Energy Intrusion Detection 2019

Protecting BKW's Electrical Energy Production and Power Grid Environments

An Active Monitoring Use Case

Amsterdam, January 30, 2019

BKW

Fra, 30. November 2016

About BKW

The **BKW** Group is a Bern-based international energy and infrastructure company employing about 7,000 people.

Its company network and extensive expertise allow it to offer its customers a full range of overall solutions. The Group plans, builds and operates infrastructure to produce **Energy** and supply it through its **Power Grid** to businesses, households and the public sector, and offers digital business models for renewable energies.

In addition, the BKW Group portfolio comprises everything from **Engineering** consultancy and planning for energy, infrastructure and environmental projects, through integrated offers in the field of **Building Solutions**, to the construction and maintenance of **Infra Services** for energy, telecommunications, transport and water networks.

BKW POWER GRID

BKW ENERGY

BKW INFRA SERVICES

BKW ENGINEERING

BKW BUILDING SOLUTIONS

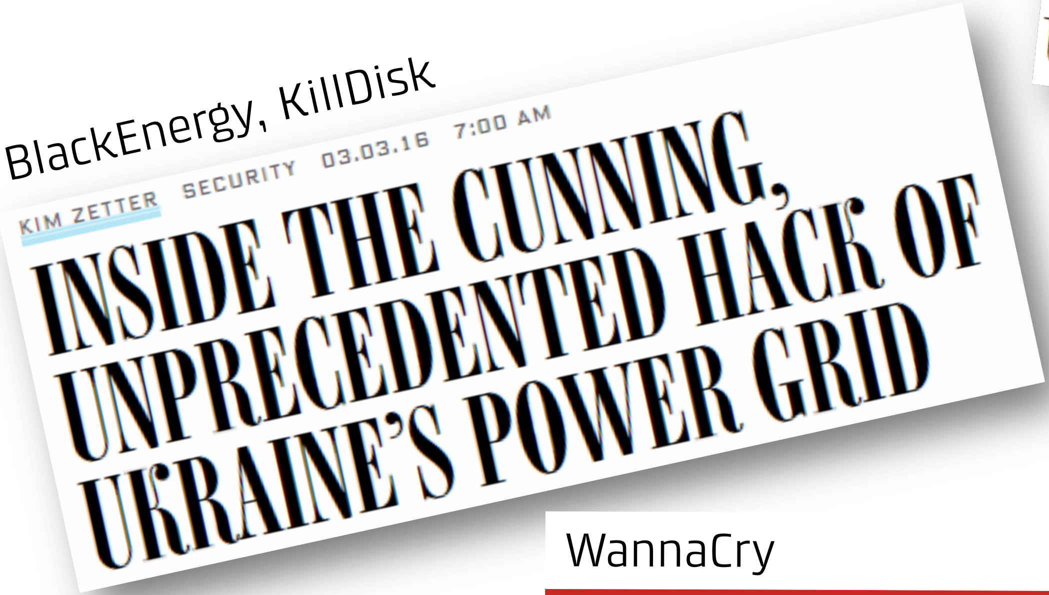
Understand The Threats

	Attackers		Motives
Dangerous (Critical Infrastructures)	Nations / Government Agencies		Sabotage Espionage
Dangerous (Intellectual Property)	Corporations, Industries & Economic		Espionage
Most probable	Organized Crime		Blackmailing
	Terrorists	→	Most scaring Damage
	Activists	→	Exposure
	Hobby Hackers	→	Self-Affirmation
Involved in 45 - 60 % of the Attacks	Internal & external Collaborators	→	All of the above

Most dangerous

Follow The Attacks

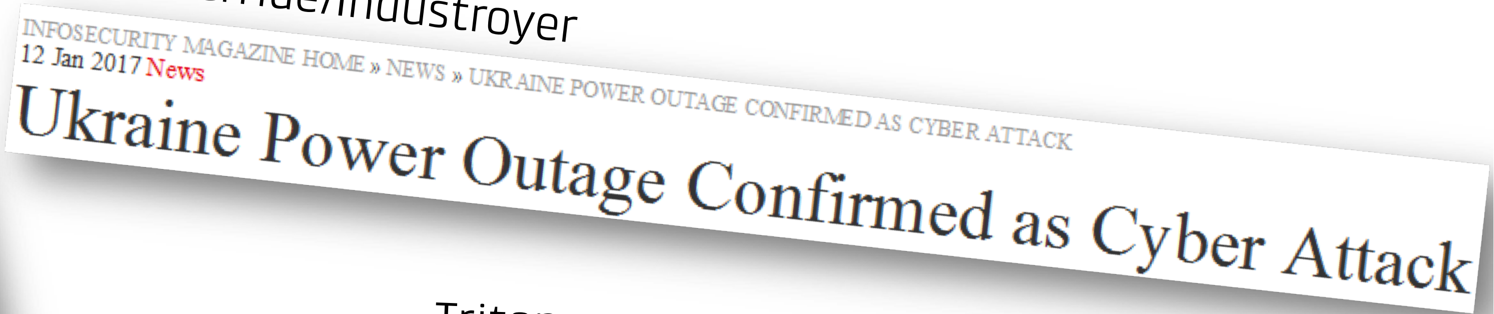
BlackEnergy, KillDisk



KIM ZETTER SECURITY 03.03.16 7:00 AM

INSIDE THE CUNNING, UNPRECEDENTED HACK OF UKRAINE'S POWER GRID

CrashOverride/Industroyer



INFOSECURITY MAGAZINE HOME » NEWS » UKRAINE POWER OUTAGE CONFIRMED AS CYBER ATTACK

12 Jan 2017 News

Ukraine Power Outage Confirmed as Cyber Attack

Triton

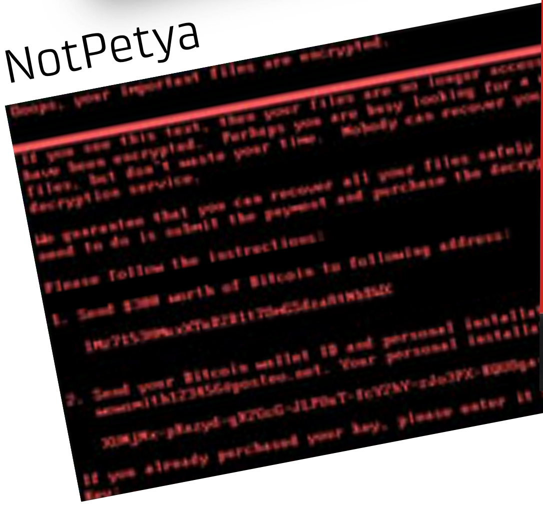
The Guardian

Fri 15 Dec 2017 11.14 GMT

Triton: hackers take out safety systems in 'watershed' attack on energy plant

Sophisticated malware halts operations at power station in unprecedented attack

NotPetya



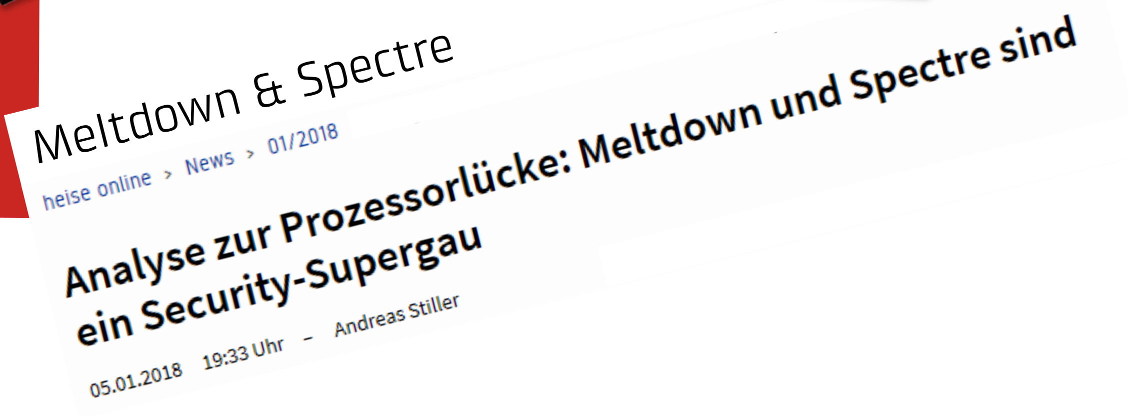
```
Ooops, your important files are encrypted.
If you see this text, then your files are no longer access
have been encrypted. Perhaps you are busy looking for a
files, but don't waste your time. Nobody can recover you
decryption service.
We guarantee that you can recover all your files safely
need to do is submit the payment and purchase the decry
Please follow the instructions:
1. Send $300 worth of Bitcoin to following address:
   1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX
2. Send your Bitcoin wallet ID and personal installa
   wowsmith123456@posteo.net. Your personal installa
   [illegible]-JLPDeT-fcY2kY-zJe3PX-EQQQg4
   XXMjMx-pRazyd-gX2GcG
If you already purchased your key, please enter it
Key:
```

WannaCry

WannaCry Ransomware Attack

Patch for Unsupported Windows (Apply Now)

Meltdown & Spectre

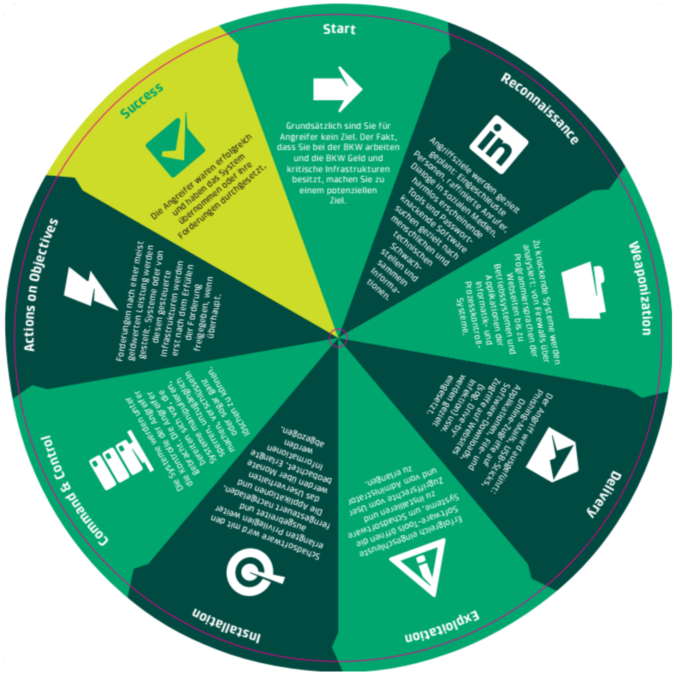


heise online › News › 01/2018

Analyse zur Prozessorlücke: Meltdown und Spectre sind ein Security-Supergau

05.01.2018 19:33 Uhr – Andreas Stiller

Understand The Cyber Kill Chain



Start

Grundsätzlich sind Sie für Angreifer kein Ziel. Der Fakt, dass Sie bei der BKW arbeiten und die BKW Geld und kritische Infrastrukturen besitzt, machen Sie zu einem potenziellen Ziel.

Reconnaissance

Angriffsziele werden gezielt geplant: Eingeschleuste Personen, raffinierte Anrufer, Dialoge in sozialen Medien, harmlos erscheinende Tools und Passwort-knackende Software suchen gezielt nach menschlichen und technischen Schwachstellen und sammeln Informationen.

Weaponization

Zu knackende Systeme werden analysiert: von Firewalls über Programmiersprachen der Webseiten bis zu Betriebssystemen und Applikationen der Informatik- und Prozesskontroll-Systeme.

Delivery

Der Angriff wird ausgeführt: Phishing-Mails, USB-Sticks, Online-Zugriffe auf Applikationen, File- und Software-Downloads, Zugriffe auf Websites (sog. Drive-by-Infektion) usw. werden gezielt eingesetzt.

Exploitation

Erfolgreich eingeschleuste Software-Tools öffnen die Systeme, um Schadsoftware zu installieren und Zugriffsrechte vom User und vom Administrator zu erlangen.

Installation

Schadsoftware wird mit den erlangten Privilegien weiter ausgebreitet und ferngesteuert nachgeladen. Die Applikationen und das Userverhalten werden über Monate beobachtet. Erlangte Informationen werden abgezogen.

Command & Control

Die Systeme werden unter die Kontrolle der Angreifer gebracht. Die Angreifer bereiten sich vor, die Systeme manipulieren, unzugänglich machen, verschlüsseln, sperren, oder sogar ganz löschen zu können.

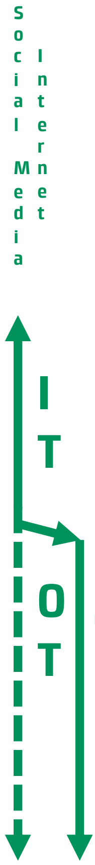
Actions on Objectives

Forderungen nach einer meist geldwerten Leistung werden gestellt. Systeme oder von diesen gesteuerte Infrastrukturen werden erst nach dem Erfüllen der Forderung freigegeben, wenn überhaupt.

Success

Die Angreifer waren erfolgreich und haben das System übernommen oder ihre Forderungen durchgesetzt.

IT = Information Technology
OT = Operational Technology



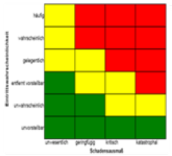
Start	BKW may be identified as a target for its funds and critical infrastructure.
Reconnaissance	Intruder researches target, and attempts to identify vulnerabilities in it.
Weaponization	Intruder creates remote access malware weapon tailored to vulnerabilities.
Delivery	Initial Infection: (Spear) Phishing, USB Sticks, CEO-Fraud, Social Engineering, Malware Downloads, Fake Password Change, Watering Hole
Exploitation	Malware code triggers, escalates privileges and takes action on target to exploit vulnerability.
Installation	Malware installs access point (e.g., "backdoor") usable by intruder's command & control networks.
Command & Control	Malware enables intruder to have persistent access to target network.
Actions on Objectives	Intruder takes action, such as data exfiltration, destruction, or encryption.

A successful attack is only a matter of time and resources invested

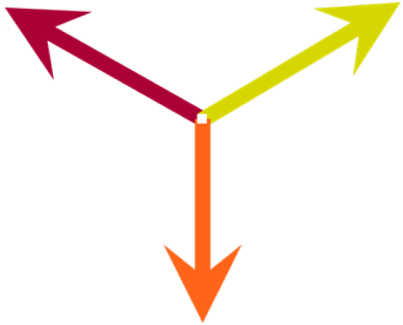
Define Your Strategy and Have IT Approved by The Board

ESTABLISH GOVERNANCE

PROACT, DETECT, REACT
Reach Resilience
Know the Risks and make them manageable
Recognize & Cope with Attacks



BECOME & STAY AWARE
Create Awareness
Reach Acceptance both, at Work and at Home



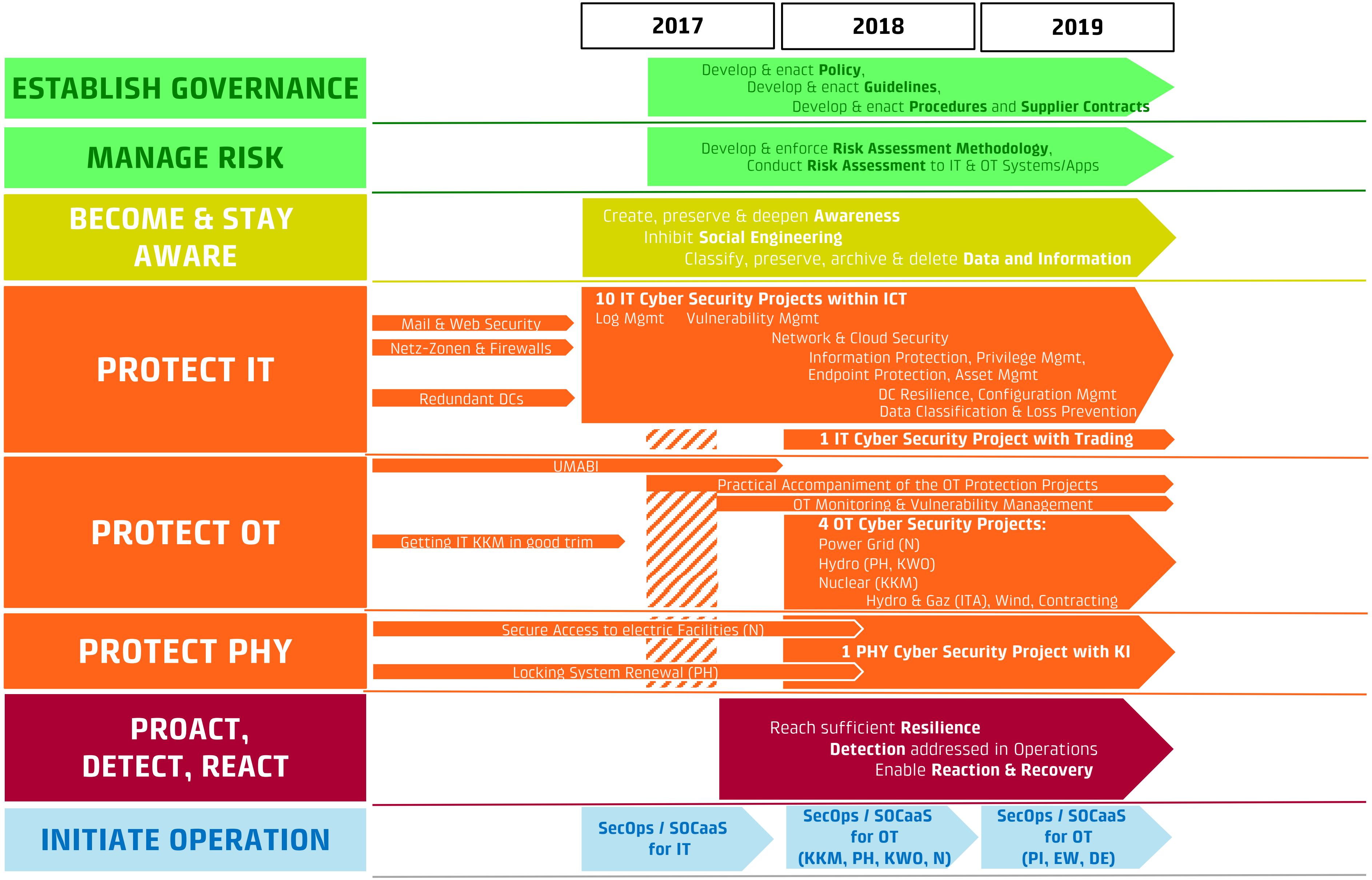
MANAGE RISK

PROTECT IT, OT, PHY
Take Measures
Get IT & OT in good trip and keep it secure

INITIATE OPERATION

IT = Information Technology
OT = Operational Technology

Setup The Programme



2017 | 2018 | 2019

ESTABLISH GOVERNANCE

Develop & enact **Policy**,
Develop & enact **Guidelines**,
Develop & enact **Procedures** and **Supplier Contracts**

MANAGE RISK

Develop & enforce **Risk Assessment Methodology**,
Conduct **Risk Assessment** to IT & OT Systems/Apps

BECOME & STAY AWARE

Create, preserve & deepen **Awareness**
Inhibit **Social Engineering**
Classify, preserve, archive & delete **Data and Information**

PROTECT IT

Mail & Web Security
Netz-Zonen & Firewalls
Redundant DCs

10 IT Cyber Security Projects within ICT
Log Mgmt Vulnerability Mgmt
Network & Cloud Security
Information Protection, Privilege Mgmt,
Endpoint Protection, Asset Mgmt
DC Resilience, Configuration Mgmt
Data Classification & Loss Prevention

1 IT Cyber Security Project with Trading

PROTECT OT

UMABI
Practical Accompaniment of the OT Protection Projects
OT Monitoring & Vulnerability Management
Getting IT KKM in good trim

4 OT Cyber Security Projects:
Power Grid (N)
Hydro (PH, KWO)
Nuclear (KKM)
Hydro & Gaz (ITA), Wind, Contracting

PROTECT PHY

Secure Access to electric Facilities (N)
Locking System Renewal (PH)
1 PHY Cyber Security Project with KI

PROACT, DETECT, REACT

Reach sufficient **Resilience**
Detection addressed in Operations
Enable **Reaction & Recovery**

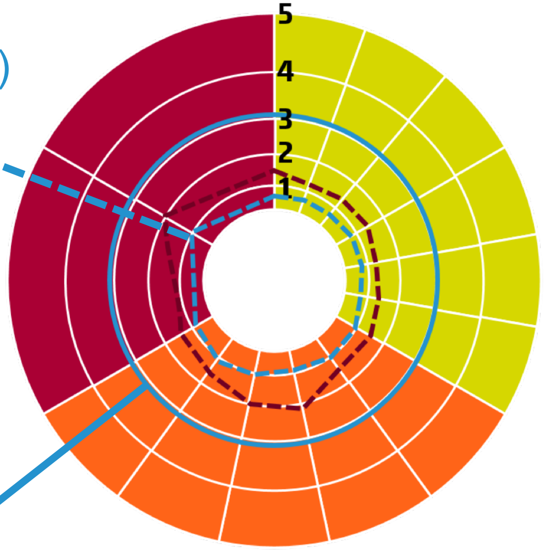
INITIATE OPERATION

SecOps / SOCaaS for IT
SecOps / SOCaaS for OT (KKM, PH, KWO, N)
SecOps / SOCaaS for OT (PI, EW, DE)

Set and Measure The Target

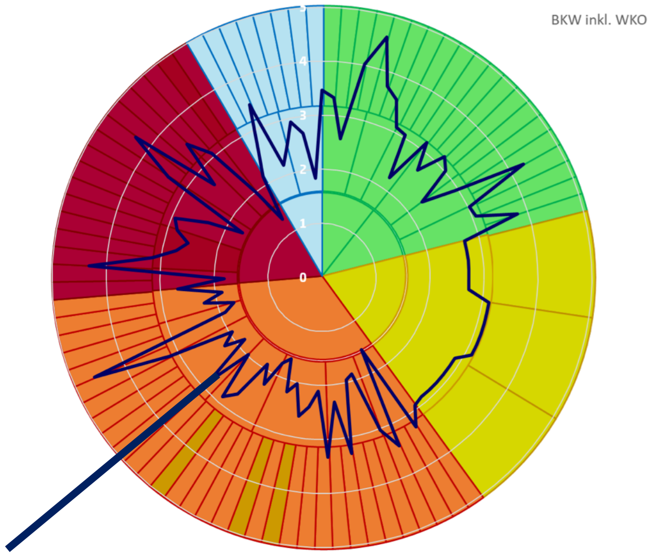
CMMI Cybermaturity 2015 & 2016

Start
(2015, 2016)



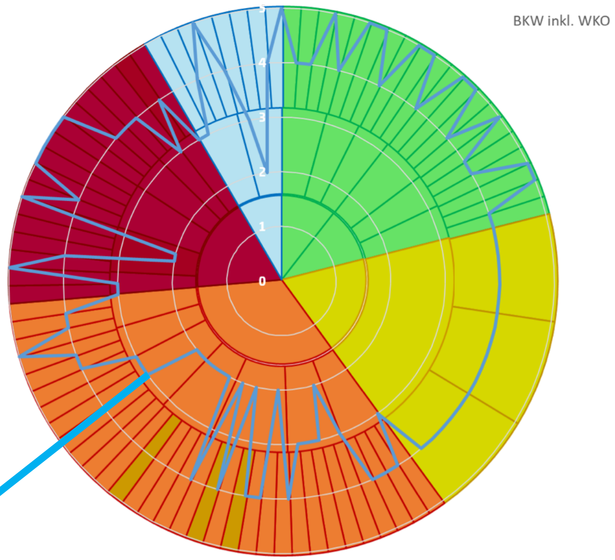
Target 2019
(2015)

CMMI Cybermaturity State Mid 2018



State 2018

CMMI Cybermaturity Actual Target 2019



Target 2019
(2018)

Use an Established Method: The CMMI Cybermaturity Platform

In April 2018 the CMMI Institute launched a Platform (SaaS) for the risk-based Assessment of the Cybersecurity Maturity of an Organisation.

I had and continue to have the opportunity to accompany the CMMI Institute during the development and implementation of its CMMI Cybermaturity Platform.

It is my pleasure to give you a brief overview of the method and its application with the BKW Group as a whole and with seven of its Units.

① You determine your Risk Profil which in turn determines your Maturity Targets,

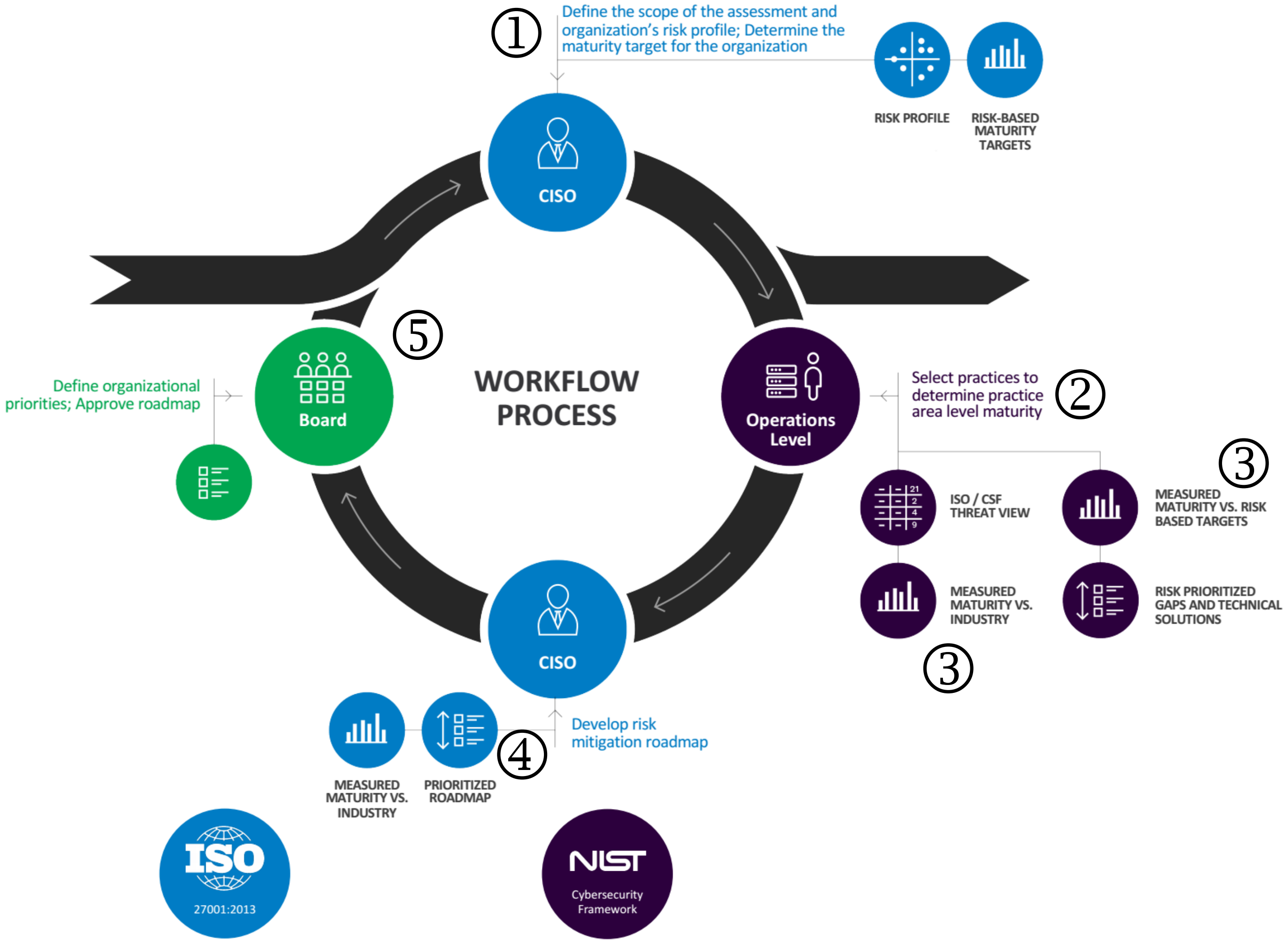
② You gather your Cybersecurity Maturity,

③ You compare it with your Targets & your Peers,

④ You get a risk prioritized Roadmap and

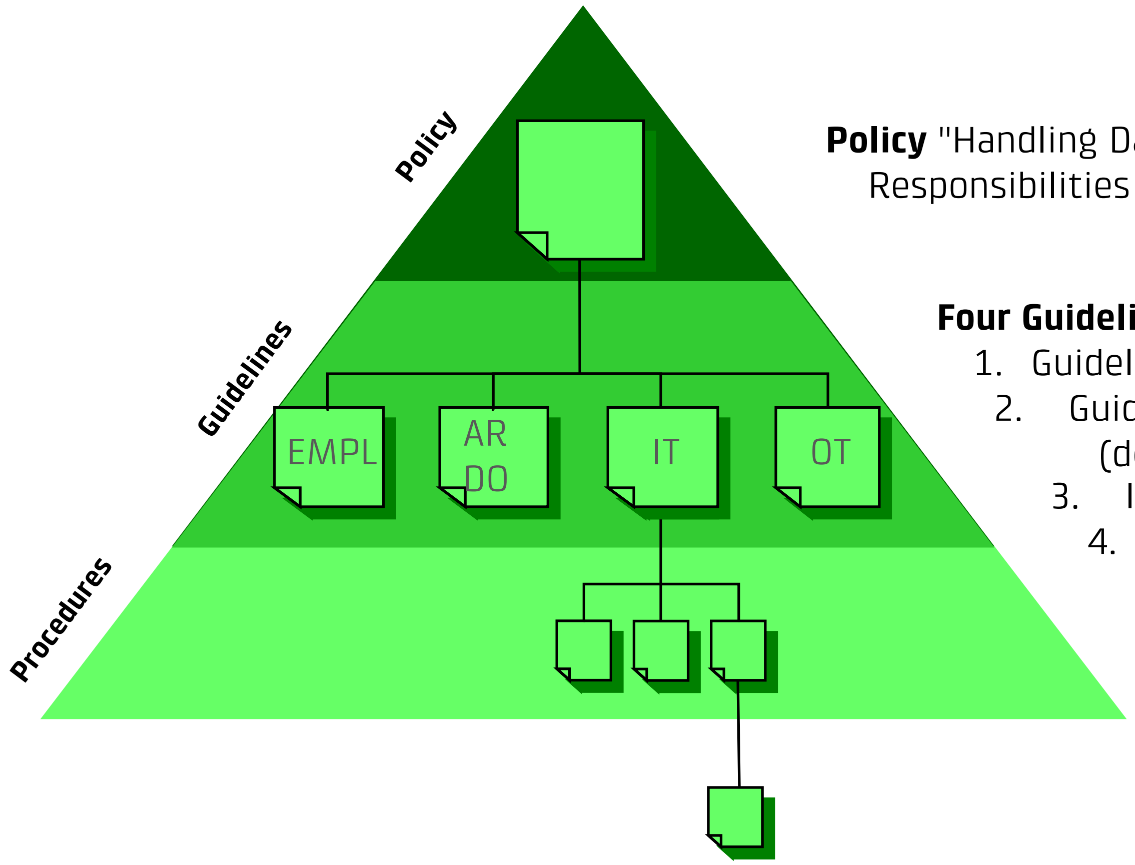
⑤ You present the Results to the ExCom and the BoD.

Finally you get a mapping of your Compliance with ISO 27001/27002, NIST CSF and further Standards.


①
Define the scope of the assessment and organization's risk profile; Determine the maturity target for the organization
RISK PROFILE
RISK-BASED MATURITY TARGETS
CISO
⑤
Board
Define organizational priorities; Approve roadmap
WORKFLOW PROCESS
Operations Level
Select practices to determine practice area level maturity
②
③
ISO / CSF THREAT VIEW
MEASURED MATURITY VS. RISK BASED TARGETS
MEASURED MATURITY VS. INDUSTRY
RISK PRIORITIZED GAPS AND TECHNICAL SOLUTIONS
③
CISO
Develop risk mitigation roadmap
④
MEASURED MATURITY VS. INDUSTRY
PRIORITIZED ROADMAP
ISO 27001:2013
NIST Cybersecurity Framework

CMMI Institute

Establish The Governance



Policy "Handling Data and Information Safely"
Responsibilities & Principles for the whole BKW Group
-> *aimed at all Employees, specially to BU-Leaders and GMs*

Four Guidelinies: -> *address specific Target Audiences*

1. Guideline for Employees
2. Guideline for Business Functions
   (defining e.g. Application Responsibles & Data Owners)
3. IT Guideline
4. OT Guideline

Standard Operating Procedures
Generic, independent of Products / Releases

Technical Operating Procedures
Product- / Release-dependant Instructions

Supplier Contracts
Model contract with Appendices

Become & Stay Aware

Our Slogan is:

Ready. Safe? Go!

Step by Step towards a cybersafe BKW

- The Flyer

Liebe Kolleginnen, liebe Kollegen

[illegible]

Ihre Suzanne Thoma

2017 2018 2019

3 Schritte für mehr Sorgfalt.

Geben Sie Schadsoftware keine Chance

[illegible]

Schützen Sie Ihren Computer

[illegible]

Verschlüsseln Sie vertrauliche Dokumente

[illegible]

3 Schritte für mehr Vorsicht.

Sprechen Sie unbekannte Personen an

[illegible]

Verbinden Sie sich unterwegs mit sicheren Netzen

[illegible]

Aktualisieren Sie regelmässig Betriebssysteme und Software

[illegible]

3 Schritte für mehr Offenheit.

Übergreifend zusammenarbeiten

[illegible]

Missgeschick? Kann passieren

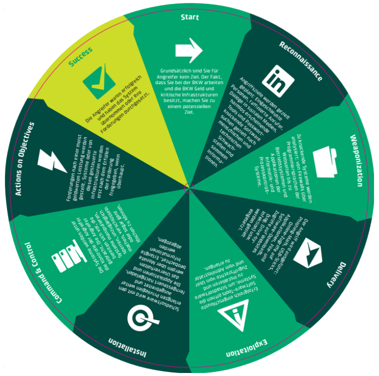
[illegible]

Melden Sie Verdachtsfälle

[illegible]

- The Training

- The Kill Chain



Start

Grundsätzlich sind Sie für Angreifer kein Ziel. Der Fakt, dass Sie bei der BKW arbeiten und die BKW Geld und kritische Infrastrukturen besitzt, machen Sie zu einem potenziellen Ziel.

Reconnaissance

Angriffsziele werden gezielt geplant: Eingeschleuste Personen, raffinierte Anrufer, Dialoge in sozialen Medien, harmlos erscheinende Tools und Passwort-knackende Software suchen gezielt nach menschlichen und technischen Schwachstellen und sammeln Informationen.

Weaponization

Zu knackende Systeme werden analysiert: von Firewalls über Programmiersprachen der Webseiten bis zu Betriebssystemen und Applikationen der Informatik- und Prozesskontroll-Systeme.

Delivery

Der Angriff wird ausgeführt: Phishing-Mails, USB-Sticks, Online-Zugriffe auf Applikationen, File- und Software-Downloads, Zugriffe auf Websites (sog. Drive-by-Infektion) usw. werden gezielt eingesetzt.

Exploitation

Erfolgreich eingeschleuste Software-Tools öffnen die Systeme, um Schadsoftware zu installieren und Zugriffsrechte vom User und vom Administrator zu erlangen.

Installation

Schadsoftware wird mit den erlangten Privilegien weiter ausgebreitet und ferngesteuert nachgeladen. Die Applikationen und das Userverhalten werden über Monate beobachtet. Erlangte Informationen werden abgezogen.

Command & Control

Die Systeme werden unter die Kontrolle der Angreifer gebracht. Die Angreifer bereiten sich vor, die Systeme manipulieren, unzugänglich machen, sperren, verschlüsseln oder sogar ganz löschen zu können.

Actions on Objectives

Forderungen nach einer meist geldwerten Leistung werden gestellt. Systeme oder von diesen gesteuerte Infrastrukturen werden erst nach dem Erfüllen der Forderung freigegeben, wenn überhaupt.

Success

Die Angreifer waren erfolgreich und haben das System übernommen oder ihre Forderungen durchgesetzt.

- The Tips in the Employee Magazine

BKW CYBERSÉCURITÉ

Au poste de travail.

En déplacement.

Et à la maison.

The OT Protection Evaluation – A Human Team Building Exercise

Step 1

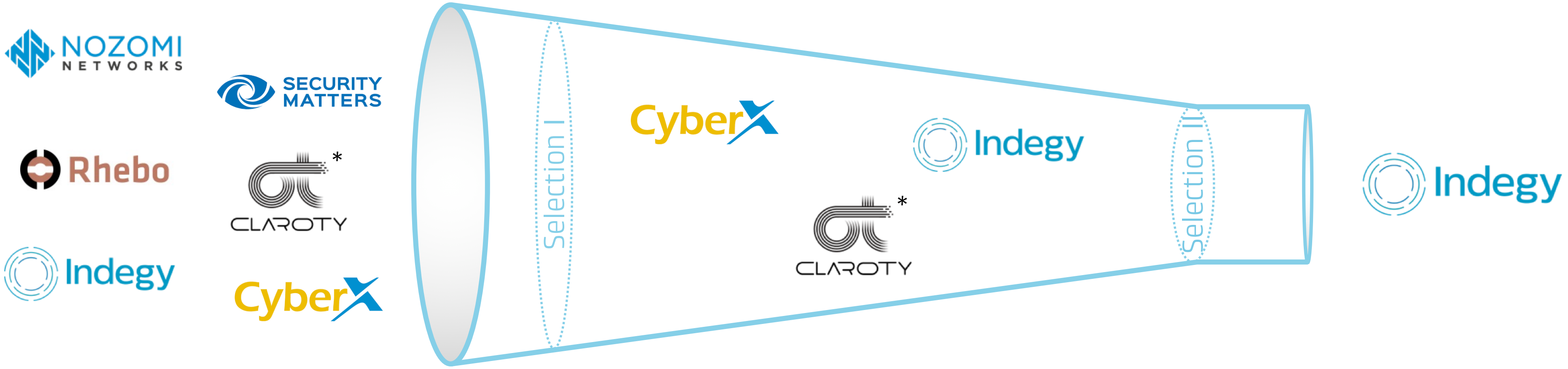
Develop RFI/RFP, Determine Longlist, Run first PoCs with Longlist Providers

Step 2

Hold Comprehensive technical Workshops, Run second PoC with Shortlist Providers

Step 3

Negoziate detailed commercial and technical Terms



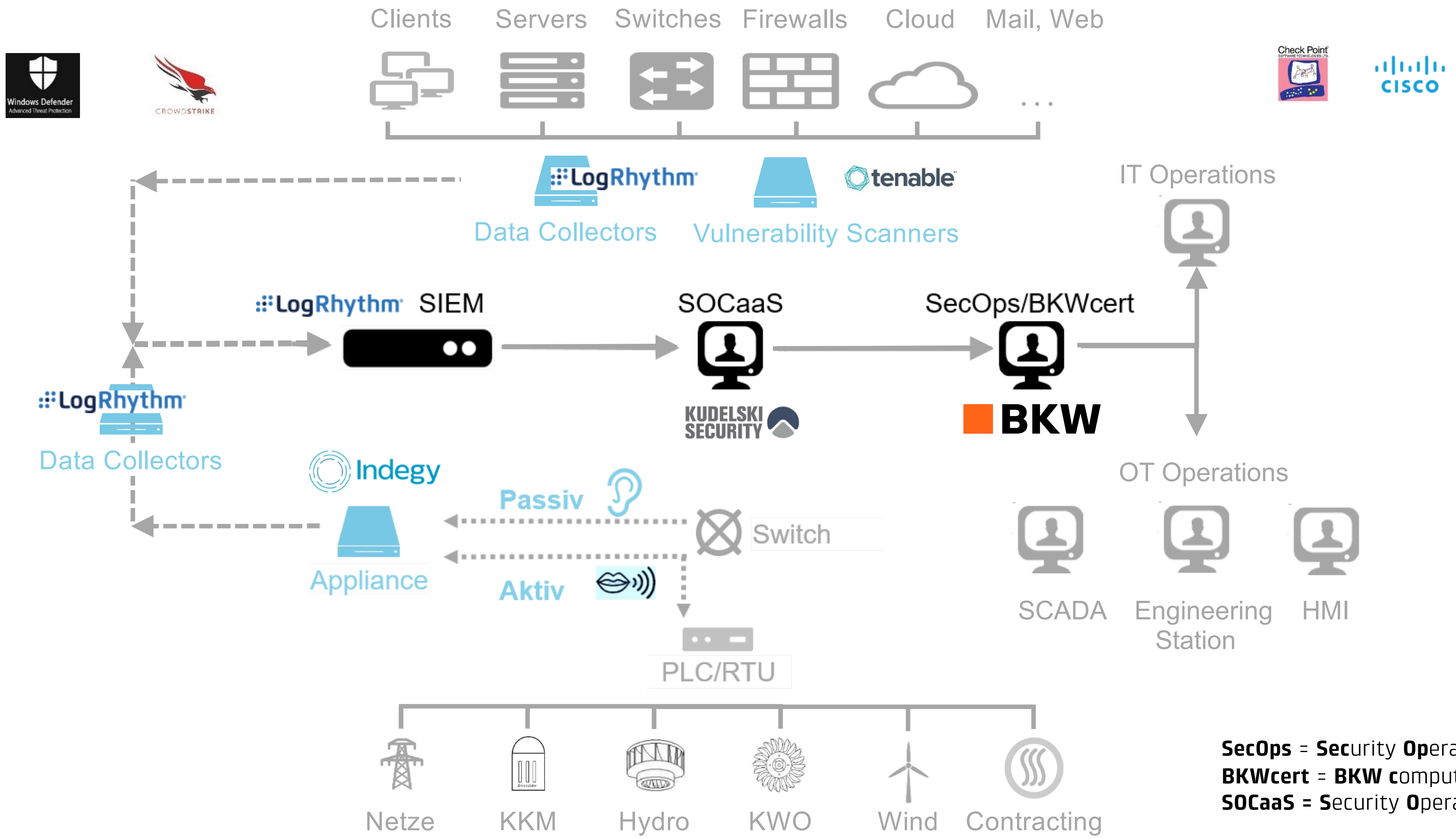
RFI/RFP with over 80 Criteria

On site technical workshops at KWO/BKW

Detailed Purchasing & Service Contracts

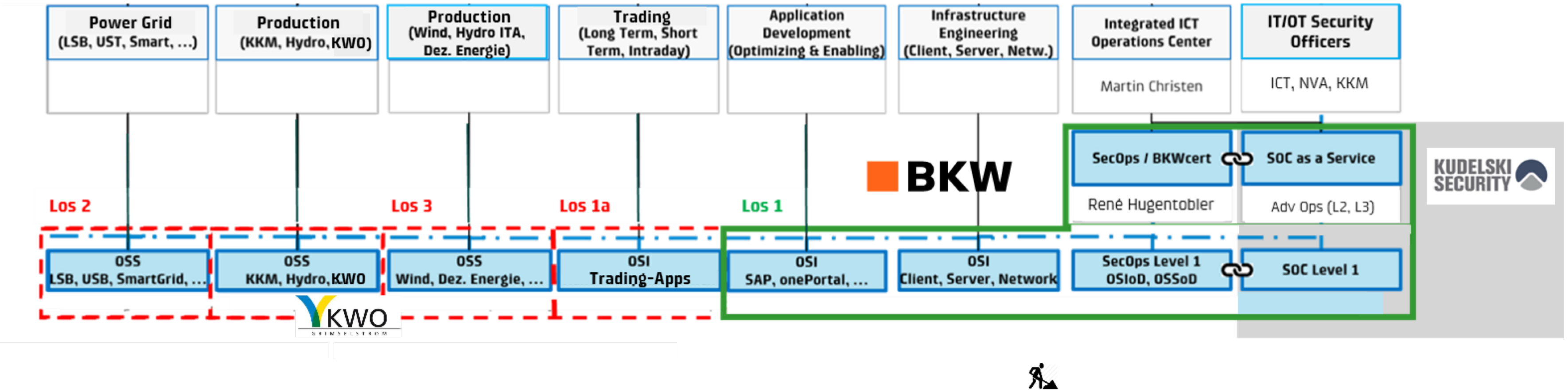
Have The Team Members Socialize with Each Other
Get Top Management to Attend

How IT & OT Protection Play Together



SecOps = **Sec**urity **Op**eration**s**,
BKWcert = **BKW c**omputer **e**mergency **r**esponse **t**eam,
SOCaaS = **S**ecurity **O**perations **C**enter **a**s **a S**ervice

The virtual Security Operations Center – Everyone Concentrates on His Strenghts


Power Grid (LSB, UST, Smart, ...)
Production (KKM, Hydro, KWO)
Production (Wind, Hydro ITA, Dez. Energie)
Trading (Long Term, Short Term, Intraday)
Application Development (Optimizing & Enabling)
Infrastructure Engineering (Client, Server, Netw.)
Integrated ICT Operations Center
Martin Christen
IT/OT Security Officers
ICT, NVA, KKM
BKW
SecOps / BKWcert
René Hugentobler
SOC as a Service
Adv Ops (L2, L3)
KUDELSKI SECURITY
Los 2
Los 3
Los 1a
Los 1
OSS LSB, USB, SmartGrid, ...
OSS KKM, Hydro, KWO
OSS Wind, Dez. Energie, ...
OSI Trading-Apps
OSI SAP, onePortal, ...
OSI Client, Server, Network
SecOps Level 1 OSIoD, OSSoD
SOC Level 1
KWO

1 Line Management down from the ExCom is responsible to have Cyber Security Projects executed and Operations ensured according to the Policy released by the ExCom.

2 The CSO/CISO proposes the Policy to the ExCom, defines the Cyber Security Strategy, runs the Program, releases the Guidelines and steers Operations strategically.

3 The Head ICT provides the Resources (Contract, Finance, Personnel) for the operational Lead of SecOps (SOCaaS, Head SecOps/BKWcert). The Head ICT Operations leads the virtual SOC operationally.

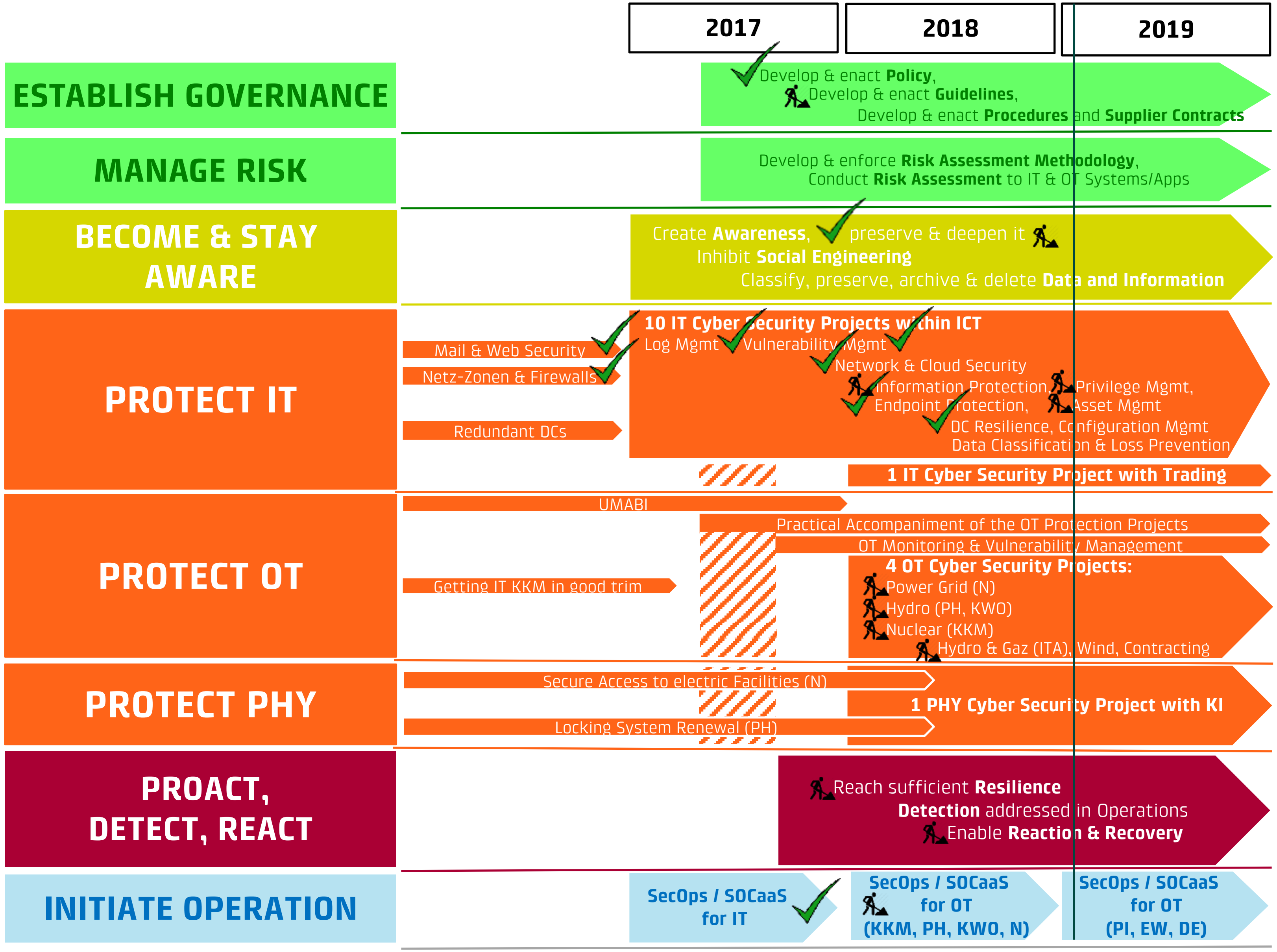
4 The IT/OT Security Officers steer the secure Use of the Applications and Infrastructure in IT & OT by applying the Guidelines. They advise Projects & Operations, in particular the OSIs/OSSs and approve the Procedures.

5 The Department & Team Leaders in **IT** and **OT** and the Application Responsibles (AR) and Data Owners (DO) in the Business Functions ensure the daily Security Operations by assigning, and enabling **O**perational **S**ecurity Engineer **I**T (OSIs) and to **O**perational **S**ecurity Engineers **S**CADA (OSSs). They assign one of each on a weekly basis to the Head SecOps/BKWcert to interface to the SOCaaS.

SCADA = **S**upervisory **C**ontrol **a**nd **D**ata **A**cquisition

The defense will be successful, if the effort of the adversery in relation to his expected return is too high.

The Current State of the Programme



2017 | 2018 | 2019

ESTABLISH GOVERNANCE
✓ Develop & enact **Policy**,
Develop & enact **Guidelines**,
Develop & enact **Procedures** and **Supplier Contracts**

MANAGE RISK
Develop & enforce **Risk Assessment Methodology**,
Conduct **Risk Assessment** to IT & OT Systems/Apps

BECOME & STAY AWARE
Create **Awareness**, ✓ preserve & deepen it
Inhibit **Social Engineering**
Classify, preserve, archive & delete **Data and Information**

PROTECT IT
Mail & Web Security ✓
Netz-Zonen & Firewalls ✓
Redundant DCs
10 IT Cyber Security Projects within ICT
Log Mgmt ✓ Vulnerability Mgmt ✓
✓ Network & Cloud Security
Information Protection, Privilege Mgmt,
✓ Endpoint Protection, Asset Mgmt
✓ DC Resilience, Configuration Mgmt
Data Classification & Loss Prevention
1 IT Cyber Security Project with Trading

PROTECT OT
UMABI
Practical Accompaniment of the OT Protection Projects
OT Monitoring & Vulnerability Management
Getting IT KKM in good trim
4 OT Cyber Security Projects:
Power Grid (N)
Hydro (PH, KWO)
Nuclear (KKM)
Hydro & Gaz (ITA), Wind, Contracting

PROTECT PHY
Secure Access to electric Facilities (N)
1 PHY Cyber Security Project with KI
Locking System Renewal (PH)

PROACT, DETECT, REACT
Reach sufficient **Resilience**
Detection addressed in Operations
Enable **Reaction & Recovery**

INITIATE OPERATION
SecOps / SOCaaS for IT ✓
SecOps / SOCaaS for OT (KKM, PH, KWO, N)
SecOps / SOCaaS for OT (PI, EW, DE)

PinkSquirrel Communication Ideas
CISCO
CISCO
LogRhythm
tenable
zscaler
Microsoft Azure Information Protection
CROWDSTRIKE
now
LogRhythm
Indegy
CMMI Institute
KPMG
KUDELSKI SECURITY
BKW
KWO GRIMSELSTROM

BKW Cyber Security Bericht Dezember 2018

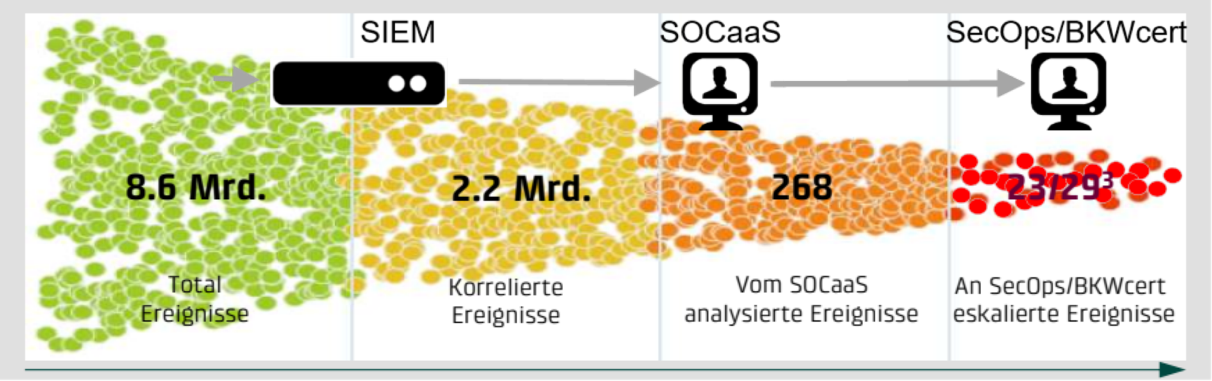
Aktuelle Cyber Security Bedrohungen (Quelle: MELANI et altera)

Publiziert	Name	Vermutl. Ursprung	Kategorie	BKW betroffen	nicht betroffen
6. Dezember	Mail mit falscher Swisscom-Rechnung	Org. Kriminalität od. staatlicher Akteur	Malware	x[1]	
19. Dezember	www.bkw.ch solle angegriffen werden	Aktivisten	Darknet	x[2]	

[1] Mailschutz unvollkommen, Endpoint Detection hat alarmiert

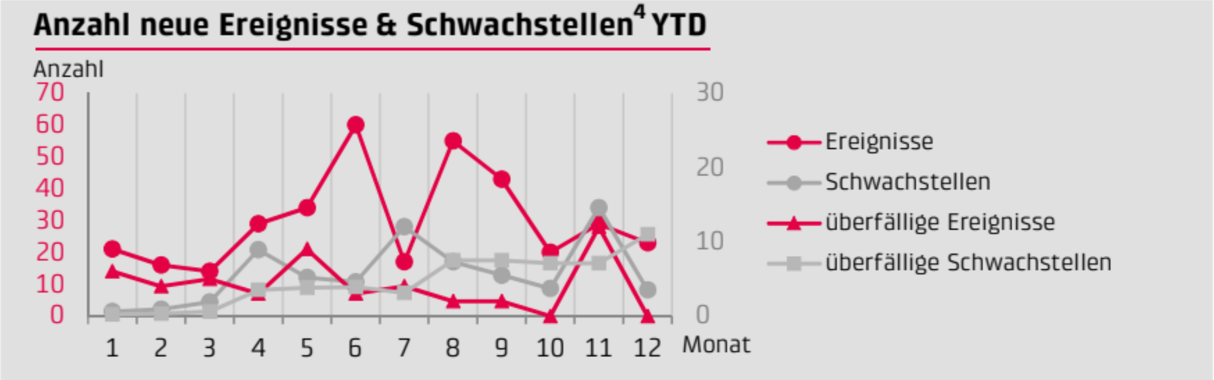
[2] Website verstärkt überwacht, keinen Angriff festgestellt

Ereignisübersicht BKW (Quelle: Kudelski Security SOCaaS für die IT)



[3] Real zu bearbeitende / Total gemeldete Ereignisse

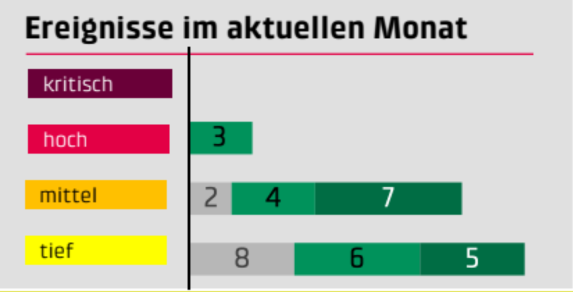
Anzahl neue Ereignisse & Schwachstellen[4] YTD



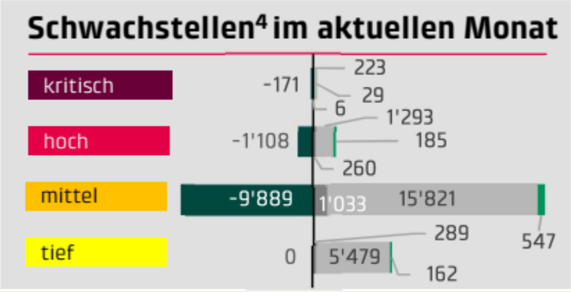
[4] Schwachstellen: Schwachstelle * Anzahl Instanzen in 1000

Bearbeitungsfortschritt Ereignisse und Schwachstellen (Quelle: SecOps/BKWcert, Kudelski Security)

Ereignisse im aktuellen Monat

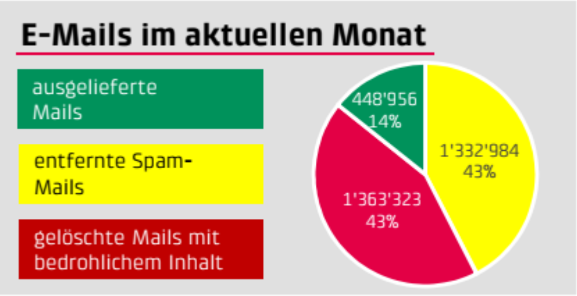


Schwachstellen[4] im aktuellen Monat

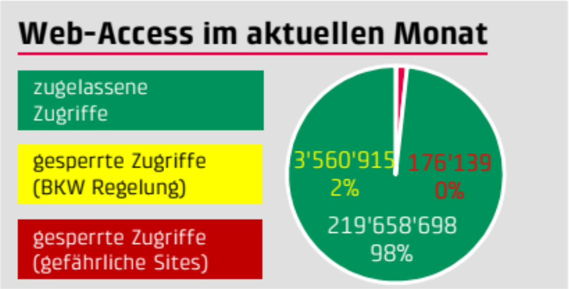


■ überfällig ■ offen (älter) ■ offen (Dezember) ■ erledigt (Dezember) ■ erledigt (älter)

E-Mails im aktuellen Monat



Web-Access im aktuellen Monat



Conclusion

- Start with the Involvement of the Board
- Address Human Factors with Priority
- Involve Top Management Formally & Informally
- Create Cross-Organisational Teams
- Concentrate on Your Strengths, involve Partners with Their Strengths
- Push Responsibility for Process & Doing down the Management Chain as deep as possible
- Use Leading Technology, avoid the Bleeding Edge

Questions?

Thank you for your attention.

Ivo Maritz
Head Cyber Security (CSO/CISO)
ivo.maritz@bkw.ch
www.bkw.ch

BKW