



State of PI System Security and European Union NIS Directive

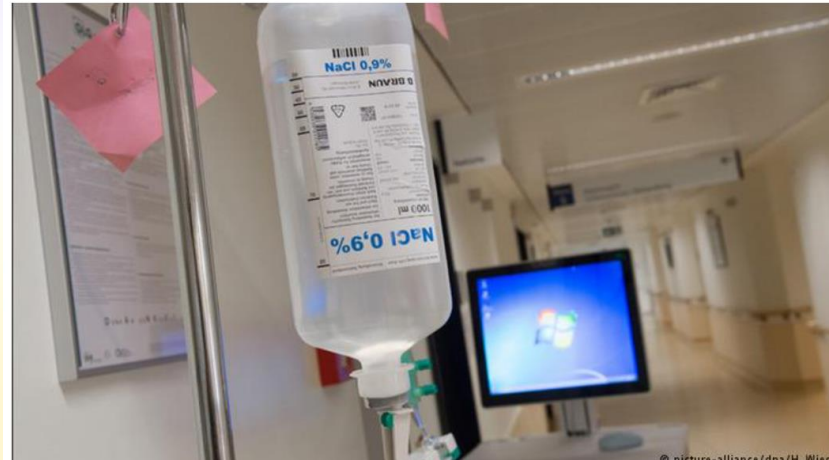
Presented by Bryan Owen PE, OSIsoft – Principal Cyber Security Manager

Ransomware: Who's next?

CYBER ATTACK

Hackers hold German hospital data hostage

Several hospitals in Germany have come under attack by ransomware, a type of virus that locks files and demands cash to free data it maliciously encrypted. It will take weeks until all systems are up and running again.



Agenda

- State of PI System Security
 - Case Study: Stolen Credentials
- NIS Directive
 - Germany's IT Security Act
- OSIsoft Policy
 - What about Vulnerabilities?
 - Ethical Disclosure



“Infrastructure Hardened” PI System

Global. Trusted. Sustainable.



What is “Infrastructure Hardened”?

- Extremely Reliable
 - Well Tested
 - Proven Capability
- } **“Trusted”**

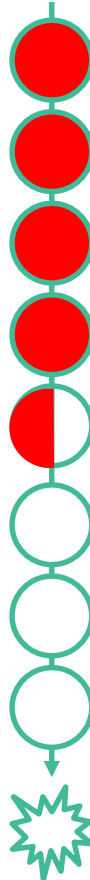
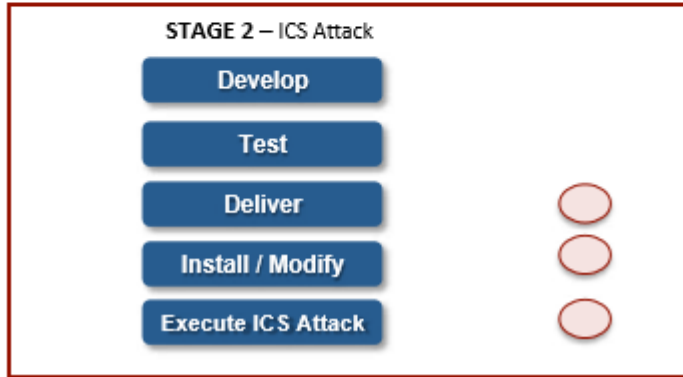
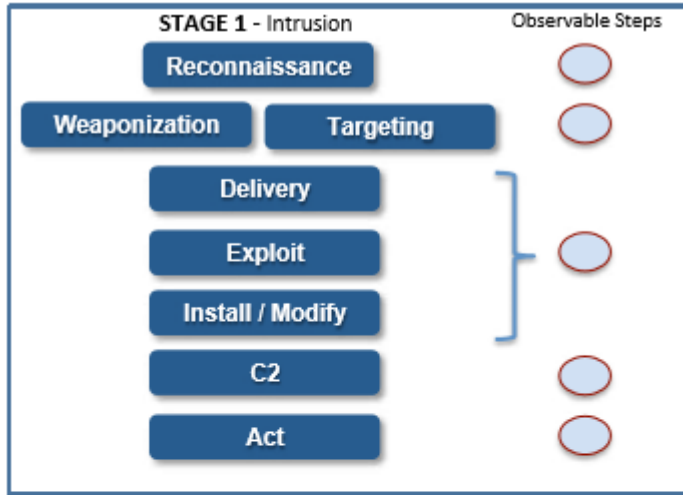


Security Development Lifecycle Process

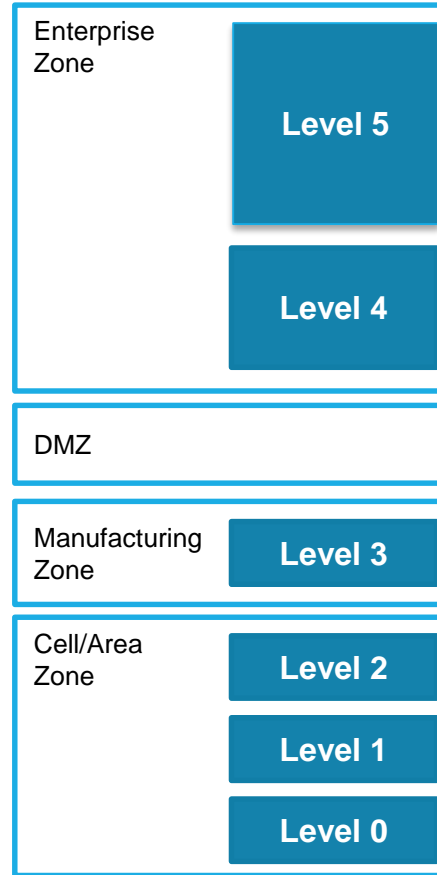
Infrastructure Hardening Informed by Experts

- **Idaho National Lab**
 - 2005 Assessment
 - 2008/2009/2012 vCampus Live!
 - 2011 Cooperative Research
- **US Army NetCom**
 - 2009 CoN #201006618
 - 2013 CoN (recertified)
- **US NRC**
 - 2010 DISA, NIST
- **SAP QBS Certification**
 - 2012/2013/2015 Veracode
- **Windows Logo Certification**
 - 2008 Windows 2008 Server Core
 - 2011 Windows 2008 R2 Server Core
 - 2012 Windows 2012 Server Core
- **Azure Penetration Testing**
 - 2014 PI Cloud Connect (Utility Partner)
 - 2014 PI Cloud Access (IOActive)
 - 2016 OSIsoft Cloud Services (In Scoping)
- **Information Security Consulting**
 - 2009 PI Server
 - 2010 PI Agent
 - 2011 PI Coresight
 - 2011 PI AF
 - 2012 PI ProcessBook
 - 2012 Products in Design (3)
 - 2013 Engineering Management
 - 2013 Products in Design (3)
 - 2013/2015 SDL for Security Champions
 - 2013/2014/2015 Defensive Programming (Cigital)
 - 2015 PI Connectors
 - 2015 PI Transport Security (IOActive)
 - 2015 PI System Security Review
 - 2015/2016 Microsoft Springfield
 - 2016 PI Coresight (IOActive)



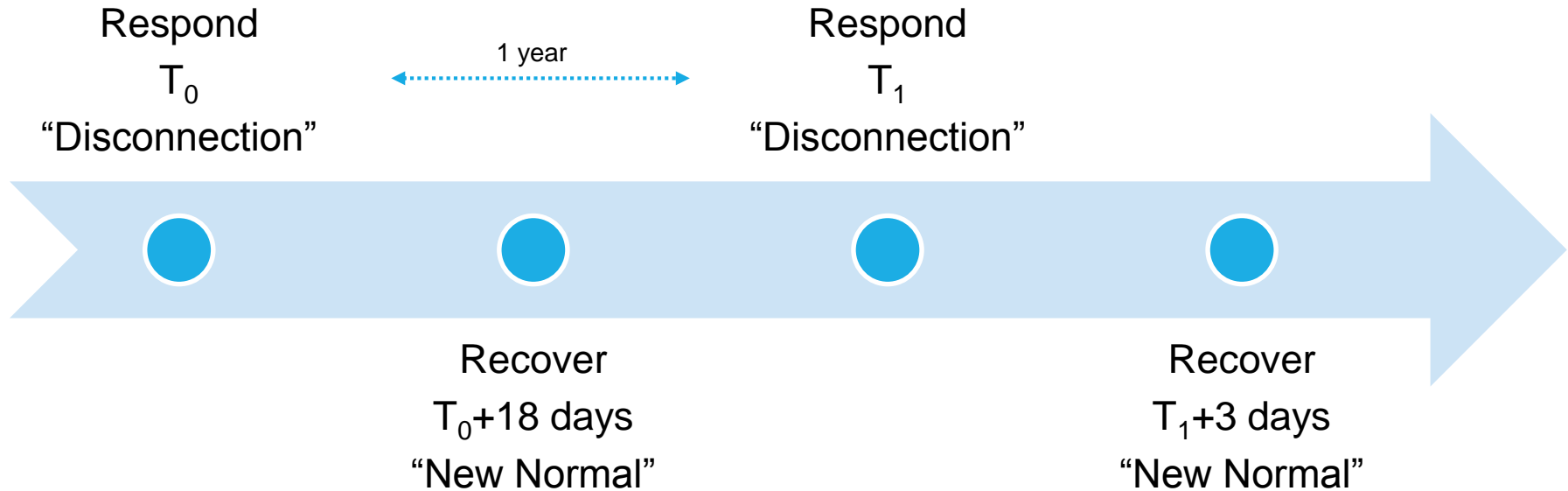


Attack with Impact



Case Study

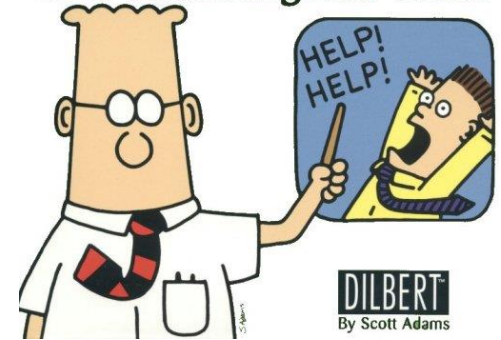
Timeline



Respond/Restore – Urgent Questions

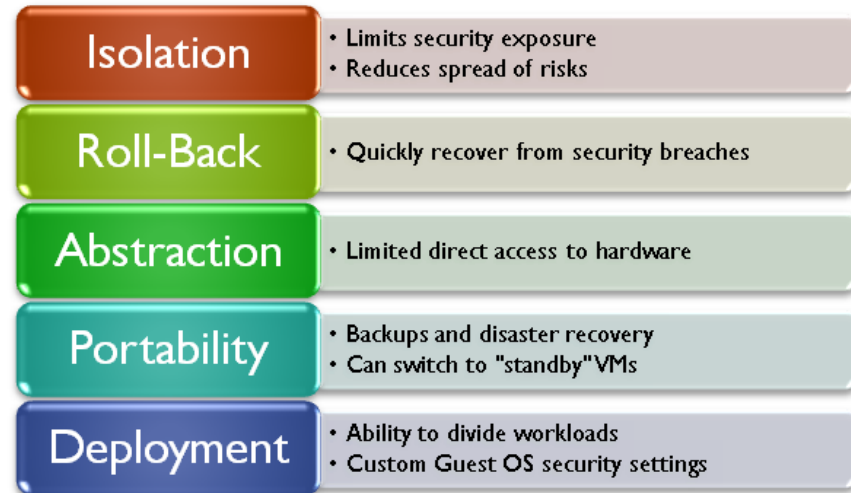
- Could attacker use stolen credentials to actuate control?
- How to disconnect without losing data?
- How are passwords stored?
- How to restore the PI System?
- Security by obscurity?
 - changing host name,
 - IP address,
 - TCP port

**Our Disaster Recovery Plan
Goes Something Like This...**



Respond/Recover – Lessons Learned

- Have a plan, 2nd time was 'rote execution'
 - Contain control protocol and credential use by zone
 - Shift majority of user load to application servers
 - Implement virtualization
 - Allow remote access
- (OSIsoft technical support)



NIST Voluntary Framework – “Respond/Recover”

...plans to take action regarding a detected cybersecurity event...



...plans for resilience and to restore any capabilities or services that were impaired...



NIS Directive

A Harmonized Approach to Cyber Security within EU

Member States

- Competent Authorities
- National Strategy
- Readiness Team

Essential Service Providers

- Incident Reporting
- State of the Art Security
- Compliance Audits



Under the NIS Directive, essential service providers must adopt requirements within 21 months of August 2016 or **face fines of up to €10m or 2% globally.**

Germany: Fight Against “Digital Carelessness”

Minister Complains About Digital Carelessness



Thomas de Maizière, Germany's Federal Minister of the Interior, recently complained about the German industry and population's lack of awareness about online security issues.

The requirement for businesses to report data breaches is a touchy issue, he said. Yet without such a rule, security could not be achieved in the long run.

Source: ECO International 22.05.2015

German IT Security Law (IT-SiG)

Security- & Risk - Culture

- ❑ Sector specific minimal requirements
 - ❑ Sector specific Security standards
- => Legal certainty

Effectiveness of Measures

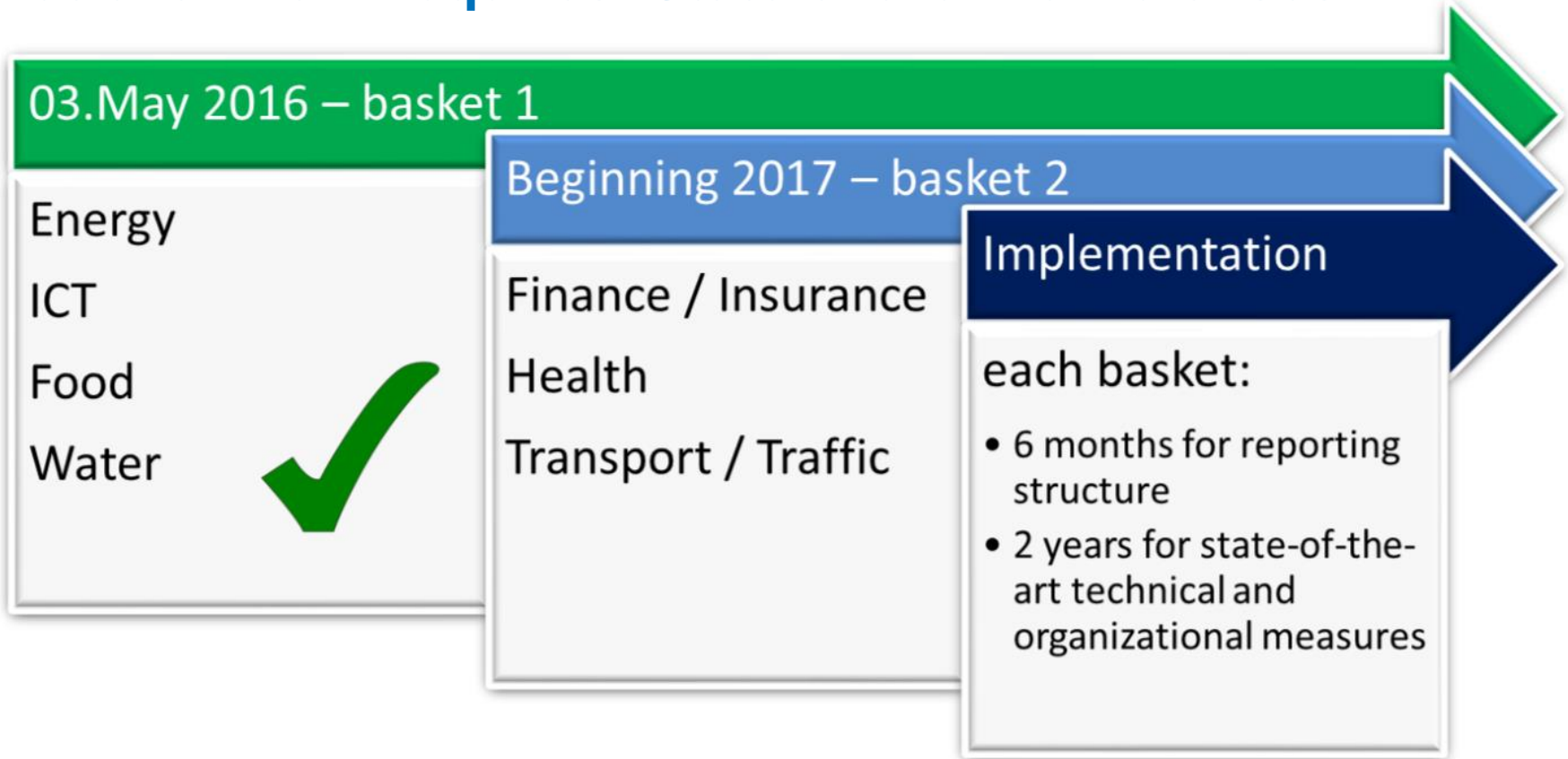
- ❑ Auditing obligation (every 2 years)
- ❑ Demonstrate compliance through audit reports
- ❑ Security flaws => Involvement of BSI

Situation Report

- ❑ BSI: drafting & distribution of situation reports & warnings
- ❑ KRITIS - Operators & Owners: Reporting obligation of (serious) incidents

Source: Olaf Götz (BMI) & Jens Wiesner (BSI) "Germany's Cyber Security Situation and the ITSecAct" 2016.09.15

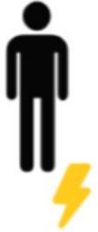
National Plan Requires 'State of the Art' Defenses



Source: Olaf Götz (BMI) & Jens Wiesner (BSI) "Germany's Cyber Security Situation and the ITSecAct" 2016.09.15

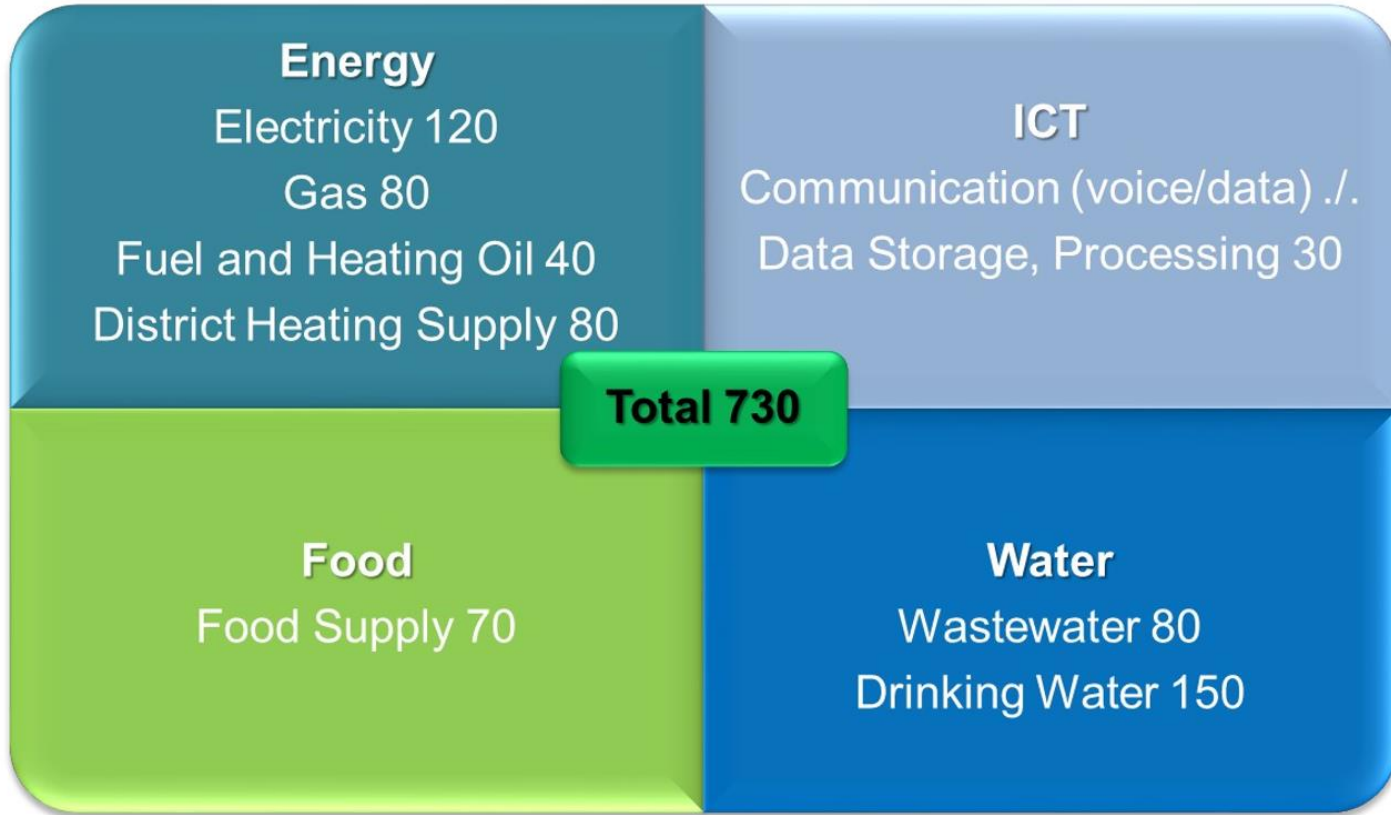
Method to Identify Critical Infrastructure

- Example: Electrical Generation for 500,000 Persons


$$\frac{590 \frac{TWh}{Jahr}}{80.000.000 \text{ Persons}} = 7375 \frac{kWh}{\text{Persons} * Jahr}$$
$$\text{Threshold} = \frac{7375 \text{ kWh}}{\text{Persons} * Year} \cdot 500.000 \text{ Persones} \approx \mathbf{420 \text{ MW}}$$

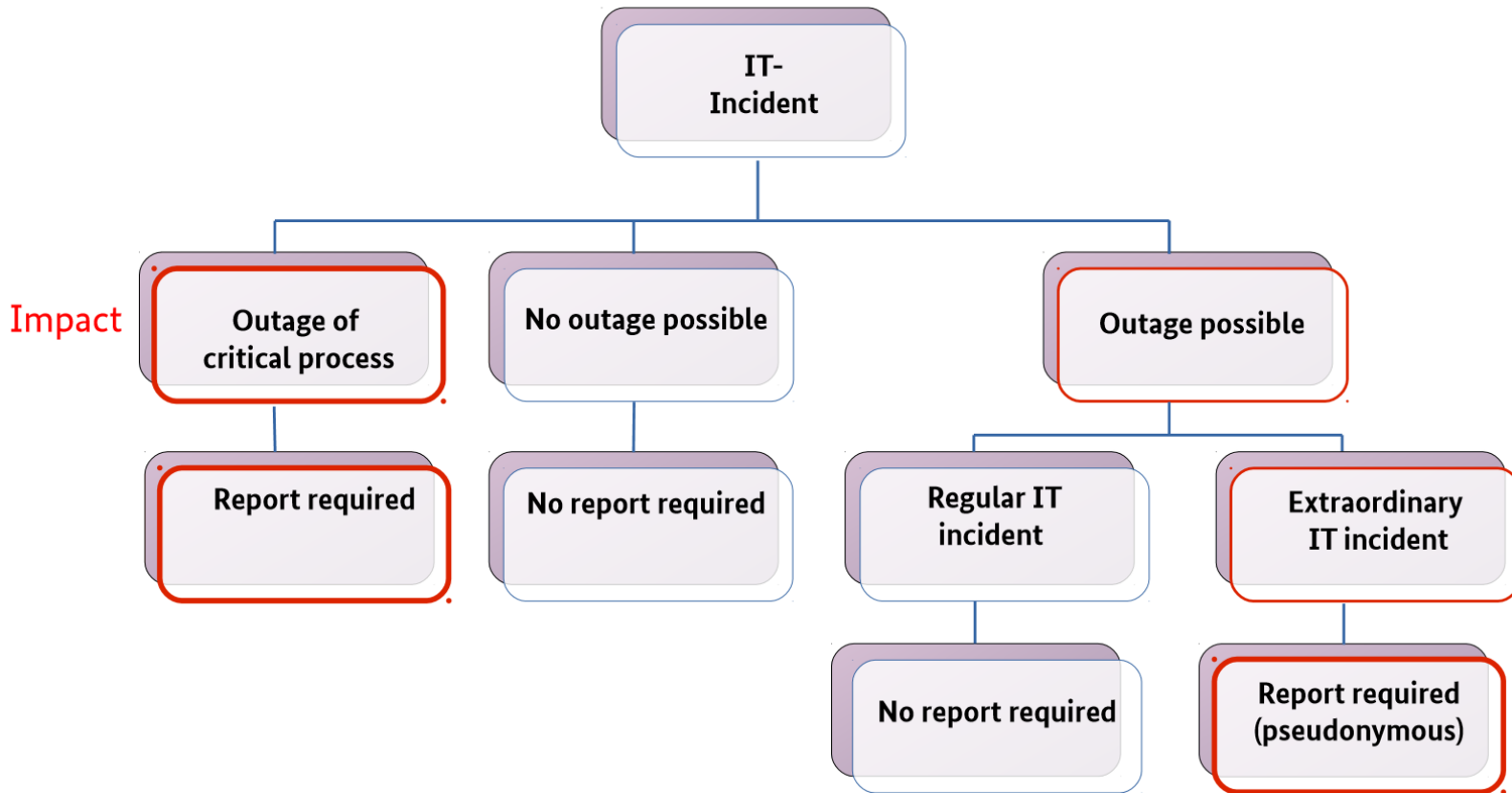
Source: Olaf Götz (BMI) & Jens Wiesner (BSI) "Germany's Cyber Security Situation and the ITSecAct" 2016.09.15

Overall Facilities in Scope



Source: Olaf Götz (BMI) & Jens Wiesner (BSI) "Germany's Cyber Security Situation and the ITSecAct" 2016.09.15

Incident Reporting Requirements



Source: Olaf Götz (BMI) & Jens Wiesner (BSI) "Germany's Cyber Security Situation and the ITSecAct" 2016.09.15

Security Act Applicability to Software Supply Chain

§ 8b (6) BSIG

Zentrale Stelle für die Sicherheit in der
Informationstechnik Kritischer Infrastrukturen



(6) Soweit erforderlich kann das Bundesamt vom Hersteller der betroffenen informationstechnischen Produkte und Systeme die Mitwirkung an der Beseitigung oder Vermeidung einer Störung nach Absatz 4 verlangen. Satz 1 gilt für Störungen bei Betreibern und Genehmigungsinhabern im Sinne von § 8c Absatz 3 entsprechend.

BSI may demand from

Vendors of products or systems

containing vulnerabilities

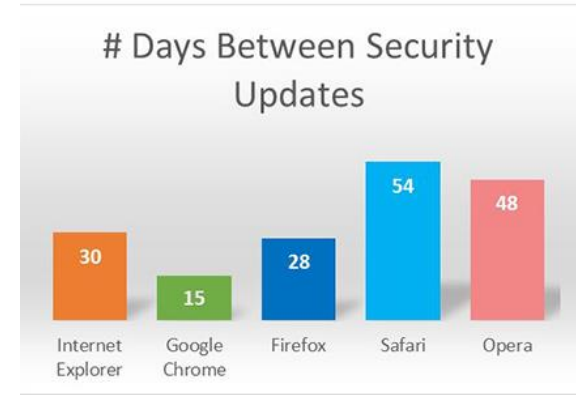
participation

in their removal or mitigation

(6) Soweit erforderlich kann das Bundesamt vom Hersteller der betroffenen informationstechnischen Produkte und Systeme die Mitwirkung an der Beseitigung oder Vermeidung einer Störung nach Absatz 4 verlangen. Satz 1 gilt für Störungen bei Betreibern und Genehmigungsinhabern im Sinne von § 8c Absatz 3 entsprechend.

(6) Soweit erforderlich kann das Bundesamt vom Hersteller der betroffenen informationstechnischen Produkte und Systeme die Mitwirkung an der Beseitigung oder Vermeidung einer Störung nach Absatz 4 verlangen. Satz 1 gilt für Störungen bei Betreibern und Genehmigungsinhabern im Sinne von § 8c Absatz 3 entsprechend.

Source: Olaf Götz (BMI) & Jens Wiesner (BSI) "Germany's Cyber Security Situation and the ITSecAct" 2016.09.15



What about Vulnerabilities?

Ethical Disclosure

- Disclose vulnerabilities in a predictable and reliable process
- Provide actionable information
- Empower our customers, not would-be attackers



Ethical Disclosure Policy
for Software Code vulnerabilities

<https://techsupport.osisoft.com/Troubleshooting/Ethical-Disclosure-Policy>

Vulnerability Disclosure Process

OSIsoft Discovered Vulnerabilities

- Generate remediation plan and security bulletins for high and medium level issues
- Communicate actionable information: release of a product update, avoidance procedure, ...
- Release security bulletins on the 2nd Tuesday of the month
- Communicate with customers and partners one month prior to any public service (example: ICS-CERT)

3rd Party Discovered Vulnerabilities

- Work with the 3rd party to replicate the **OSIsoft Discovered Vulnerability** process
- Adjust as necessary to keep the 3rd party engaged as a partner in the resolution
- Engage the 3rd party in testing the actionable information before release
- Recognize the 3rd party's work, give them the recognition they deserve

Actively-exploited Vulnerabilities

- Actively engage partners and customers with recommended defenses and guidance on vulnerabilities being exploited
- Engage with customers immediately, do not wait to follow the regular cycle of patch or software release
- Provide software updates addressing vulnerabilities as soon as available
- Involves senior leadership within the company to ensure adequacy of resources and timeliness of response



Incident Response is a Community of Interest

- OSIssoft Technical Support
- secure@osisoft.com
- National CERTs



Response is last but not least, Be Prepared!

Contact Information

Bryan Owen PE

bryan@osisoft.com

Principle Cyber Security Manager
OSIsoft

Stay tuned for exciting news about security updates on Day 3
“What’s New in PI Security”

Thursday 15:45-16:15 (Techcon Track 2 in Potsdam III)

Also visit the Cyber Security Expo Pod

Questions

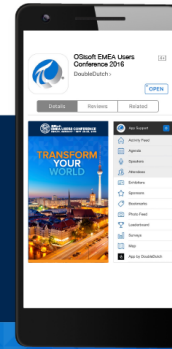
Please wait for the **microphone** before asking your questions



State your **name & company**

Please remember to...

Complete the Online Survey for this session



Download the Conference App for **OSISOFT EMEA Users Conference 2016**

- View the latest agenda and create your own
- Meet and connect with other attendees



search **OSISOFT** in the app store

<http://ddut.ch/osisoft>



감사합니다

谢谢

Danke

Merci

Gracias

Thank You

ありがとう

Спасибо

Obrigado



OSIsoft.

EMEA USERS CONFERENCE • BERLIN, GERMANY

© Copyright 2016 OSIsoft, LLC



OSIsoft®

EMEA USERS CONFERENCE

BERLIN, GERMANY • SEPT 26-29, 2016



OSIsoft.

EMEA USERS CONFERENCE • BERLIN, GERMANY

© Copyright 2016 OSIsoft, LLC