How Sophisticated Penetration Testers Get Through the Defenses

Amsterdam, 08 September 2008

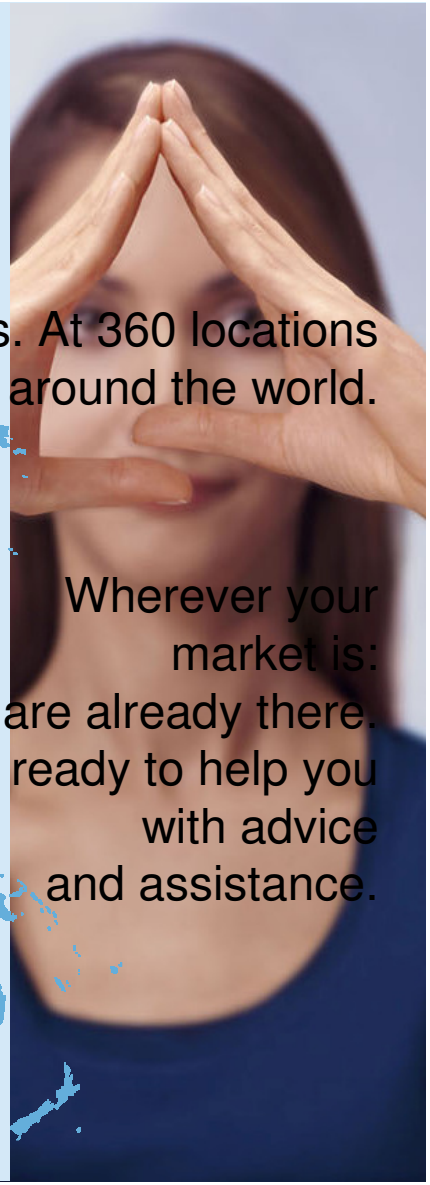
TÜVRheinland®
Precisely Right.

Precisely Right. Safe and sound.
And a clear competitive edge.

We:
Advise.
Develop.
Facilitate.
Inspect.
Certify.

Precisely Right.
For you.

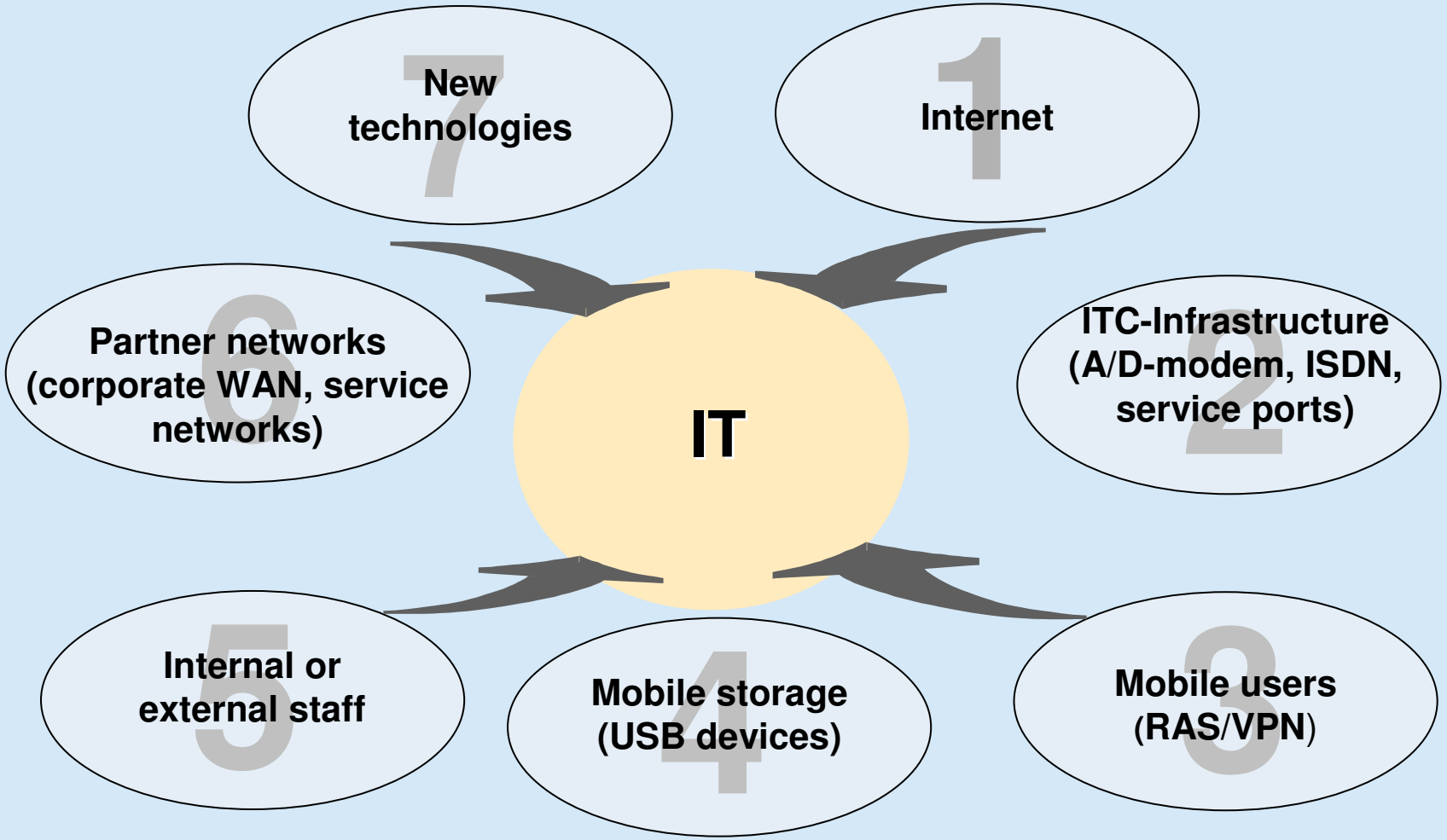
79 associated companies overseas. At 360 locations in 62 countries around the world.



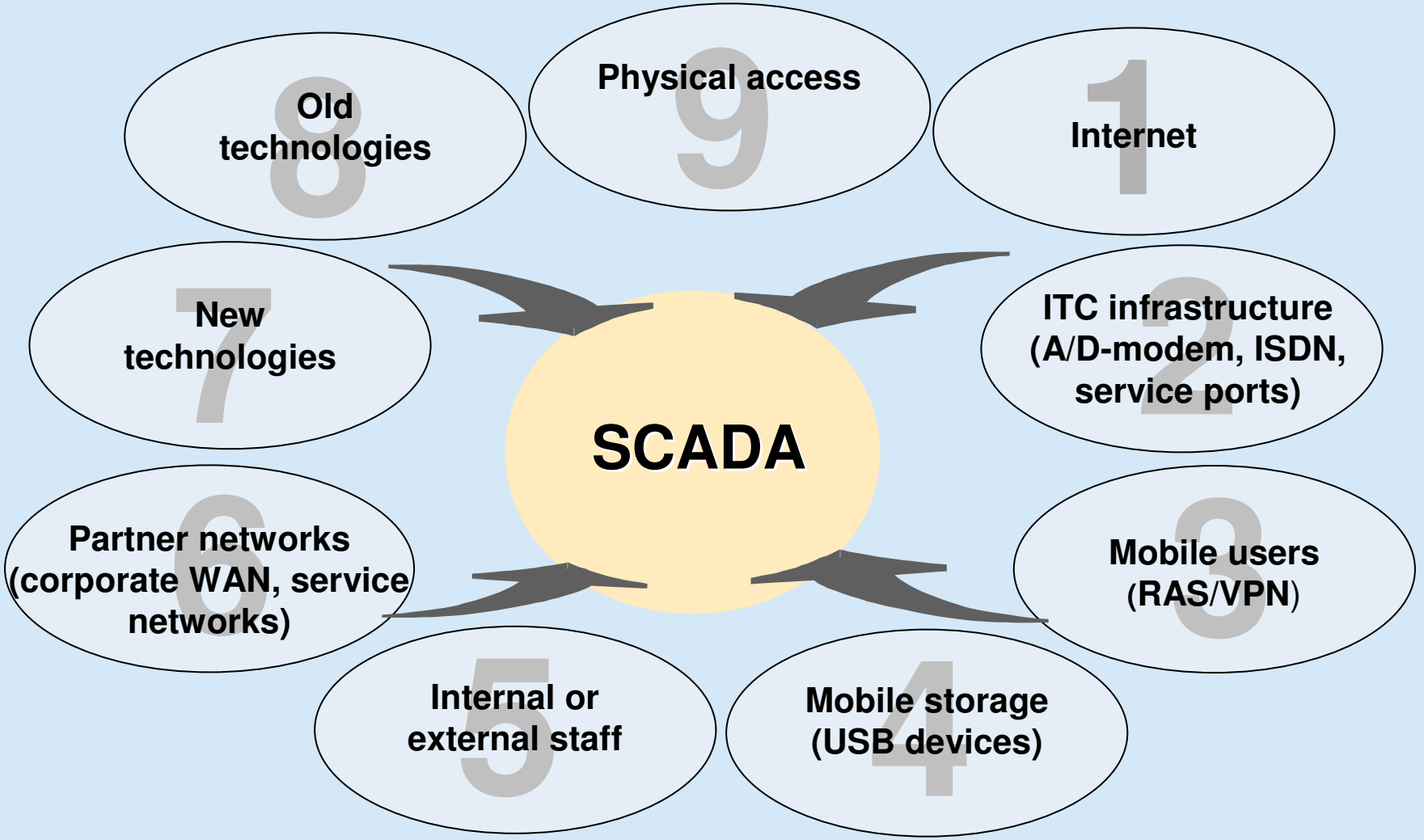
Wherever your market is:
we are already there.
And ready to help you with advice and assistance.

„Traditional“ ways

to get through the defenses



Which of these apply to SCADA?



Focus on some examples
Access from not trustworthy networks

- No or weak firewalls
  - Insufficient access controls
  - Too much communication allowed
    - Generic sources and destinations
    - Unnecessary ports
    - Forgotten protocols (e.g. IPX)

- Explicitly allowed communication
  - Web applications
    - Used to display information in office networks
    - Used as interface to corporate, partner or regulatory authority networks
  - Tunnels or jumping into other networks
    - Resolution of public DNS records, ICMP

Focus on some examples
Insecure protocols

- Serial or analog protocols ported to IP
- Proprietary protocols without authentication and encryption
  - New standard: IEC 61850

- Insecure data transfer protocols
  - http, ftp, nfs, SMTP (mail), syslog, SNMP, …
- Insecure remote control protocols
  - SNMP, telnet, X11, SSH, …
- Ineffective encryption

- Radio communications
  - Wireless LAN, Bluetooth, ZigBee, …

Focus on some examples
Physical access

- External & internal service technicians
  - Service laptops
    - Direct access to SCADA networks
    - Insufficient policies
  - Mobile storage
    - USB U3 flash drives
- Interfaces in the field
  - Easy access to sensors or field busses
    - Security vulnerabilities in processing software
  - Easy access to IP networks
    - Routers in remote stations
- Access to the facilities

What it all comes down to:
Organization, procedures and processes

- High awareness for safety but little or **no awareness for security**
  - Threats are neither known nor dealt with
  - People hardly know that IT is involved
  - Frequent excuse: “Border security”

- Insufficient processes and policies
  - Undefined responsibilities
  - No information security management
  - Policies apply to office communications
  - Processes are not adapted to special needs
  - Policies are not in line with other “traditional” policies

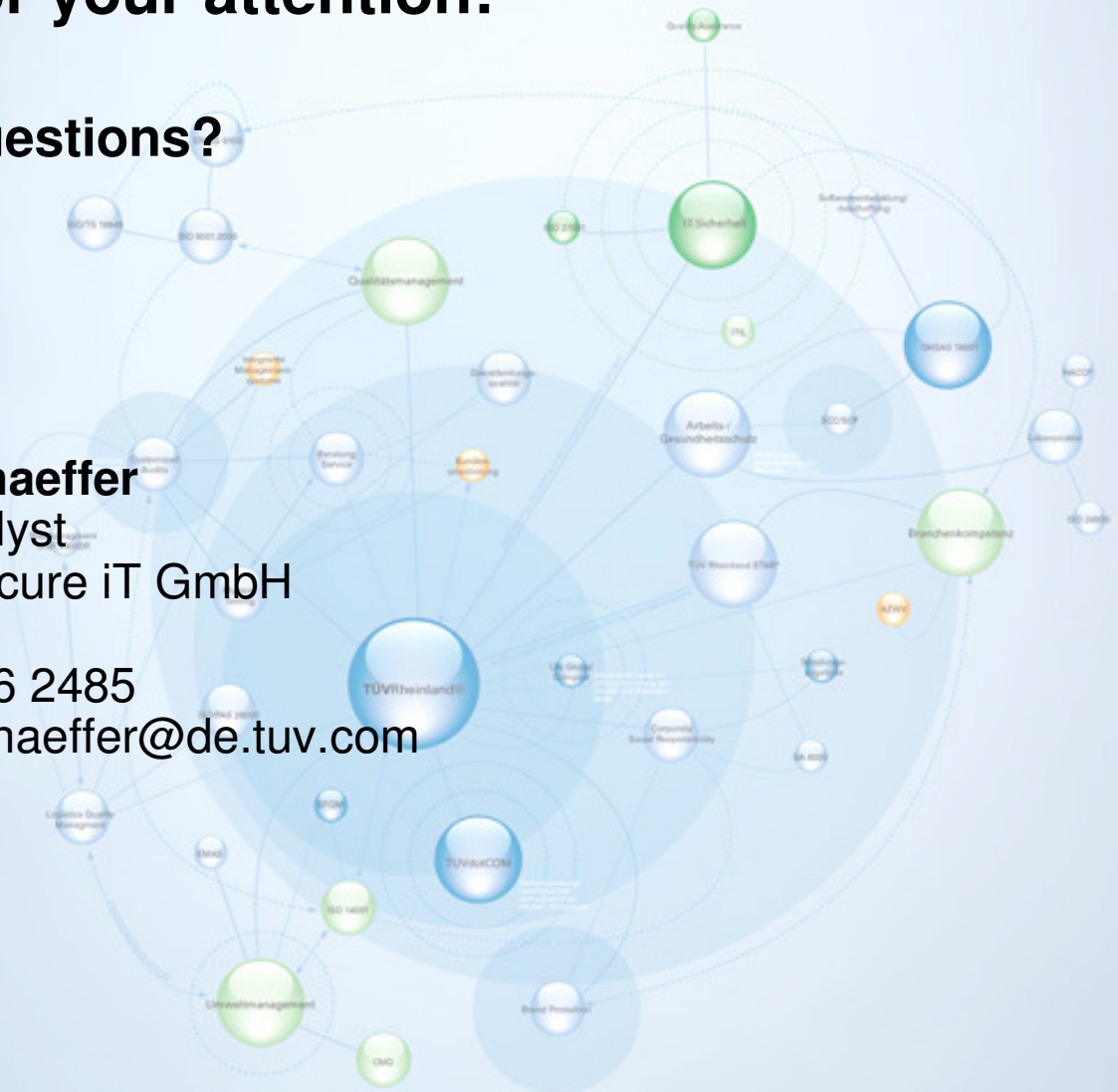
- No consistent, internationally acknowledged standard

Outlook
Duties and challenges

- Building awareness
  - Workshops and trainings
  - Information exchange with vendors and suppliers
- Development of an international standard
  - Information security management for SCADA
  - Technical requirements
  - Implementation guidelines and best practices
  - Templates for policies and processes
- Audits, assessments, reviews and penetration tests

Thank you for your attention!

Do you have questions?



Philippe A. R. Schaeffer
Chief Security Analyst
TÜV Rheinland Secure iT GmbH

Phone +49 221 806 2485
Email Philippe.Schaeffer@de.tuv.com