Federal Office
for Information Security

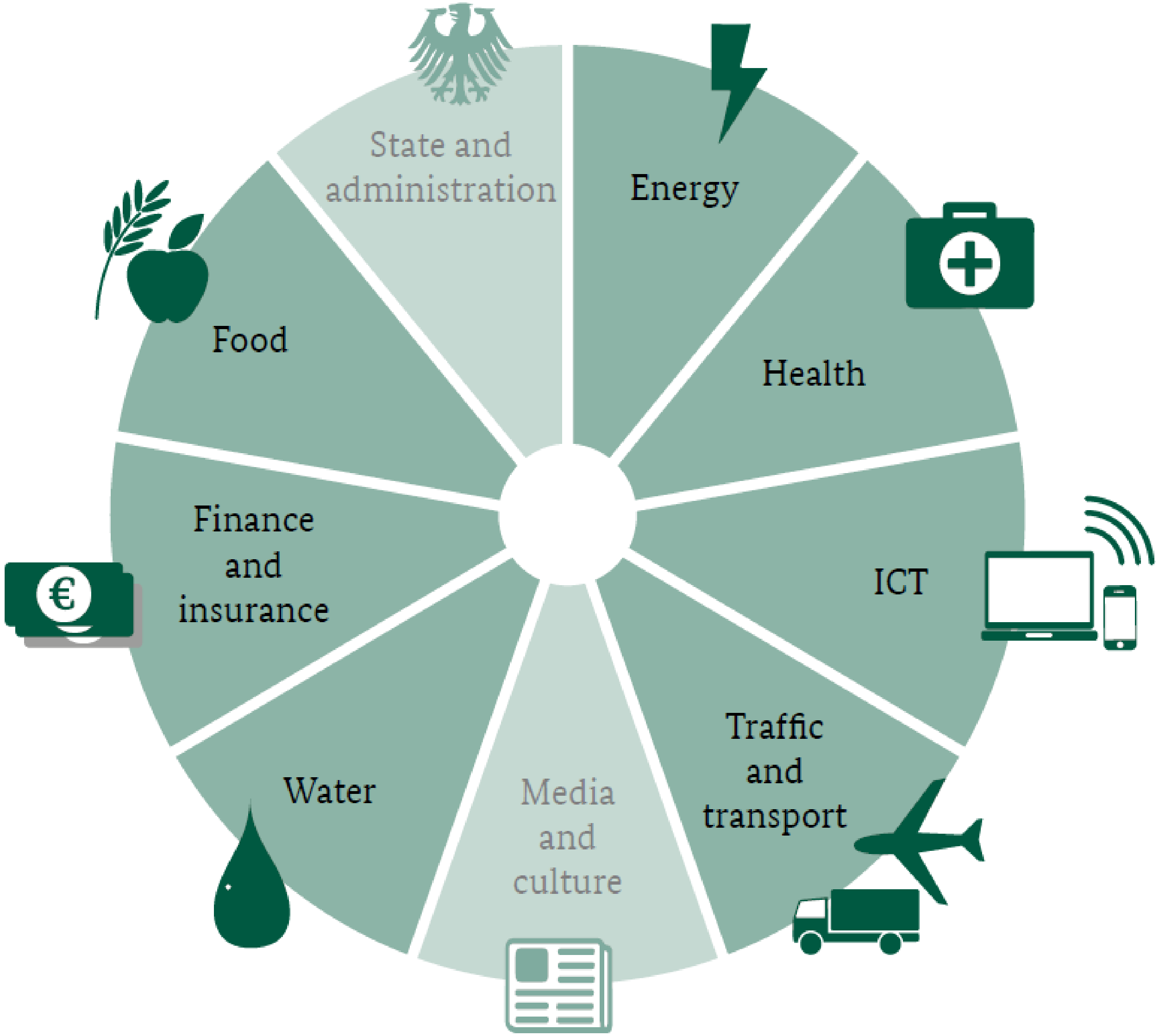
Protection of Critical Infrastructure in Germany

ISH Conference, May 6th, 2019

Dr. Harald Niggemann

1. Critical Infrastructure (CI) in Germany

Critical Infrastructure sectors in Germany



Mandatory: IT-Security Law (IT-SiG)

Provisions	▪ CI facilities must be secured appropriately
Assurance	▪ Operators must prove appropriateness of provisions ▪ BSI checks if proof is valid and adequate
Warnings/ Situational Awareness	▪ BSI: Situation reports and warnings ▪ Operators: Mandatory reporting of incidents
CI Identification (BSI-KritisV)	▪ Operators self-identify CI facilities, according to BSI-KritisV

Voluntary: UP KRITIS – Public Private Partnership

1. Public Private Partnership
2. Open to
    1. all CI operators,
    2. their industry associations and
    3. their supervisory agencies.
3. Promotes cyber security through
    1. information sharing and
    2. strategic collaboration across CI sectors.

UP KRITIS

2. Digitalisation – does not spare CI sectors

Trends of digitalisation

>> Connected supply chains

Industry 4.0 / Smart Factory

>> Connected work environment

>> Smart factory

>> Intelligent traffic lights

Connected city

>> Interacting infrastructure

>> Smart city

>> Self-driving cars

Connected cars

>> Interaction with infrastructure

>> Smart car

>> Autonomous household robots

Connected home

>> Networked household sensors

>> Smart TV

>> Automated power supply

Smart electricity grids

>> Networked work environment

>> Smart meter

>> Automated power supply

Connected healthcare

>> New opportunities thanks to data analysis

>> eHealth

Technologies for digitalisation

>> Synergy effects

Cloud computing

>> Centralisation of data

>> Permanent access

>> Cryptocurrencies

Blockchain

>> Direct coordination of devices

>> Distributed ledger

>> Increased computing power

Quantum computing

>> Quantum cryptography

>> Post-quantum

>> Networking in cyberspace

Internet of things

>> Complexity by integration

>> Ubiquity

>> Knowledge-based systems

AI – artificial intelligence

>> New problem-solving opportunities

>> Deep learning

>> Data generation and checking

Big data

>> New analysis opportunities

>> Data mining

>> High download speed

5G mobile telecommunications standard

>> Improved service quality

>> New data collection

Sensors & actuator technology

>> Automated control

Development of digitalisation

...more data transfer

2016	2021
108,000 TB *per hour*[1]	***400,000 TB*** *per hour*[1]

...more networking

2016	2021
6 billion *M2M capable devices*[1]	***14 billion*** *M2M capable devices*[1]

...more devices

2016	2021
five *web capable devices per capita in Germany*[1]	***nine*** *web capable devices per capita in Germany*[1]

...more speed

2016	2021
27 Mbps *(landline)* ***7 Mbps*** *(mobile)*[1]	***53 Mbps*** *(landline)* ***20 Mbps*** *(mobile)*[1]

...more attacks

2016	2021
1.3 m *DDoS attacks >1 Gbps*	***3.1 m*** *DDoS attacks >1 Gbps*

[1] source: CISCO VNI, 2017

3. Threat situation – does not spare CI sectors either

How threatened is cyberspace in Germany?

- **The new quality of attacks** raised the level of the threat situation and demands **a new degree of flexible defense procedures**.
- Concerning attacks on the government network, an average of **28,000 e-mails containing malware is intercepted per month**.
- The BSI has sent **16 million alert e-mails** in order to draw attention to hazardous situations.
- **70 % of the companies** have become **victims of cyber attacks in 2016/2017** according to a survey by the Allianz für Cyber-Sicherheit (“Alliance for Cyber Security”).
- In 2018 approximately **390,000 variations of new malware programmes were detected per day**.
- In the first quarter of 2018, **DDoS attacks of up to 190 Gbit/s** have been detected in Germany.
- **New dimension of vulnerabilities was found in hardware**.

Federal Office
for Information Security

The State of IT Security
in Germany 2018

Source: BSI

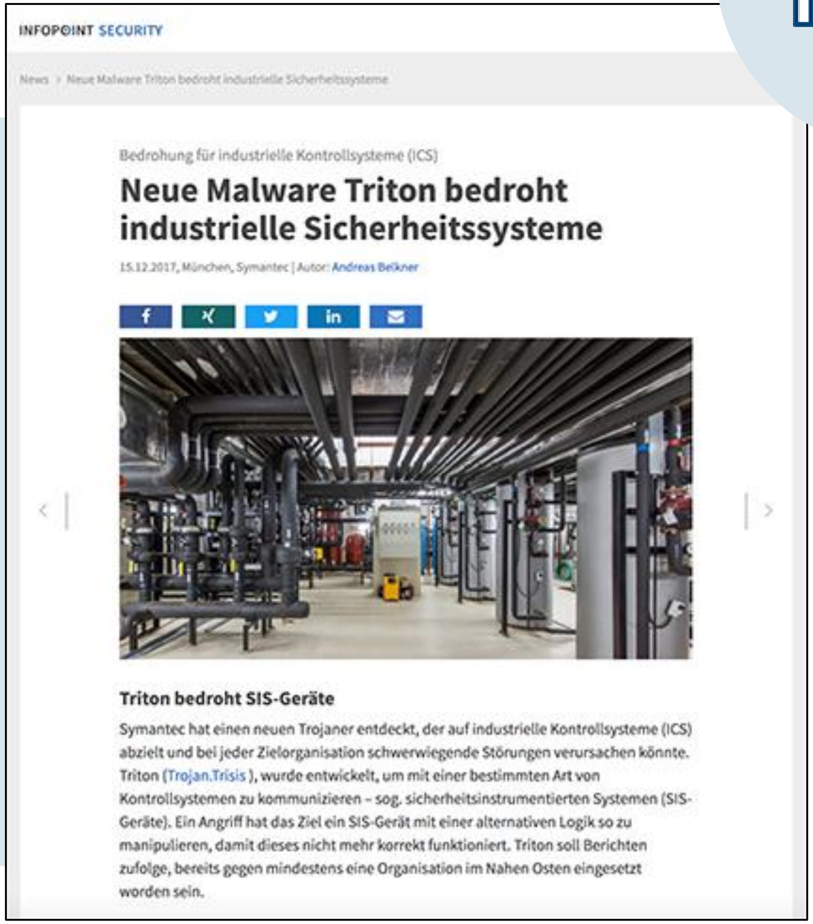
Threat situation – close up

Economy

Malware threatens safety systems

- Trojan that specifically attacks industrial control systems (ICS).
- Deactivates “Safety Instrumented Systems”:
  The last line of defence against
  big-time failure.
- Elaborate piece of malware of an obviously resourceful threat actor (APT).
- Clear intent: maximum destruction.

Source: infopoint-security.de



INFOPOINT SECURITY

News › Neue Malware Triton bedroht industrielle Sicherheitssysteme

Bedrohung für industrielle Kontrollsysteme (ICS)

Neue Malware Triton bedroht industrielle Sicherheitssysteme

15.12.2017, München, Symantec | Autor: Andreas Belkner

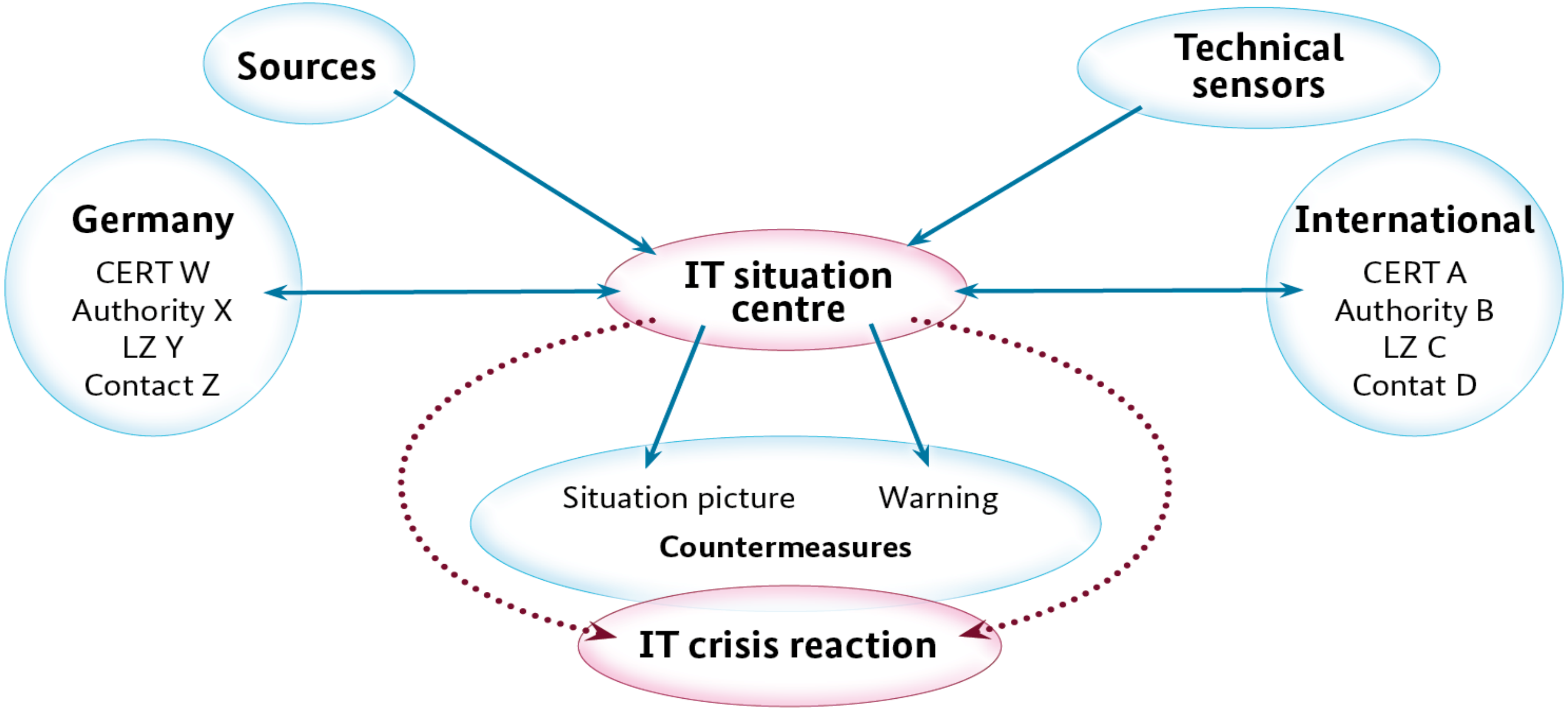
Triton bedroht SIS-Geräte

Symantec hat einen neuen Trojaner entdeckt, der auf industrielle Kontrollsysteme (ICS) abzielt und bei jeder Zielorganisation schwerwiegende Störungen verursachen könnte. Triton (Trojan.Trisis), wurde entwickelt, um mit einer bestimmten Art von Kontrollsystemen zu kommunizieren – sog. sicherheitsinstrumentierten Systemen (SIS-Geräte). Ein Angriff hat das Ziel ein SIS-Gerät mit einer alternativen Logik so zu manipulieren, damit dieses nicht mehr korrekt funktioniert. Triton soll Berichten zufolge, bereits gegen mindestens eine Organisation im Nahen Osten eingesetzt worden sein.

Federal Office
for Information Security

4. BSI – products and services

Information sharing



Products and services

BÜRGERCERT
Ins Internet - mit Sicherheit

BSI FÜR BÜRGER
INS INTERNET - MIT SICHERHEIT

Bundesamt für Sicherheit in der Informationstechnik
VS-Anforderungsprofil
BSI-VS-AP-XXXX-20XX

Bundesamt für Sicherheit in der Informationstechnik
Deutsches IT-Sicherheitszertifikat
Zertifikat Nummer:
BSI-DSZ-XXXX-20XX

Plan
Do
Check
Act
Informations-sicherheitsberatung

Sichere Informationstechnik
MINDESTSTANDARD

MISP
Threat Sharing

MIRT
Mobile Incident Response Team

BSI
Sichere mobile Lösungen

UP KRITIS

Allianz für Cyber-Sicherheit

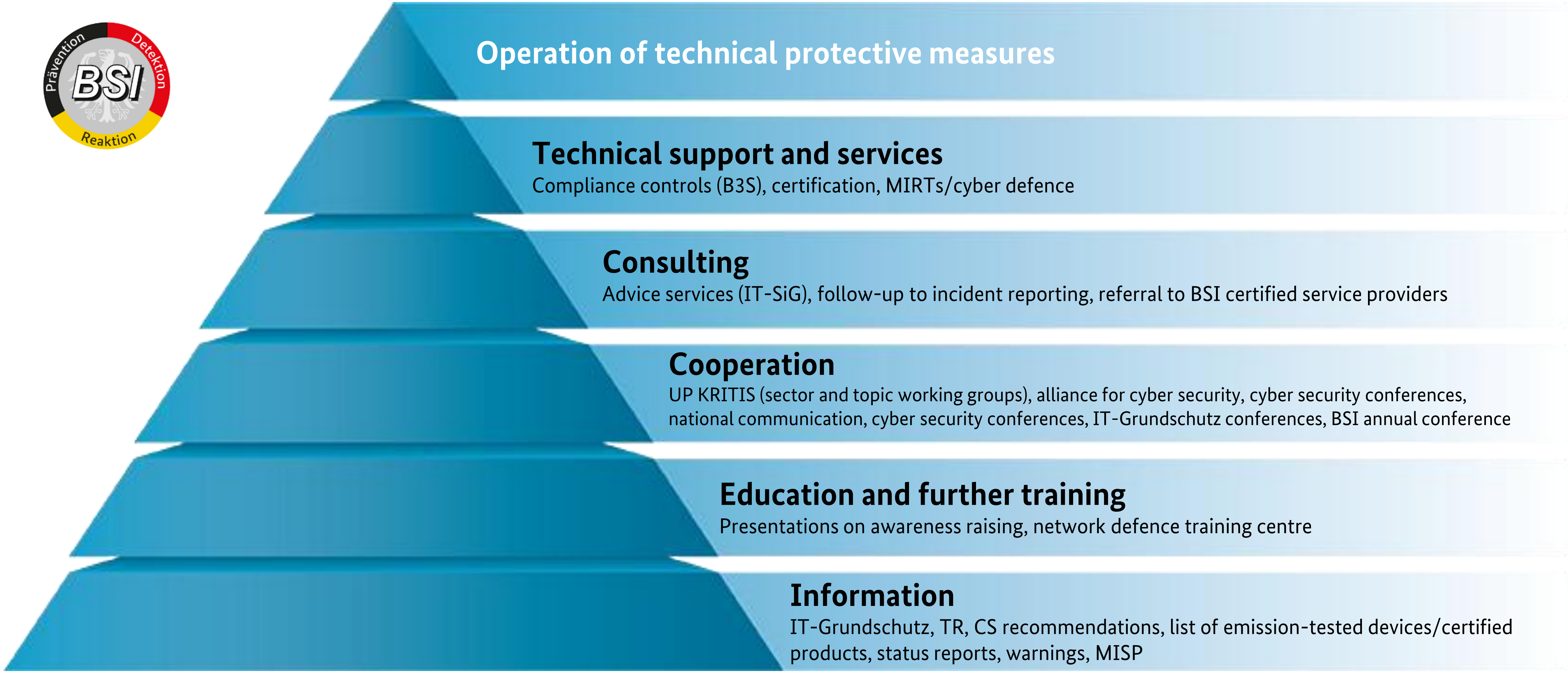
Lizenzierte IT-Grundschutz-Inhalte
Bundesamt für Sicherheit in der Informationstechnik

Bundesamt für Sicherheit in der Informationstechnik
Zertifikat
nach Technischen Richtlinien des BSI
BSI-TR-03104
Zertifikat-Nr.:
BSI-K-TR-0065-2010

Cloud Computing

Federal Office
for Information Security

BSI offers for KRITIS/INSI



Operation of technical protective measures

Technical support and services
Compliance controls (B3S), certification, MIRTs/cyber defence

Consulting
Advice services (IT-SiG), follow-up to incident reporting, referral to BSI certified service providers

Cooperation
UP KRITIS (sector and topic working groups), alliance for cyber security, cyber security conferences, national communication, cyber security conferences, IT-Grundschutz conferences, BSI annual conference

Education and further training
Presentations on awareness raising, network defence training centre

Information
IT-Grundschutz, TR, CS recommendations, list of emission-tested devices/certified products, status reports, warnings, MISP

8. Conclusion

Conclusion

- BSI is closely cooperating with (among others)
  - CI operators,
  - their business associations and
  - their supervisory agencies,
- both, on a mandatory and on a voluntary basis,
- for the joint benefit of government, business, and society.

Thank you for your attention!

Contact

Dr. Harald Niggemann
Cyber Security Strategist

Federal Office for Information Security (BSI)

Godesberger Allee 185 - 189
53175 Bonn, Germany

Phone: +49 228 99 9582 5368
E-Mail: harald.niggemann@bsi.bund.de
Internet: www.bsi.bund.de/EN/

Prävention
Detektion
BSI
Reaktion