUELLE: www.qgroup.de/galerie

The problem…

- The complexity of ICT systems is increasing
  - Landing on the moon with 7.500 Lines of Code
  - Today: F-35 fighter jet: 5,7 Mio; Boeing 787: 6,5 Mio; Mercedes S-Class: 20 Mio; Chevrolet Volt: 100 Mio.
- Systems are getting more and more interconnected
  - Internet-of-Things, Always-on, Pervasive Computing
  - M2M (Machine-to-Machine) Communication
  - Virtual Infrastrucutures (Cloud), etc.
- Industry trend towards open network architectures
  - Open protocols (e.g. IP)
  - Increased number of „third parties“
- The dependency on ICT systems is increasing
  - Smart Grid, Smart Home, Smart City, Smart Phone
  - eGovernment, eCommerce, eHealth, eMobility

Increased Number of Vulnerabilities

Increased Risk

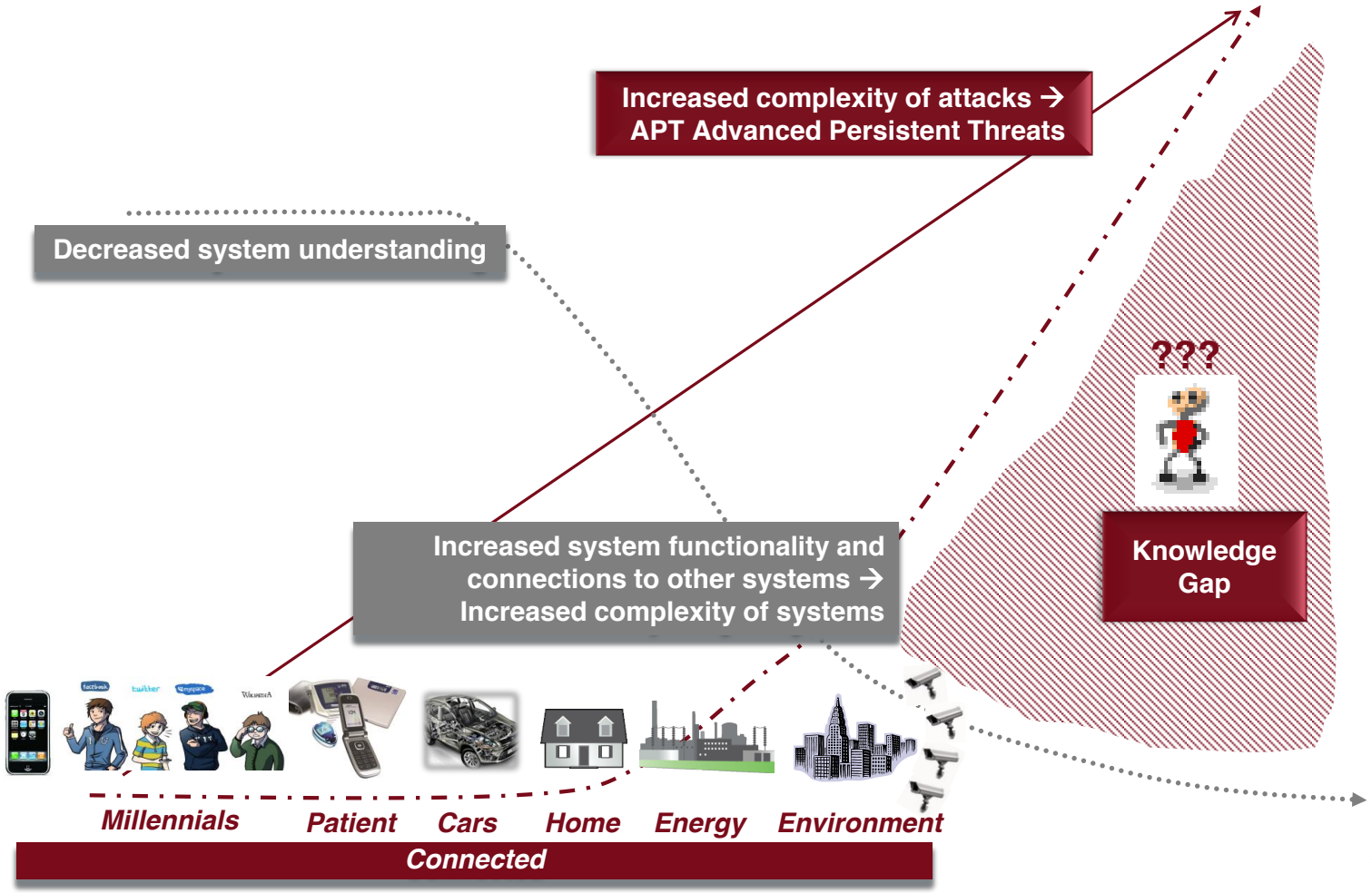
Increased Impact

New IT trends don‘t stop at critical infrastructure IT

- Cloud Computing
- Bring your own device
- Consumerization
- Social Networks und Social Media

Bild: http://oldcomputers.net/pics/newton-right.jpg

The knowledge gap is increasing…

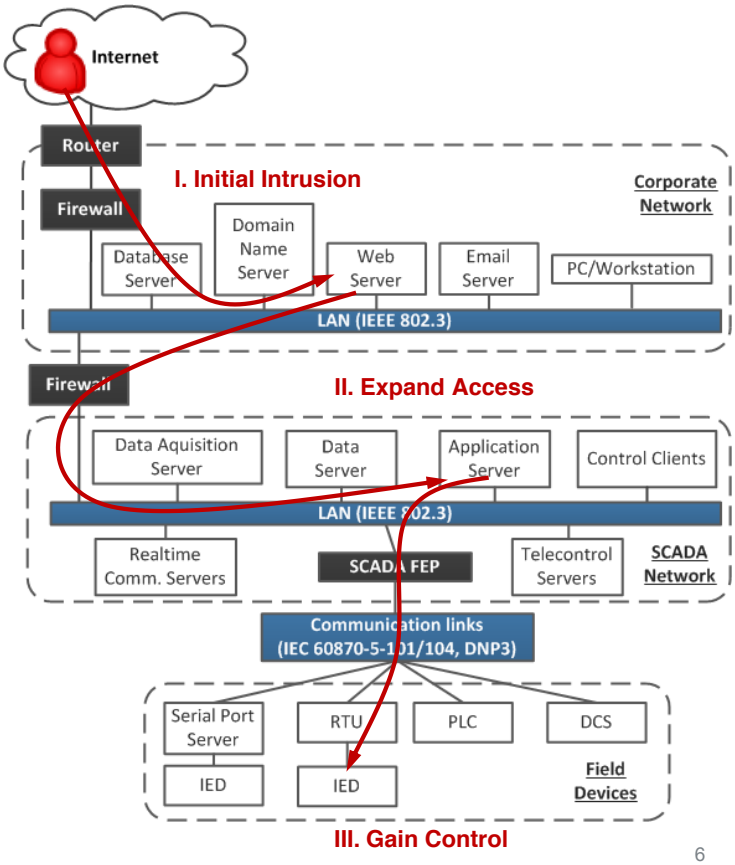


Multistage attacks (APT) against CI targets…

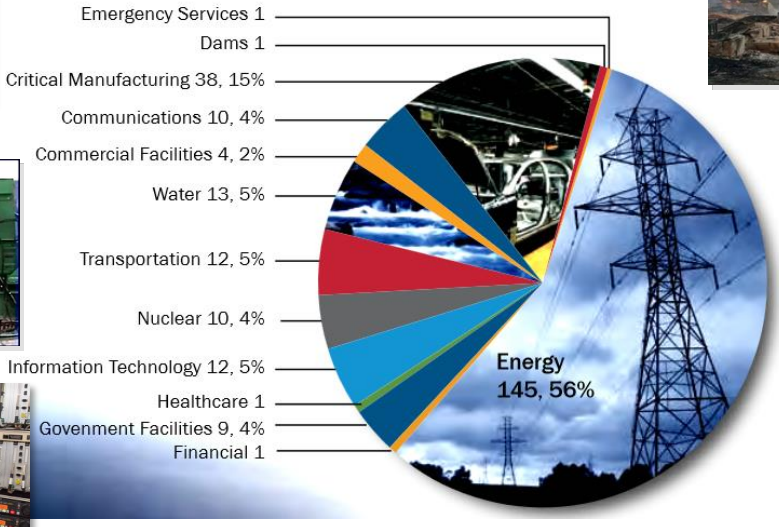
I. Initial Intrusion
- Exploit weaknesses (configuration error, SW vulnerability (e.g., RDP))

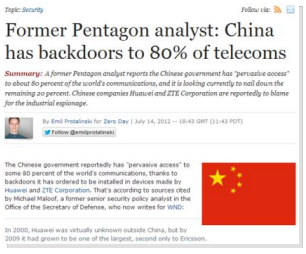
II. Expand Access and Strengthen Foothold
- Access control system from within the trusted environment

III. Gain Control
- Send fabricated control messages



Industrial Control System Incidents

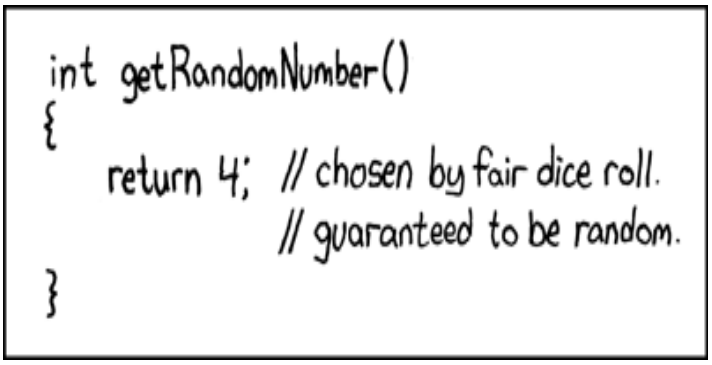




Industrial Control System Incidents (ICS) the US ICS-CERT responded to in FY-13,
Source: ICS-CERT

Security is a shared responsibility…

- Critical Infrastructures are typically a „System of Systems“
- Creating secure components is **not enough**
- Secure **implementation** and **operation** is key
- Reliance on security of specific components
- Responsibility for specific security aspects needs to be defined
- Private vs. Industrial vs. „Virtual“ Participants



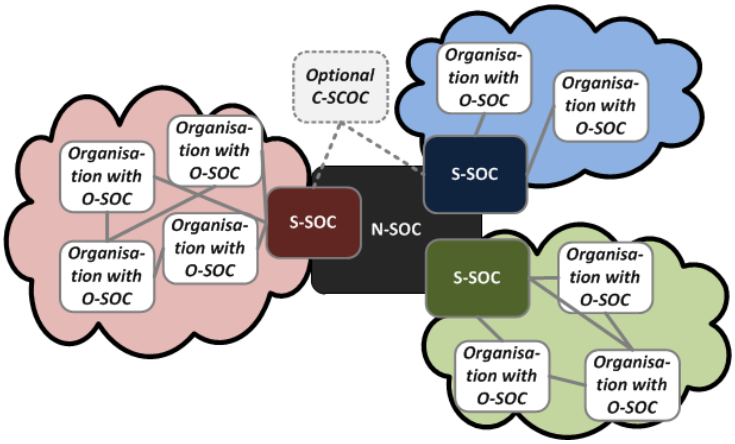
Prevention, detection and reaction…

- Prevention is useless without detection and reaction!
- System Complexity
- Responsibility vs. Competence
- User awareness
- Securing devices in „hostile environments“
- Situational awarenss
- Information Sharing, Reporting

Efficient information sharing

- Hybrid models are necessary– peer-to-peer and hierarchical
  - Enhances trust between organizations
  - Decide about data sharing **inside** of organizations
  - Still for CI national organizations need to have situational awareness

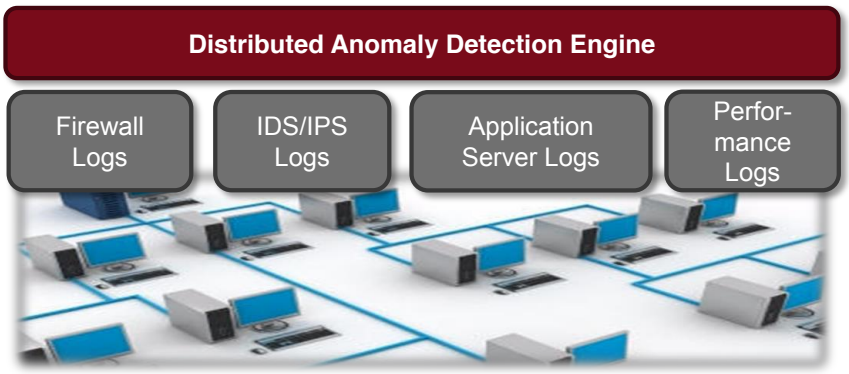
- Security Operation Centers (SOCs)
  - Organizational Level
  - Sectoral Level
  - Cross-Sectoral Level
  - National and European Level



Early detection of attacks

- (Future) attacks are complex and coordinated
  - Single pieces often below detection threshold
  - Monitoring single systems is not enough
  - Attacks are not only on the technical level

- Additional mechanisms are necessary to detect attacks
  - Detect coordinated attacks against multiple targets
  - Dected attacks using multiple attack vectors



Critical Infrastructure Security Research @ AIT

Research Topics:

- Risk analysis and management for Critical Infrastructures
- Secure architectures for resilient ICT systems in CI
- Security Lifecycle Tools
- Situational awareness – anomaly detection, incident information sharing

Selected reference projects:

- **SPARKS** | FP7 SEC (coord) | Smart Grid Protection against Cyber Attacks
- **PRECYSE** | EU FP7 SEC | Prevention, protection and reaction to cyberattacks to critical infrastructures
- **HYRIM** | FP7 SEC (coord) | Hybrid Risk-Management for Utility Providers
- **ECOSSIAN** | FP7 SEC | European Control System Security Incident Analysis Network
- **CAIS** | KIRAS| Cyber Attack Information System
- **CIIS** | KIRAS| Cyber Incident Information Sharing

Selected research partners:

AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

AIT Austrian Institute of Technology

your ingenious partner

Andrea Nowak
Head of Business Unit Information Management
Deputy Head of Safety & Security Department
andrea.nowak@ait.ac.at | +43 664 6207703 | www.ait.ac.at