INCIDENCE RESPONSE

WHAT WE CAN LEARN FROM FIREFIGHTERS

CERTivation

intro

- Video from Belgium Firedepartment
- https://www.youtube.com/watch?v=X4NIFi7yDh0

- To get an impression

Overview

- Introduction
- Incidence response – definitions & standards
- Similarities between firefighters and organisations
- Room for improvement
- Training and drilling
- Q&A

Why this Talk?

First idea came up during my qualification to a

- “Gruppenführer” or “section leader”

Talking about that with friends

Final decision during qualification to

- “Zugführer” or “Platoon Leader”

Figuring out there is something that we can learn from us

Stephan Gerling @ObiWan666

I am older than the internet
Certified as “GCFA, CISSP, MCSE, CCNA, etc.”
Electronic Specialist,
several years German Aviation Army navigation system electronic specialist
More than 32 years a volunteer firefighter
Security Evangelist @ROSEN-Group in Oil & Gas Industrie and CERTivation,
I void warranties

Volunteering
- Geraffel („veteran Nerds“)
- IamTheCavalry
- AG Kritis

Stephan Gerling @ObiWan666

Incidence response – definitions & standards

Incidence response…..

Is the last link in a chain of preparation for “the worst case”

- From small to big
- Could start with a phishing mail and end with business loss
- Part of Business continuity, disaster recovery and other Plan’s

Too often only a bullet point on the list

Incidence response – definitions & standards

Incidence response – part of Business Continuity and Risk Management

Incidence response ….. =

- Management
- Process
- Team
- Plan

Real Life scenarios – are u prepared?

Fire in nuclear facility in the neighborhood? (producing uranium fuel rods)

Many firedepartments and special CRN Units alarmed
evacuation of neighbor company could prevented (because of weather)
The day later emergency plan was signed by upper management

Incidence response management

ISO IEC 27035 – Security Incidence response Management

“addresses the development of guidelines to increase the confidence of an organization’s actual readiness to respond to an information security incident.

This is achieved by addressing the policies and plans associated with incident management, as well as how to establish the incident response team and improve its performance over time by adopting lessons learned and by evaluation.”

(https://www.iso.org/obp/ui/fr/#iso:std:iso-iec:27035:-2:ed-1:v1:en)

Computer Security Incident Handling Guide

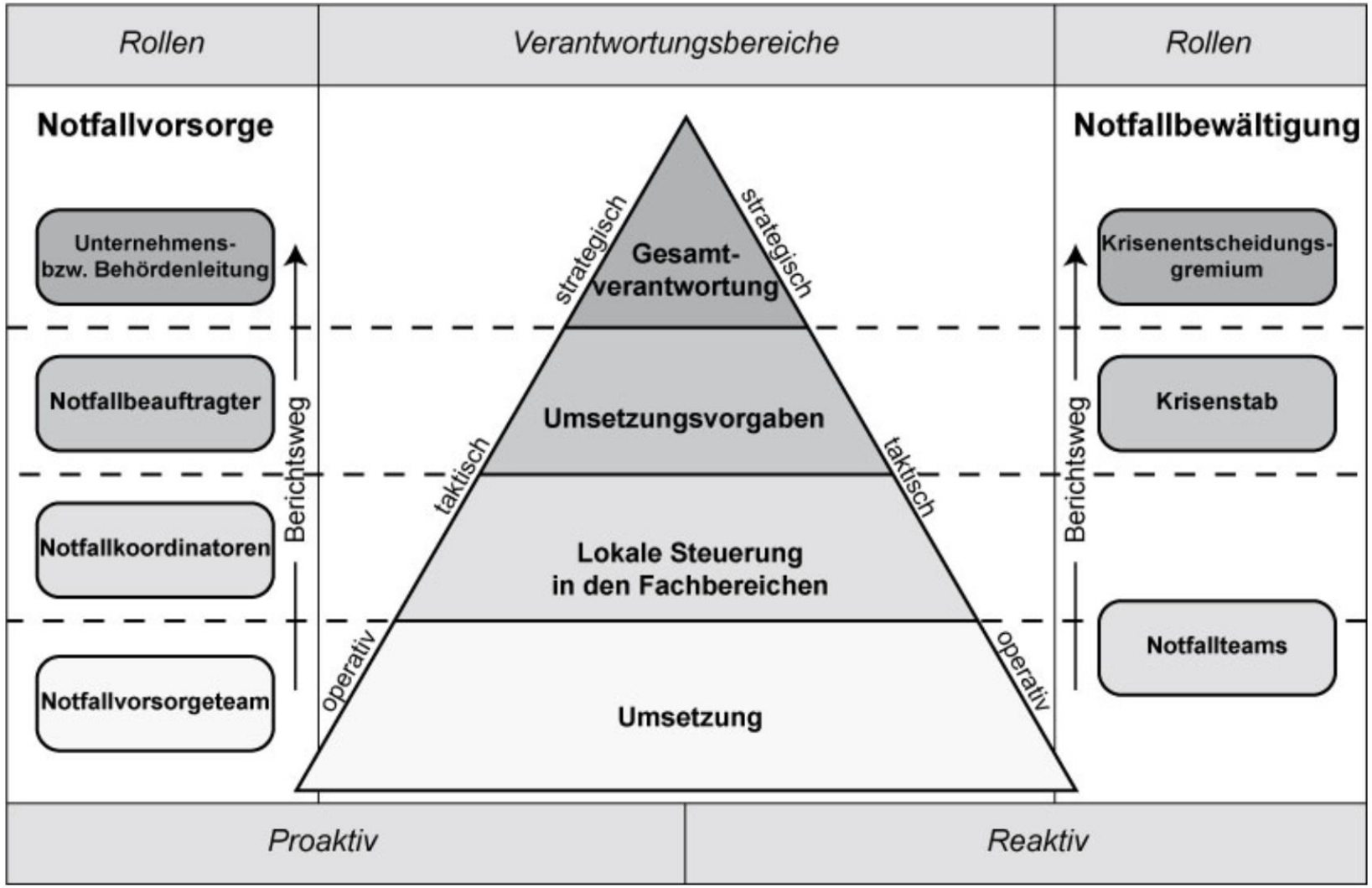
NIST SP 800-61 r2 describes the “Computer Security Incident Handling Guide”

Establishing an incident response capability should include the following actions:

- Creating an incident response policy and plan
- Developing procedures for performing incident handling and reporting
- Setting guidelines for communicating with outside parties regarding incidents
- Selecting a team structure and staffing model
- Establishing relationships and lines of communication between the incident response team and other groups, both internal (e.g., legal department) and external (e.g., law enforcement agencies)
- Determining what services the incident response team should provide
- Staffing and training the incident response team.

(https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf)

BSI Standard 100-4 Notfallmanagement



(https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/Standard04/ITGStandard04_node.html)

Zustaendigkeiten bei der Feuerwehr

3.1.2 Leitung1
Die Leitung ist im Einsatz das gesamtverantwortliche Handeln für eine Einsatzstelle und für die dort eingesetzten Einsatzkräfte.

Führungskräfte der Feuerwehr in leitender Funktion sind also nicht nur für die ihnen jeweils zugeordneten taktischen Einheiten zuständig, sondern für die gesamte Einsatzabwicklung einschließlich der Koordination anderer am Einsatz beteiligter BOS.
Wer die Einsatzleitung hat, bzw. diese übernehmen kann, ergibt sich aus den gesetzlichen Regelungen.

Zustaendigkeiten

Die Unternehmens- bzw. Behördenleitung ist für die institutionsweite Sicherstellung des Notfallmanagements verantwortlich.

Der Notfallbeauftragte steuert alle Aktivitäten rund um die Notfallvorsorge und wirkt bei den damit verbundenen Aufgaben mit.

Er ist für die Erstellung, Umsetzung, Pflege und Betreuung des institutionsweiten Notfallmanagements und der zugehörigen Dokumente und Regelungen zuständig.

Zustaendigkeiten

Krisenentscheidungsgremium

„Im Krisenentscheidungsgremium befinden sich die „Denker“, die die strategische Richtung in der Krise vorgeben und weitreichende Entscheidungen treffen, welche über die festgelegte Kompetenzen des Krisenstabsleiters gehen.“

„Dazu zählen beispielsweise strategische Entscheidungen in Krisen, die über den Geltungsbereich des Notfallmanagements hinausgehen, oder Geschäftsfortführungsstrategien, die längerfristige Auswirkungen auf die Institution haben können“

Beispiel

nCov2019 infection of employees at Automotive supplier

- 27. Jan. first infection
- 28. Jan. Management: no business trips to China for 2 weeks, employees could decide to work in home office
- 29. Jan. 3 new infections, **Management closes Office** up to Sun. 2.2.
- 31. Jan. 6 infected employees
- 2. Feb. 8 infected employees
- 3. Feb. **Closing facility up to 11. Feb.**
- 4. Feb. 10 infected employees

Zustaendigkeiten

Organisation	Feuerwehr
Unternehmens- bzw. Behördenleitung	Einsatzleiter (Zugfuehrer / Ortsbrandmeister / Gemeindebrandmeister)
Krisenstab	Krisenstab
Notfallteams	Loeschzuege
Fachberater	Fachberater

Krisenstab

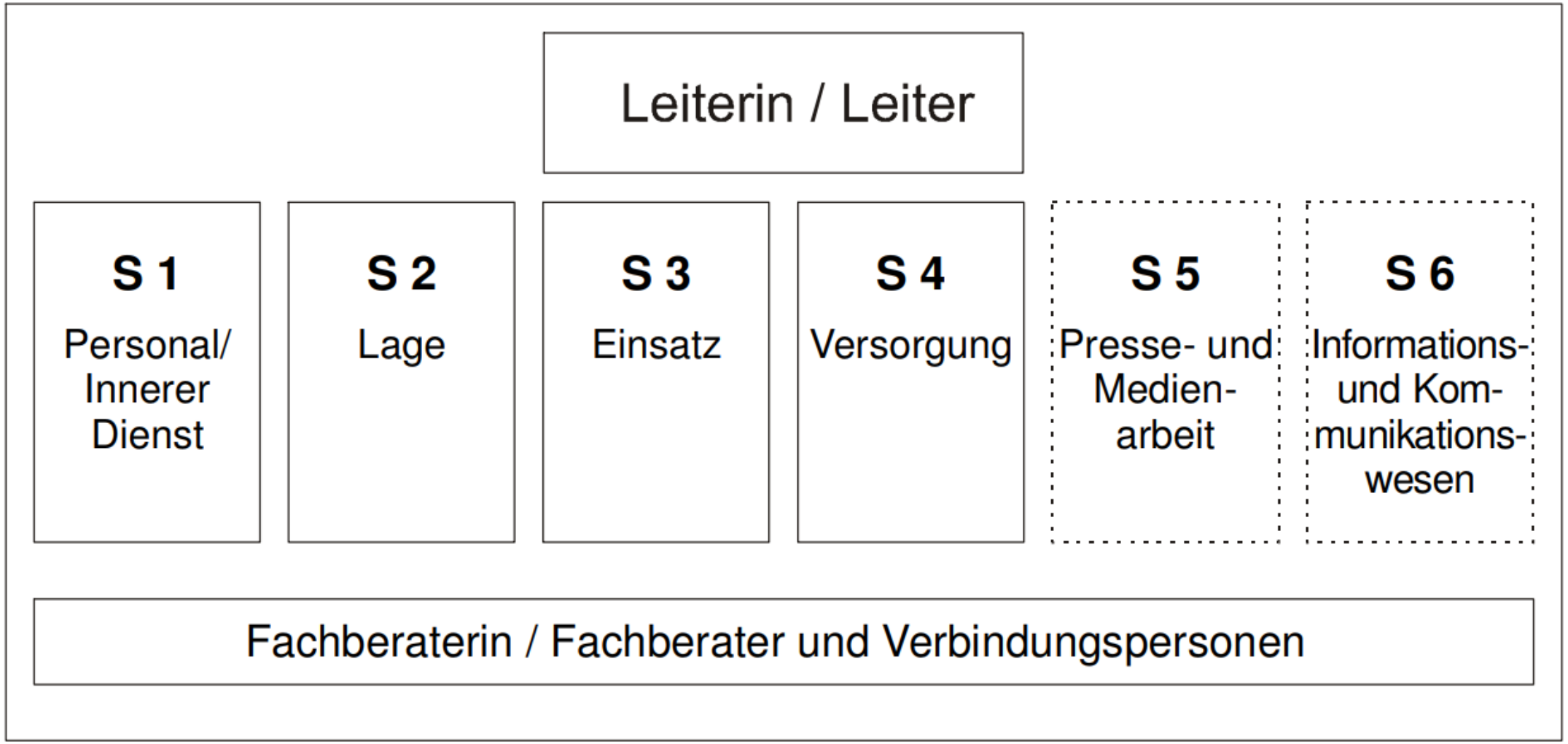
Wie setzt sich ein Krisenstab zusammen?

Krisenstabsleiter und ein bis maximal fünf wichtige Funktionsträger gebildet.

folgende Funktionen haben sich bewährt:

- die Öffentlichkeitsarbeit vertreten durch die Behörden- bzw. Unternehmenskommunikation
- die Behörden- bzw. Unternehmenssicherheit bestehend aus Informationssicherheit wie auch Betriebssicherheit (also Safety und Security).
- Je nach Ausprägung der Institution kann auch ein Vertreter des IT-Betriebs zum Kernteam gehören

Krisenstab bei der Feuerwehr



Definiert in der FwDV 100 – Leitung und Fuehrung

Presse und Medienarbeit (S5)

In Zeiten der Social Media wird die Bedeutung von einem geeigneten Pressesprecher immer wichtiger.

- Es kann aber auch falsch gemacht werden….
- https://www.youtube.com/watch?v=RtOxYOBqUkM

Compare between firefighters #1

Organisations	Firefighters
IR policy and Plan	Brandschutzgesetz
procedures for performing IR	Feuerwehr Dienstvorschriften (FwDV xxx), UVV, etc.
Selecting a team structure and staffing model	Feuerwehr Dienstvorschriften (FwDV xxx)
Staffing and training the incident response team	Feuerwehr Dienstvorschriften (FwDV xxx)

NIST Recommendations

Establish a formal incident response capability.

- Create an incident response policy.
- Develop an incident response plan based on the incident response policy.
- Develop incident response procedures.
- Establish policies and procedures regarding incident-related information sharing.
- Provide pertinent information on incidents to the appropriate organization.
- Consider the relevant factors when selecting an incident response team model.
- Select people with appropriate skills for the incident response team.
- Identify other groups within the organization that may need to participate in IR
- Determine which services the team should offer.

Compare between firefighters #2

Organisations	Firefighters
Selecting a team structure and staffing model	FwDV 1 Grundtaetigkeit Loescheinsatz
Staffing and training the incident response team	FwDV 2 Ausbildung der Freiwilligen Feuerwehr
	FwDV 3 Einheiten im Loesch und TH Einsatz
	FwDV 7 Atemschutz
	FwDV 8 Tauchen
	FwDV 10 Tragbare Leitern
	PDV/DV 810 BOS Sprechfunk
Team Lead qualification?	FwDV 100 Fuehrung und Leitung im Einsatz
	FwDV 500 Einheiten im ABC Einsatz

FwDV 2 Ausbildung der Freiwilligen Feuerwehr

Taetigkeiten	Qualifikationen
Truppausbildung	Truppmannausbildung 1&2
	Truppführer
Technische Ausbildung	Sprechfunker
	Atemschutzgeräteträger
	Maschinisten
	Technische Hilfeleistung
	ABC-Einsatz
Führungsausbildung	Gruppenführer
	Zugführer
	Verbandsführer
Fortbildungen	……

Computer Security Incident Handling Guide

Figure 2-1. Communications with Outside Parties

Incidence response Team Qualifications

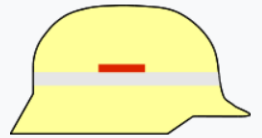
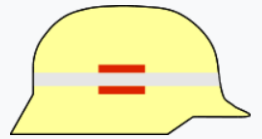
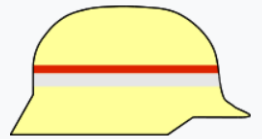
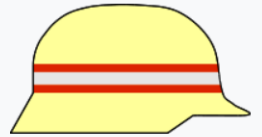
Incidence response Team	Qualifikationen
Team member skills	Network Infrastructure
	Communication infrastructure (Mail, VoIP, Skype,…)
	Database Infrastructure
	Facility
	Datacenter operator / storage specialists
	Cloud
Team Leader qualification	nope

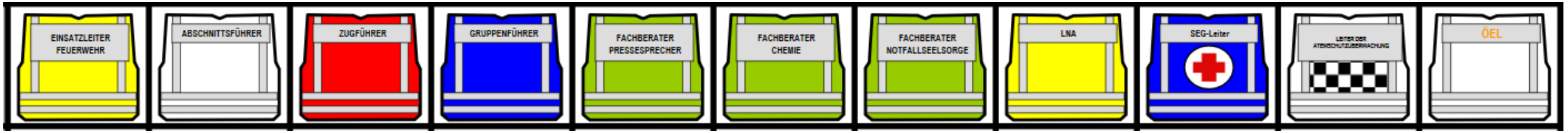
Incidence response Team Identification

How to spot the responsible Person?

Do you know who does what?

In the Firefighter World, even this is standardized.

Kennzeichnung	NI[6]
	• Gruppenführer (Qualifikation)
	• Zugführer (Qualifikation) • Ortsbrandmeister (Funktion)
	• Gemeindebrandmeister (Funktion) • Bereitschaftsführer (Funktion)
	• Abschnittsleiter (Funktion) • Kreisbrandmeister (Funktion) • Regierungsbrandmeister (Funktion)



Incidence response Team Identification

Alarming the IR Teams

How to call the Teams

Vacation?

Qualification

Vendors

Etc.

Alarming the IR Teams

- **Digitalisierung: Neue AAO und Digitale Pager für die FF Lingen**
- Alarm- und Ausrückordnung (AAO)
- Diese neue AAO wurde vom Landkreis Emsland vorgegeben und für die FFL nochmals extra angepasst, da wir viele Sonderfahrzeuge besitzen. Einsatzstichworte

Training and drilling

- How often Trainings and drill occours?
- Comparing against FD

Sample demo:

Cost saving through training?

Training = cost ?

Why training helps to save costs

- Identifying bottlenecks
- Selecting and preparation is done in front of a IR case
- No time wasted to prepare tools for IR case
- …..

Good training and preparation helps to response faster and save costs.

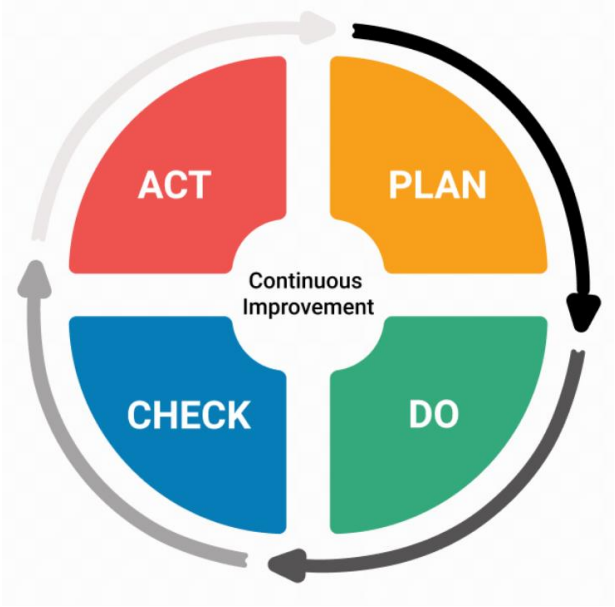
Basic incidence response cycle

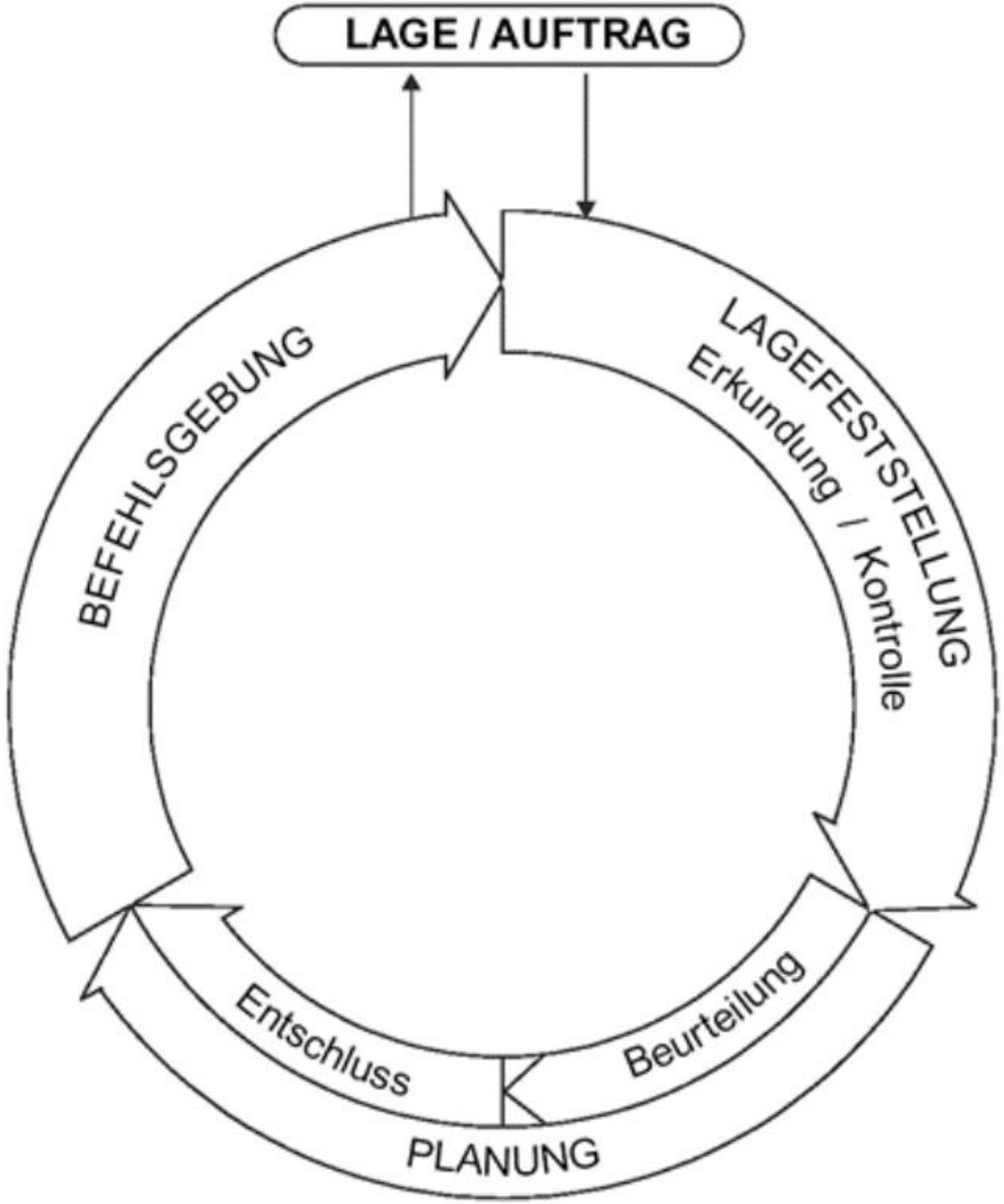
1. Determining if there is an incident
2. Determining how to handle the incident
3. Communicate the incidence
4. Perform the detaild investigation
5. Contain the incidence
6. Eradicate
7. Recovery

Quick Descission making needed

Firefighters needs a scheme for quick Decision making

Like in P.D.C.A. but faster





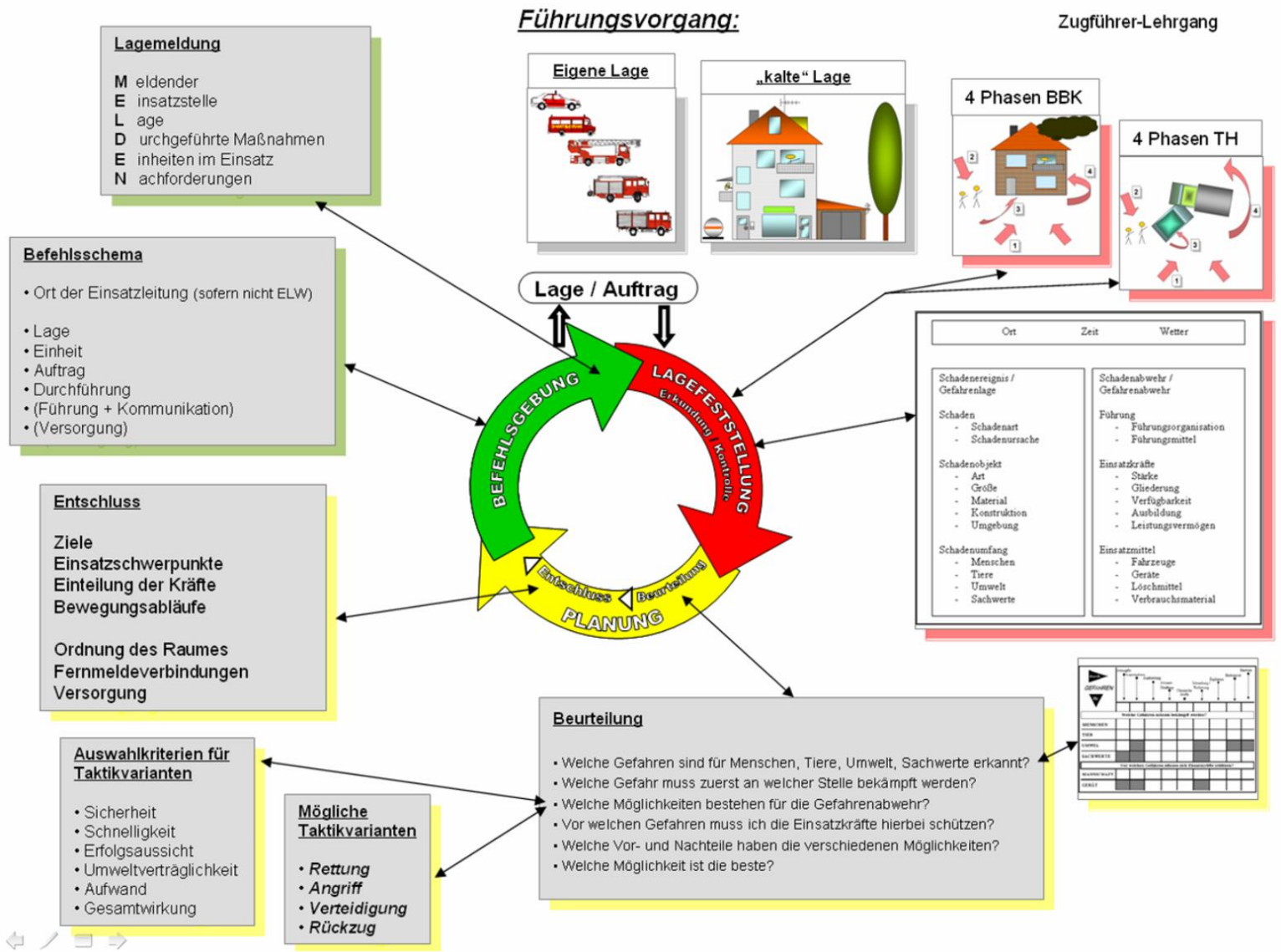
Lagefestellung

Lage/Auftrag

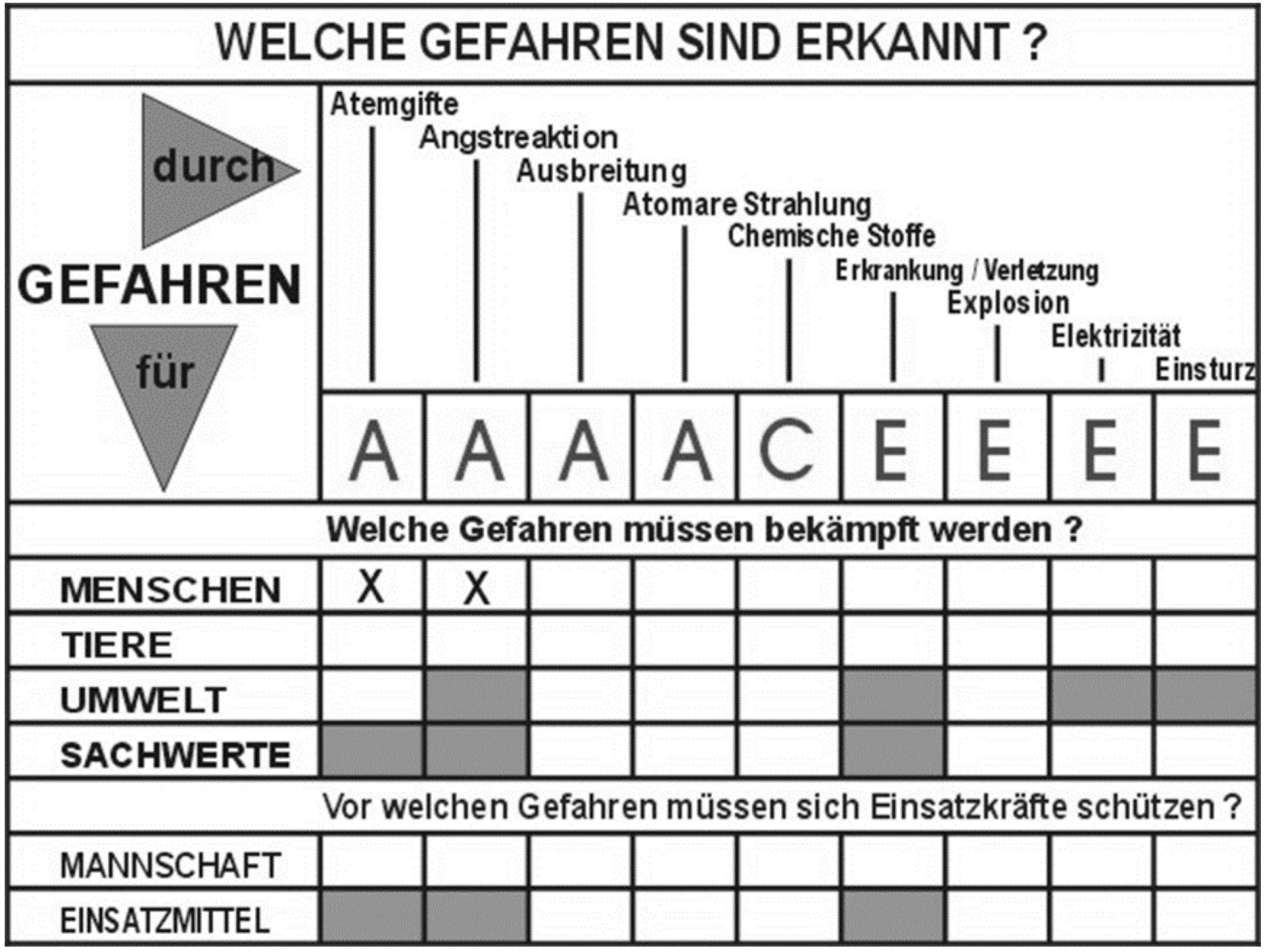
Ort	Zeit	Wetter
Schadenereignis / Gefahrenlage Schaden - Schadenart - Schadenursache Schadenobjekt - Art - Größe - Material - Konstruktion - Umgebung Schadenumfang - Menschen - Tiere - Umwelt - Sachwerte		Schadenabwehr / Gefahrenabwehr Führung - Führungsorganisation - Führungsmittel Einsatzkräfte - Stärke - Gliederung - Verfügbarkeit - Ausbildung - Leistungsvermögen Einsatzmittel - Fahrzeuge - Geräte - Löschmittel - Verbrauchsmaterial

Planung

Quick Decision making needed



Quick Decision making needed



Quick Decision making needed

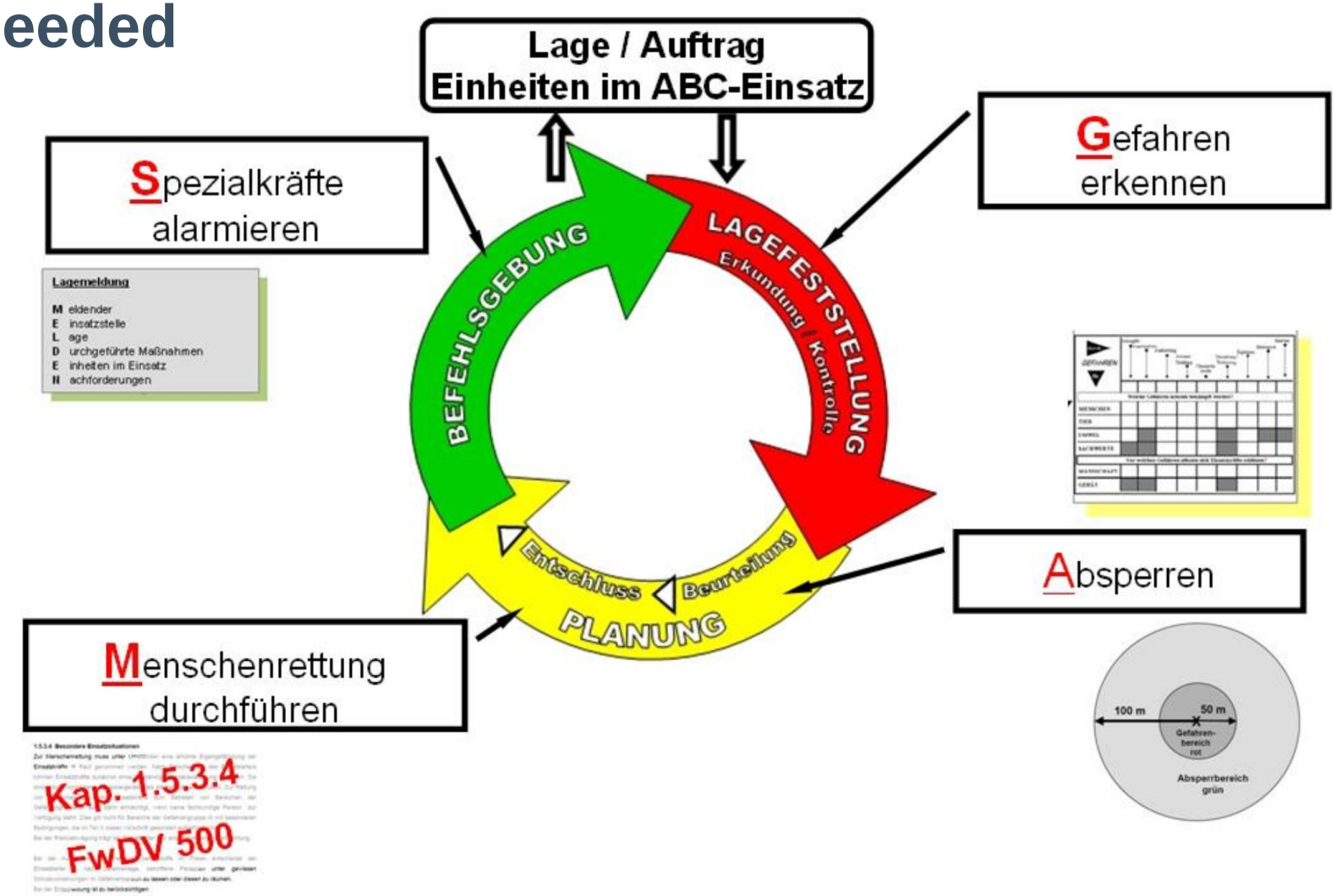


Abbildung 4: Besonderheiten des Führungsvorgangs im ABC-Einsatz

P.D.C.A. in incidence response

P. Plan

planning of scenarios and possible solutions

D. Do

C. Check

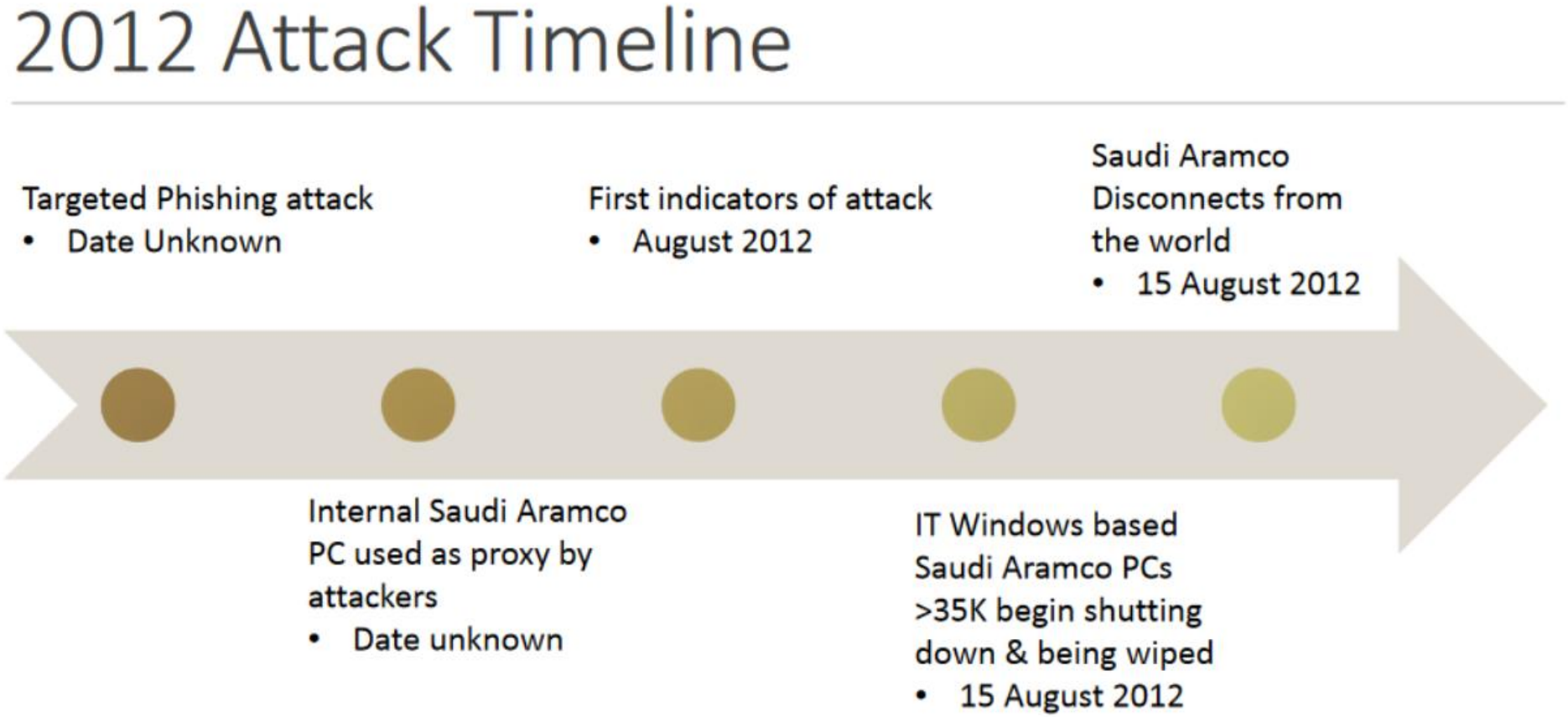
A. Act

Real Life scenarios – are u prepared?

Are u prepared for the following?

- Nearly all PC infected with a wiper malware?
- Fire in nuclear facility in the neighborhood?
- Mysterious virus infection of employees?

Real Life scenarios – are u prepared?



https://en.wikipedia.org/wiki/Shamoon#/media/File:Shamoon_1_attack_timeline.png

Real Life scenarios – are u prepared?

Are u prepared for the following?

nCov2019 infection of employees at Automotive supplier

- 27. Jan. first infection
- 28. Jan. Management: no business trips to China for 2 weeks, employees could decide to work in home office
- 29. Jan. 3 new infections, Management closes Office up to Sunday (2.2.)
- 31. Jan. 6 infected employees
- 2. Feb. 8 infected employees
- 3. Feb. Closing facility up to 11. Feb.
- 4. Feb. 10 infected employees

Real life – expect the unexpected

When you think, you have seen everything….

- https://youtu.be/gbr6NIHp348

Real life – expect the unexpected

29.01.2020 | 11:40 Uhr

Vorlesen

Penisring sitzt fest: Mediziner holen in Dresden Feuerwehr zu Hilfe

Immer gut kühlen: Feuerwehr für heikle Missionen trainiert

Die Retter haben den Angaben zufolge dann mit einem Multifunktionswerkzeug den rund zehn Zentimeter großen Edelstahlring unter ständiger Kühlung in zwei Teile zerlegt. Der Patient kam nicht zu Schaden. Glück für den 46-Jährigen: Die Feuerwehr hatte nach eigenen Angaben im Jahr 2018 "im Rahmen der jährlichen Fortbildung ein solches Szenario trainiert, um den Umgang mit diesem Spezialwerkzeug und die damit verbundene Feinfühligkeit sowie das filigrane Arbeiten sicher zu beherrschen".

Quelle: MDR/lam/dpa

seinem Penisring zu befreien. Wie die Feuerwehr mitteilte, war der 46-jährige Pechvogel

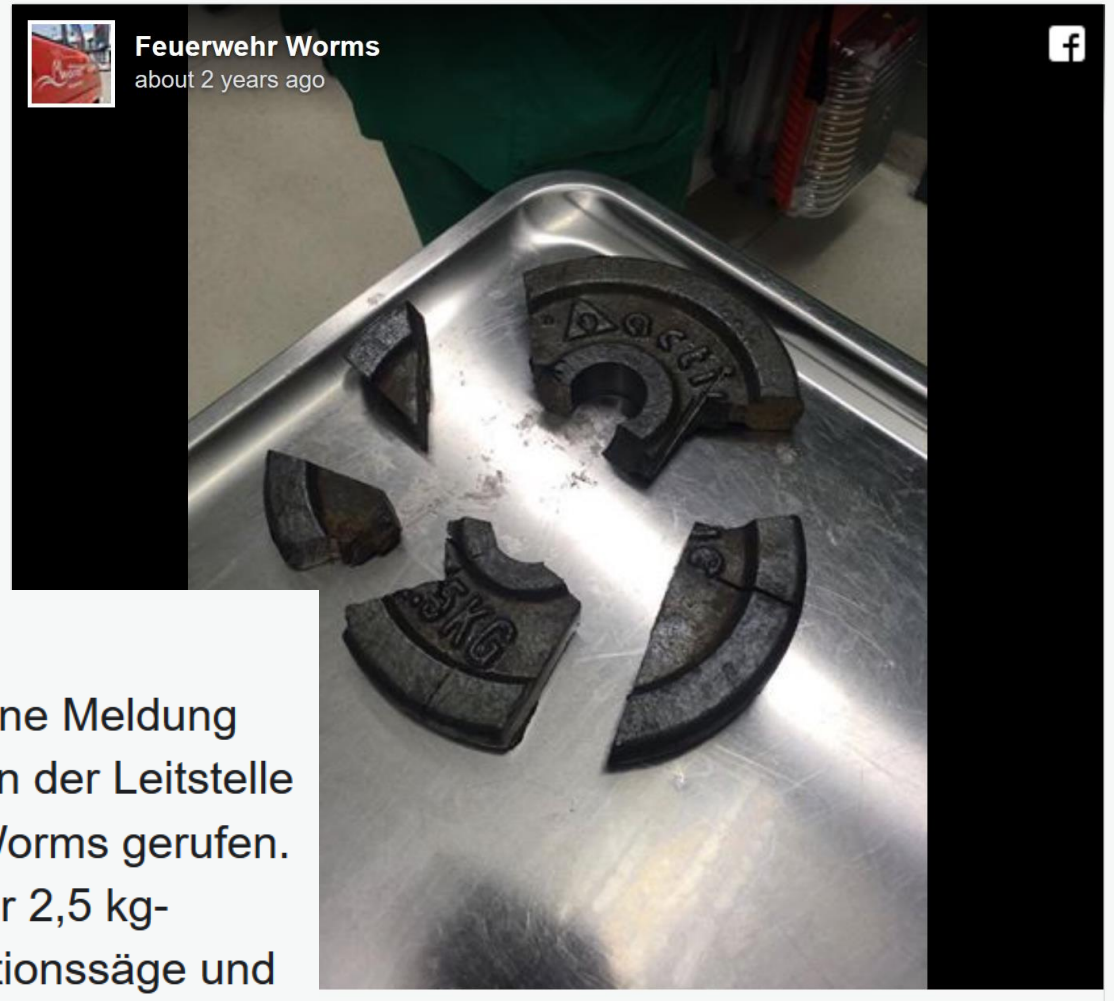
Real life – expect the unexpected

Wie uebt mann solche Scenarien?

https://www.youtube.com/watch?v=m_HZm6ZfKN8

Real life – expect the unexpected

When you think, you have seen everything…



Einsatzbericht: Kurioser Trainingsunfall - Hilfeleistung fürs Klinikum

Wie heikel so mancher Einsatz unserer Feuerwehr sein kann, zeigt eine Meldung der etwas anderen Art, die am heutigen Freitagmorgen, 15.09.2017, in der Leitstelle einging. Die Berufsfeuerwehr wurde zur Unterstützung ins Klinikum Worms gerufen. Eine Person hatte sich ein sehr sensibles Körperteil in dem Loch einer 2,5 kg-Hantelscheibe eingeklemmt. Mit Hilfe vom Trennschleifer, einer Vibrationssäge und einem hydraulischem Rettungsgerät konnte das Hantelgewicht nach drei Stunden entfernt werden.
Im Einsatz waren die Berufsfeuerwehr und ein Feuerwehrmann der freiwilligen Einheit Stadtmitte.

Bitte solche Aktionen nicht nachmachen!

Lessons learned

Planning and Training on regular Basis.
More than once a year

Not focusing only on IT incidence.
Plan for Business continuity. IT is automatically Part of BCM

Standardize education and minimum Trainings for the Team
Do not forget training for Incident Team Leader

Links to external material

NIST SP 800 – 61r2 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

Dutch firefighters – accident https://www.youtube.com/watch?v=mKZjNr095F0

ISO 27035 https://www.iso.org/obp/ui/fr/#iso:std:iso-iec:27035:-2:ed-1:v1:en

May the force be with u

Twitter: @ObiWan666

SGerling@ROSEN-Group.com

https://www.github.com/obiwan666/IT-Defense

THANK YOU FOR JOINING THIS PRESENTATION.

www.certivation.com

CERTivation