Antalya, October 2018

Rising new Cyber Security Threats: Protecting critical energy infrastructure

8th TURKEY ENERGY SUMMIT

pwc

PwC Cybersecurity & Privacy

Introduction

SV
GERICHTSSACHVERSTÄNDIGE

Datenschutz-Audit
Recht – Organisation – Prozess – IT
Der Praxisleitfaden zur Datenschutz-Grundverordnung
LexisNexis

EU-Datenschutz-Grundverordnung (EU-DSGVO)
Praxiseinführung in 7 Schritten
Post

Georg Beham has been working in the field of information technology since 1989 has a master degree in Information Security. He is partner with **PwC** and responsible for “**Cybersecurity & Privacy**”. In Austria he is a well known expert in cybersecurity and data protection**.** Georg supports clients to **protect their data** and **to prevent cyberattacks** for **more than 15 years**.

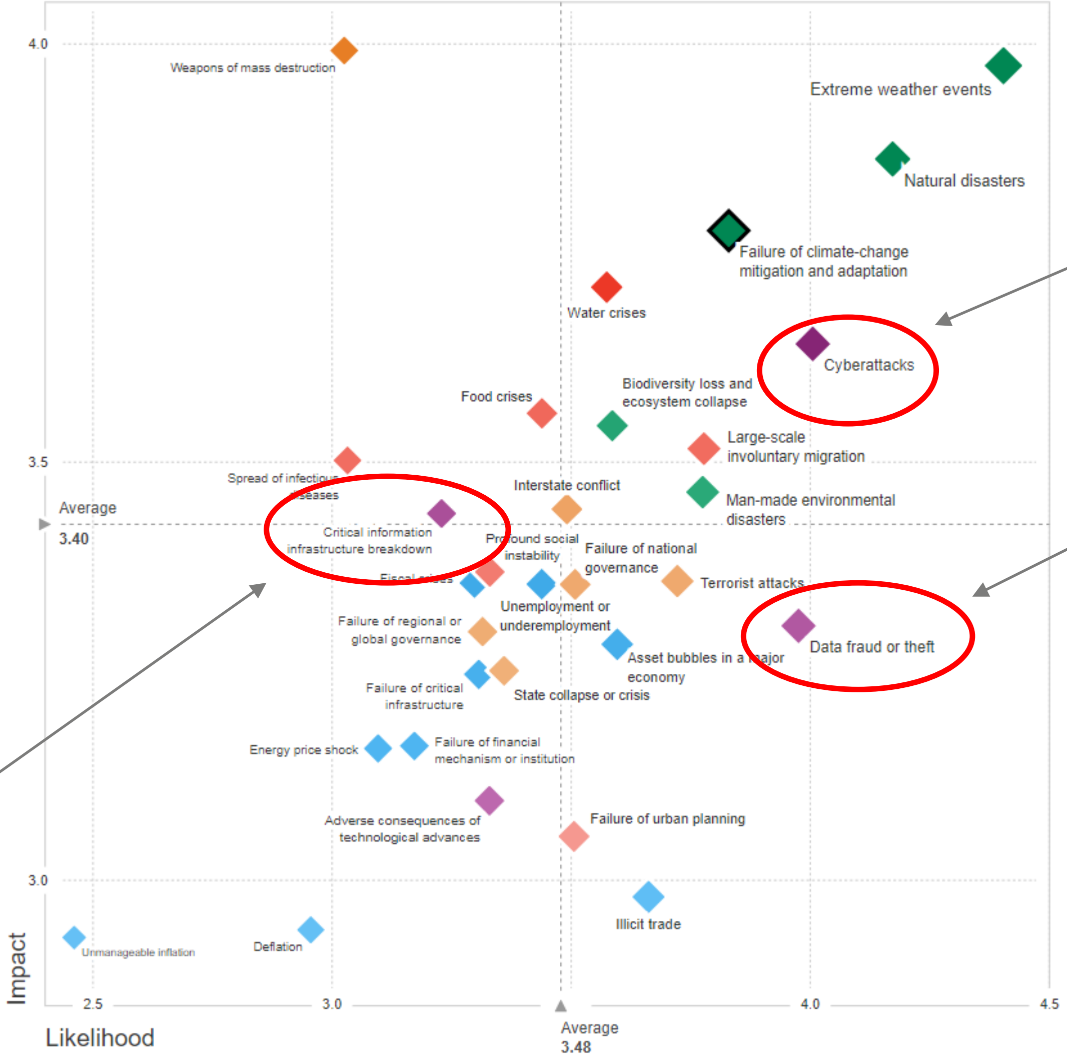
Additional key areas are cloud security, business continuity, IT forensic and incident response.

Furthermore he is certified **expert witness** in the field of Cybersecurity, cyber forensic and privacy and **lecturer** at several **universities**. Additionally he is **author** of professional books in topic of “Cybersecurity and Privacy”.

01
The Facts & Figures

WORLD ECONOMIC FORUM

The Global Risks Landscape 2018

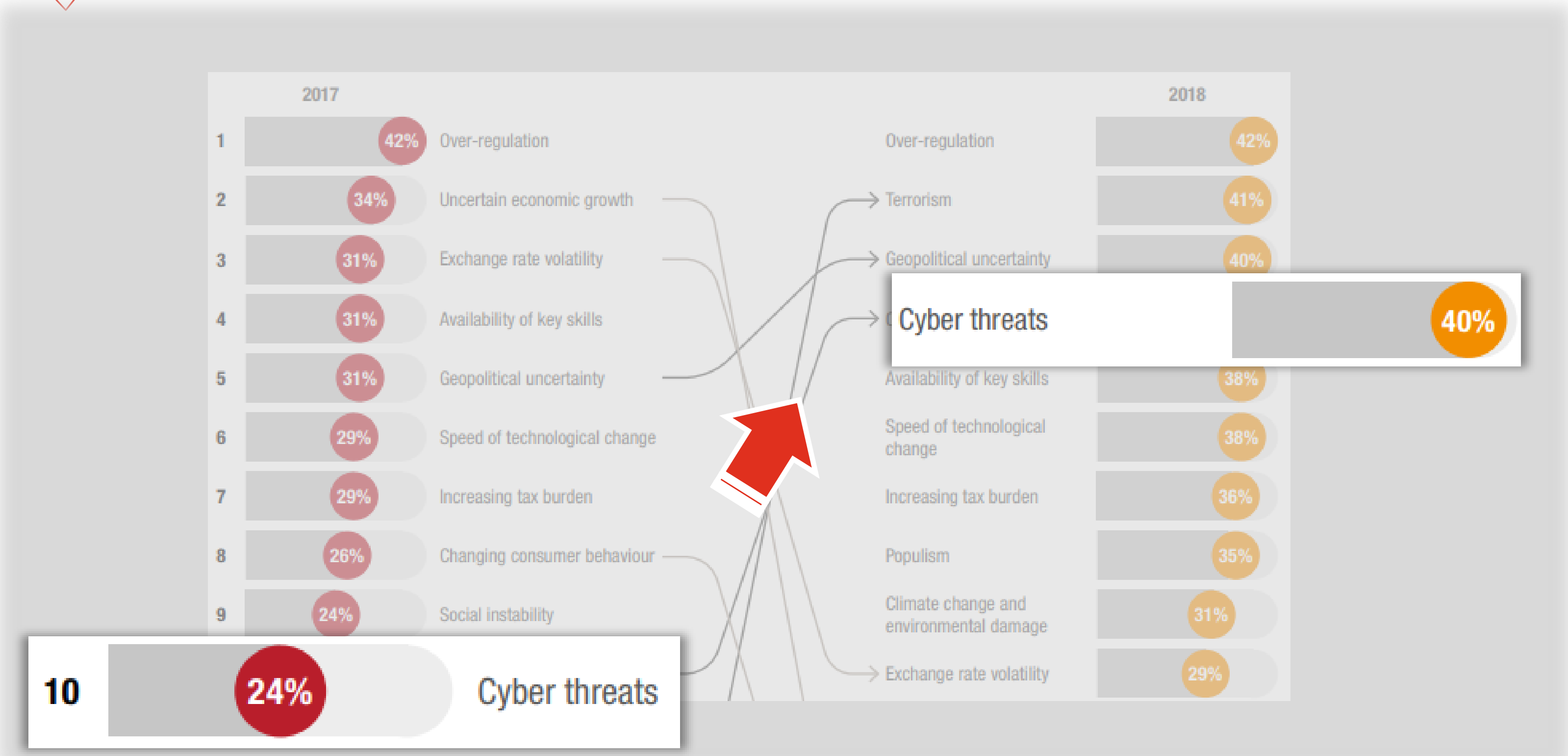


Cyberattack

Data fraud or theft

Critical Information infrastructure breakdown

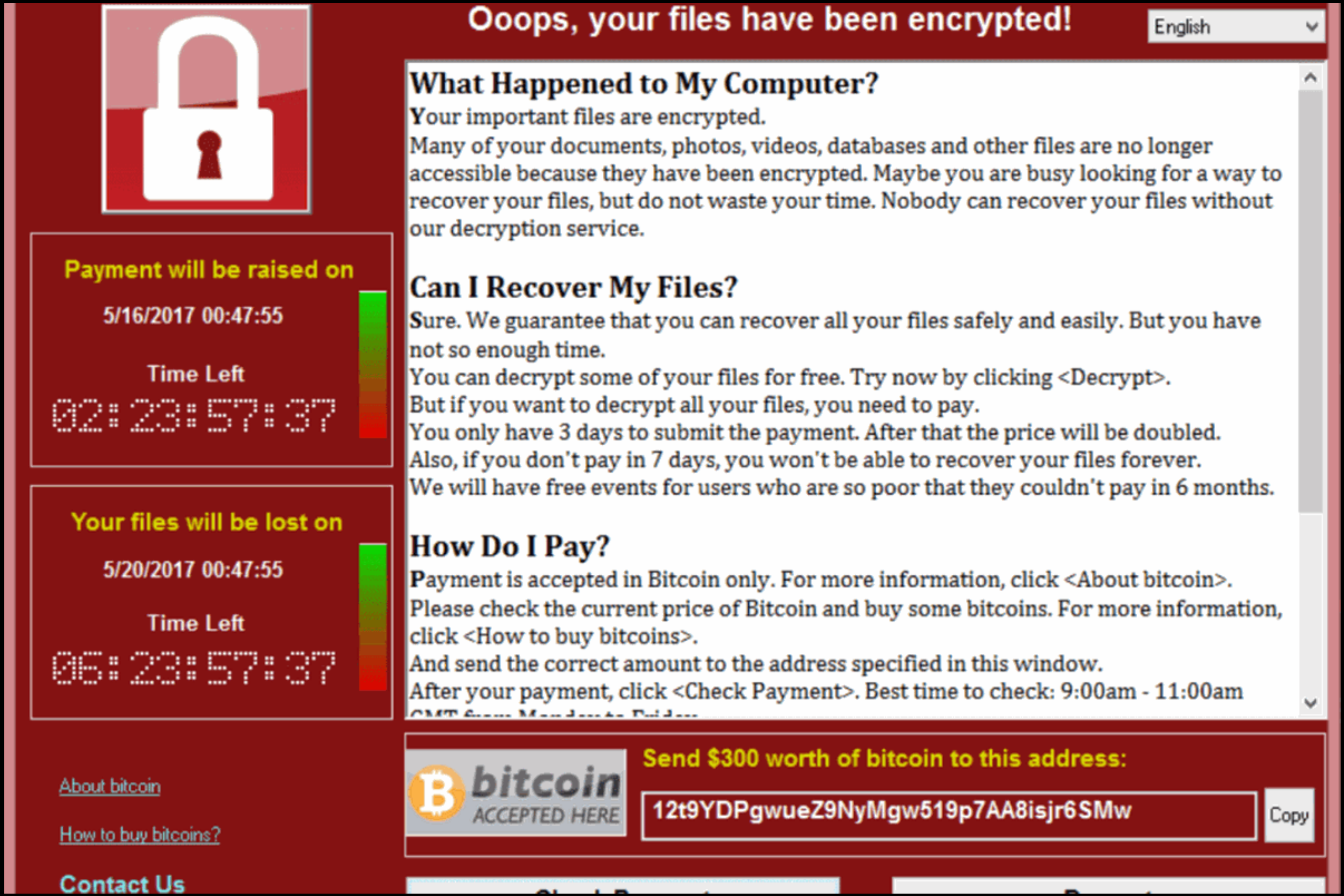
Cyber threats keep CEOs up at night
PwC's CEO Survey at World Economic Forum in Davos 2018



02

The Risk

Cyber Threat
Ransomware



Ooops, your files have been encrypted!

What Happened to My Computer?

Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

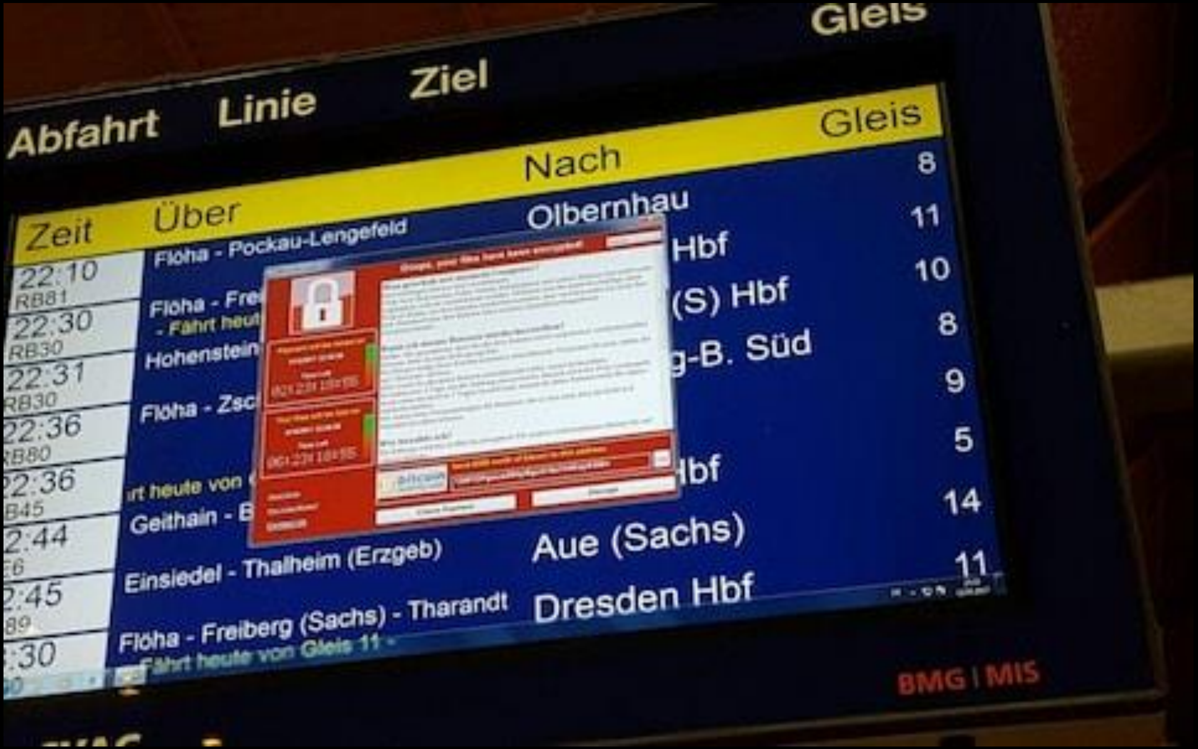
Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37

Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37

Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Cyber Threat

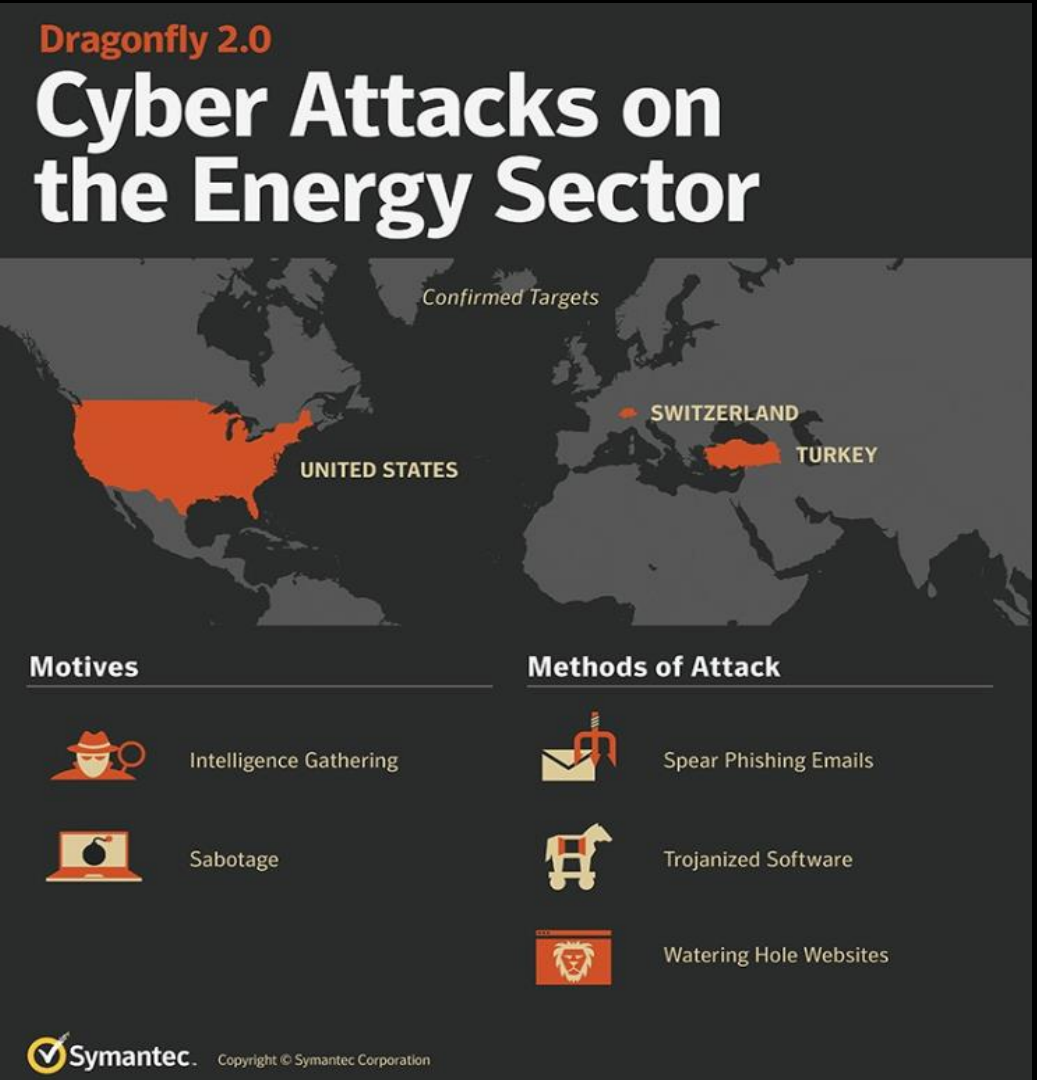
Ransomware



Example: Deutsche Bahn

- Germany's rail network was thrown into chaos on Friday night when it fell victim to a cyber attack rolling the world.
- The ransomware called WannaCry encrypted data on the computers, demanding payments to restore access
- Deutsche Bahn computers appeared to be infected with the virus, with the "ransomware" message demanding money appearing on screens at train stations.
- Pictures posted on social media by commuters showed train information monitors displaying the ransom demand to unlock the computers.

Industrial Control Systems (ICS) have been developed with a focus on:
safety, but not on **security**,
functionality, but not on **fault reaction**,
persistence, but not on **transformation**.



Dragonfly 2.0

Cyber Attacks on the Energy Sector

Motives

- Intelligence Gathering
- Sabotage

Methods of Attack

- Spear Phishing Emails
- Trojanized Software
- Watering Hole Websites

Symantec. Copyright © Symantec Corporation

Example: Dragonfly 2.0

- Campaign between 2015 and 2017
- Malicious spear phishing email campaign
  - Invitation to a New Year Party
  - Later energy industry related content
- Stolen network credentials
- Water-hole websites
  - Compromised websites frequently visited by energy sector
- Fake flash updates
- Trojanized software
  - Usual trojan framework was used
- Backdoors was established

First publically known attack on critical infrastructure in Europe was 2015

Example: Ukraine regional power suppliers

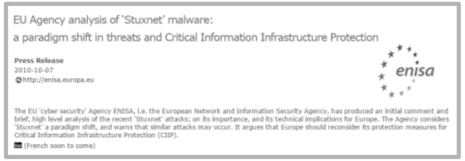
- 2015 in West-Ukraine province Iwano-Frankiwsk was target of first publically known Cyber attack
- More than a quarter million residential, companies and public authorities were without electricity for several days
- Reason was a focused and orchestrated hacker attack on three regional power suppliers
- Attacker infiltrated the infrastructure by malicious program code, the so called „BlackEnergy Trojan“ a to create DDoS (Distributed denial of service)
- Execution was started remotely and most probably even abroad

First publically known attack on critical infrastructure in Europe was 2015

Example: Local German municipal

- Stadtwerke Ettlingen, a regional German energy provider decided to do a penetration test
- The hired hacker, Felix Lindner, needed 23 minutes to crack the password of the main IT systems – via using a simple program from the Internet
- >300 energy providers use the same IT system
- In less than 2 days the control centre of the entire company was taken over – with a couple of simple mouse clicks 40,000 households could have taken off the power grid
- Main reasons were the linked networks, outdated patch releases of operating systems, deactivated security functionalities and weak passwords – plus USB sticks and smart phones

Cyber threats to the Energy sector and its critical infrastructure are also real

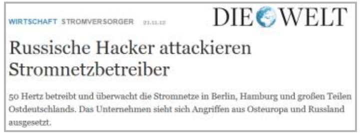


EU Agency analysis of 'Stuxnet' malware:
a paradigm shift in threats and Critical Information Infrastructure Protection

Press Release
2010-10-07
http://enisa.europa.eu

The EU 'cyber security' Agency ENISA, i.e. the European Network and Information Security Agency, has produced an initial comment and brief, high level analysis of the recent 'Stuxnet' attacks; on its importance, and its technical implications for Europe. The Agency considers 'Stuxnet' a paradigm shift, and warns that similar attacks may occur. It argues that Europe should reconsider its protection measures for Critical Information Infrastructure Protection (CIIP).

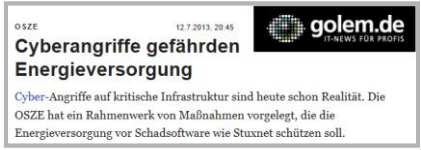
(French soon to come)



WIRTSCHAFT STROMVERSORGER [illegible] DIE WELT

Russische Hacker attackieren Stromnetzbetreiber

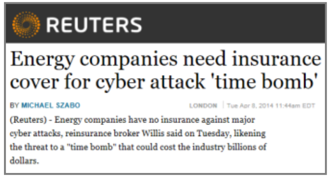
50 Hertz betreibt und überwacht die Stromnetze in Berlin, Hamburg und großen Teilen Ostdeutschlands. Das Unternehmen sieht sich Angriffen aus Osteuropa und Russland ausgesetzt.



OSZE 12.7.2013, 20:45 golem.de IT-NEWS FÜR PROFIS

Cyberangriffe gefährden Energieversorgung

Cyber-Angriffe auf kritische Infrastruktur sind heute schon Realität. Die OSZE hat ein Rahmenwerk von Maßnahmen vorgelegt, die die Energieversorgung vor Schadsoftware wie Stuxnet schützen soll.



REUTERS

Energy companies need insurance cover for cyber attack 'time bomb'

BY MICHAEL SZABO LONDON | Tue Apr 8, 2014 11:44am EDT

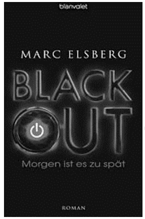
(Reuters) - Energy companies have no insurance against major cyber attacks, reinsurance broker Willis said on Tuesday, likening the threat to a "time bomb" that could cost the industry billions of dollars.

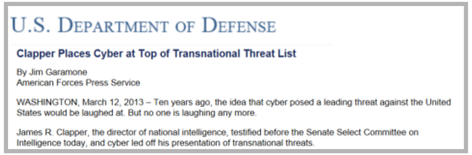
Source: World Energy Council 2016

2010

Global Energy Cyberattacks: "Night Dragon" McAfee

By McAfee® Foundstone® Professional Services and McAfee Labs™
February 10, 2011





U.S. DEPARTMENT OF DEFENSE

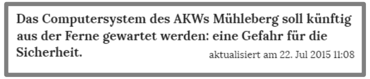
Clapper Places Cyber at Top of Transnational Threat List

By Jim Garamone
American Forces Press Service

WASHINGTON, March 12, 2013 – Ten years ago, the idea that cyber posed a leading threat against the United States would be laughed at. But no one is laughing any more.

James R. Clapper, the director of national intelligence, testified before the Senate Select Committee on Intelligence today, and cyber led off his presentation of transnational threats.

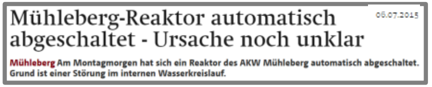
> *„Der Quellcode von Stuxnet und seinen deutlich mehr als zehn Derivaten ist im Internet verfügbar und kann mit geringem Aufwand an andere Ziele wie Kraftwerke und Stromverteilung angepasst werden [..]. Er kann damit auch eine Gefahr für Leib und Leben von Bundesbürgern darstellen.“*
>
> *Gesellschaft für Informatik, 26.06.2013*



Das Computersystem des AKWs Mühleberg soll künftig aus der Ferne gewartet werden: eine Gefahr für die Sicherheit.

aktualisiert am 22. Jul 2015 11:08

2018



Mühleberg-Reaktor automatisch abgeschaltet - Ursache noch unklar 06.07.2015

Mühleberg Am Montagmorgen hat sich ein Reaktor des AKW Mühleberg automatisch abgeschaltet. Grund ist einer Störung im internen Wasserkreislauf.

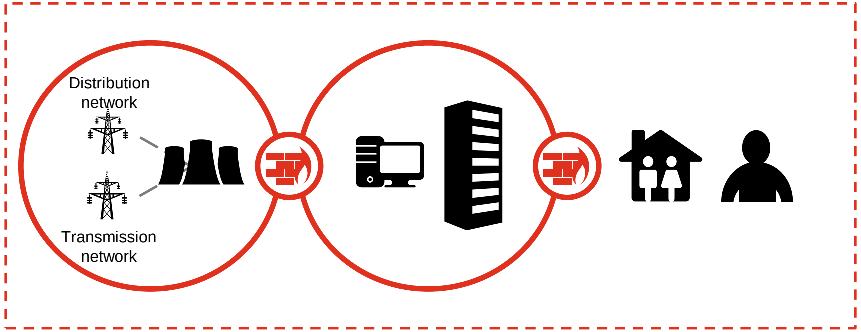
Observation

- Cyber risks are growing in terms of both their sophistication and the frequency of attacks
- The economic and physical consequences of cyber attacks against energy infrastructure could be severe, making it an attractive target
- By 2018 the oil and gas industries could be spending around US$ 2bn each year for cyber security

03
The Challenge

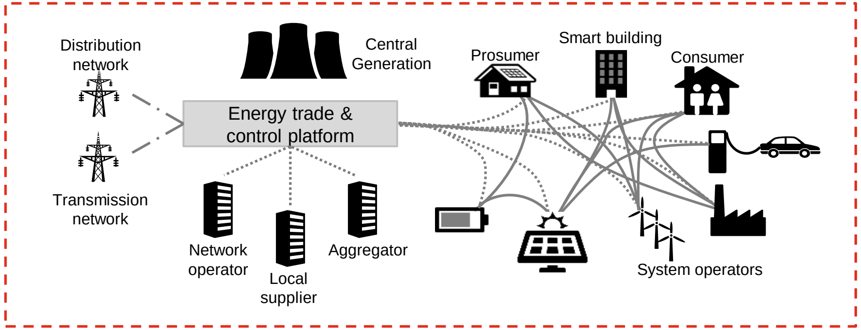
In the new utility world more points of attack threaten companies

Old energy world



- Critical infrastructure was isolated in separate closed loop
- Interfaces to the commercial IT systems were secured by a firewall
- The commercial loop itself was secured by a firewall to suppliers, customers and other parties
- The only point of attack was the commercial IT world, for attacking the critical infrastructure another firewall needed to be captured

New energy world



- Smart grids consist of many IT based components
- Examples are classic IT like PCs or servers, but also communication/grid technology, smart meters and mobile applications
- The former clear separation between technical and commercial IT is more and more disappearing
- That leads to better steering of consumption and capacities, but each of those components are potential targets for attacks

Industrial Security	vs.	Office IT-Security
Production (from clean till tough)	***Location***	Climate Office and Data Center
Engineer from Manufacturer	***Installation***	Specialized IT-engineers
Depends on ICS/SCADA system	***Topology***	Meshed in most cases, mainly IP-based
Latency < 300ms	***Availability***	Seconds or minutes of outage are acceptable
Low, switches just have a few ports	***Amount***	Quite high with switches consisting high port density
Part of the System (functional)	***Monitoring***	IT-Expert, Network Monitoring, SIEM, Vulnerability Management etc....
Up to 20 years or more	***Product Lifecycle***	One to three years

04
Solution

Business Capabilities.

Risk Identification and Mitigation

- Identification of ICS related risk
- Recommendation for ICS risk mitigations

Securing Production

- Harden and securing actual production and business
- Reduce cyber attack vectors

Business Sustainability

- Securing future business
- Ensure company sustainability

Management Capabilities.

Management Reporting

- Management compatible reporting

Audit Capabilities

- Reliable and repeatable audit trails

Vulnerability Management

- Interface for vulnerability management systems

Technical Capabilities.

System Identification

- Identification of ICS (or DCS) related systems, e.g. SCADA, control server, MTU, RTU and PLC

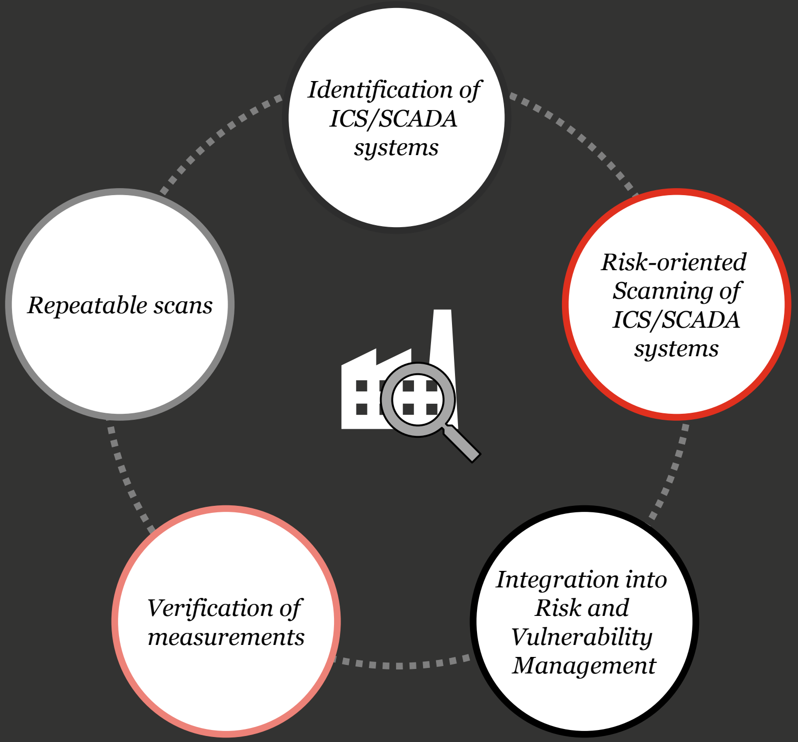
Service Detection

- Adapted ICS Service detection and enumeration

Vulnerability Scanning

- Adapted ICS Vulnerability Scanning

PwC's
ICS Scanning Service.



Identification of ICS/SCADA systems

Risk-oriented Scanning of ICS/SCADA systems

Integration into Risk and Vulnerability Management

Verification of measurements

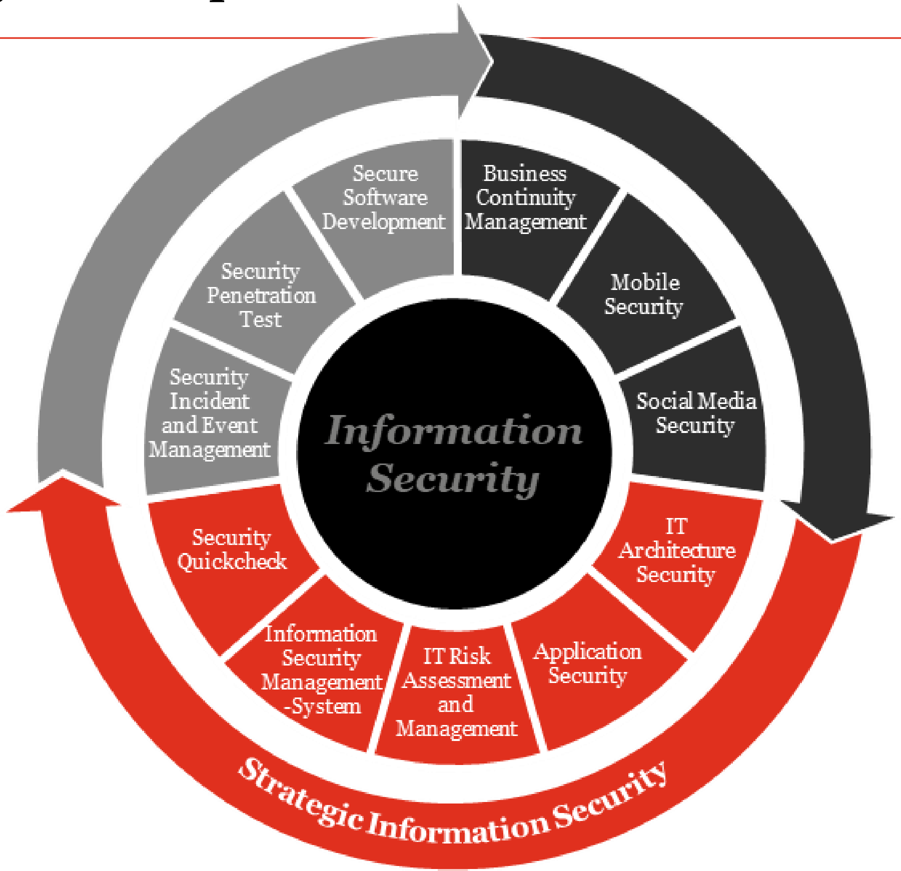
Repeatable scans

PwC‘s ICS Scanning Service

Combining Business IT and Production IT.
Combining Business Risk and Production Risk.
Combining IT Security and ICS knowledge.
Combining Risk, Safety and Security.

To reduce Risks.
To increase Security.
To enhance Sustainability in Business.
To support Readiness in a digitalized world.

PwC’s Cybersecurity service portfolio


Information Security
Secure Software Development
Business Continuity Management
Mobile Security
Social Media Security
IT Architecture Security
Application Security
IT Risk Assessment and Management
Information Security Management -System
Security Quickcheck
Security Incident and Event Management
Security Penetration Test
Strategic Information Security

Thank you!

RECHTSPRAXIS

Pachinger | Beham (Hrsg.)

Datenschutz-Audit

Recht – Organisation – Prozess – IT

Der Praxisleitfaden zur Datenschutz-Grundverordnung

Die Autoren: Pachinger | Beham | Jost | Klaebauer

DSG 2018

Checklisten & Beispiele

LexisNexis

2., aktualisierte Auflage

Georg Beham
Reinhard Hubelbauer
(Hrsg.)

AUSTRIAN STANDARDS

EU-Datenschutz-Grundverordnung (EU-DSGVO)

Management & Dienstleistungen

Praxiseinführung in 7 Schritten

Post

1. Auflage 2017

PwC Cybersecurity contact

Georg Beham
Partner
Cybersecurity & Privacy

PwC Austria
Hafenstraße 2a, 4020 Linz
Tel. +43 732 611 750-0
georg.beham@pwc.com

www.linkedin.com/in/beham

@georgbeham

Canadian Cookie Factory

Risk Management and Production Owner estimating risks and losses caused by cyber attack (worst case scenario):

- Salted dough → loss of one day of cookie production

Unfortunately real cyber attacker run standard security scanning tools against production resulting in

- attacked ICS crashed, production went offline
- dough cemented in production tubes
- production line needed to be rebuild
- production stand still for more than two weeks

Company was not ready for Industry 4.0 and the related threat landscape.

Industry 4.0 push the ICS development

ICS’s enable Industry 4.0

- Industrial Control Systems (ICS) build the technical backbone of Industry 4.0.
- Success of new business models for the production depends on gaining control over the Industry 4.0 security.
- Effective Industry 4.0 security is based on a strong ICS risk and vulnerability management.

Managing the ICS security is key

ICS threats to be identified

- The necessary ICS threat, risk and vulnerability management is based on a transparent IT and production security.
- Common IT security tools are not suitable for ICS’s.
- ICS Security Scanning tools are not available on the market.

Key questions in preparation to critical incidents

1

Clearly defined responsibilities?

Comprehensive management procedures necessary.

2

Sufficient (risk-oriented) security testing in place?

Tests need to detect significant risks and known vulnerabilities.

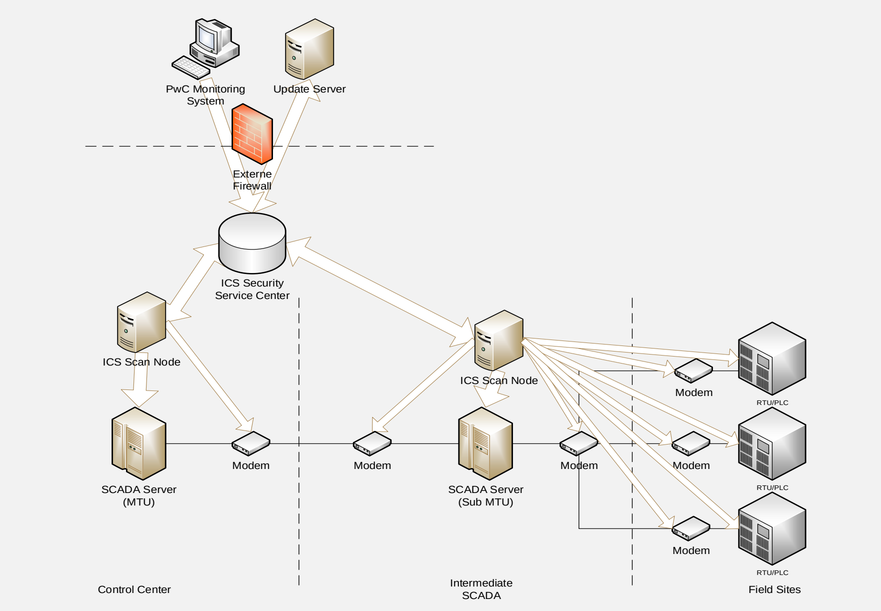
3

Evidence the scope of testing?

A coherent evidence management for testing is necessary.

Special technical features.

- Includes protocol implementation of Ethernet and PROFINET to perform detailed ICS/SCADA service analysis
- Includes protocol implementation of Siemens custom S7 protocol to receive detailed information from S7-based ICS/SCADA Systems
- Implementation of custom scanning modes to mitigate the risk of scanning sensitive ICS/SCADA environments
  - Passive mode (no data transmitting)
  - Cautious mode (low packet rate, mainly ARP, ICMP & SNMP)
  - Normal mode (Full Layer 2 and 3 ports and services)
  - Custom mode
- Offers detailed scanning timing, white- and black-listing settings


PwC Monitoring System
Update Server
Externe Firewall
ICS Security Service Center
ICS Scan Node
ICS Scan Node
SCADA Server (MTU)
Modem
Modem
SCADA Server (Sub MTU)
Modem
Modem
Modem
Modem
RTU/PLC
RTU/PLC
RTU/PLC
Control Center
Intermediate SCADA
Field Sites