IT-SA 2023

Notfallmanagement

Cyberkrisen minimieren durch richtige Vorbereitung

kaspersky

Stephan Gerling

Senior Security Researcher im
ICS CERT


WDR
FEUER- UND RETTUNGSWACHE 2
BOCHUM-INNENSTADT
FEUER & FLAMME

Notfallmanagement

Cyberkrisen minimieren durch richtige Vorbereitung

Stephan Gerling
Senior Security Researcher
Kaspersky ICS-CERT
Stephan.Gerling@Kaspersky.com

@ObiWan666

Agenda

- Einleitung
- Incidence response – Definition und Standards
- Gemeinsamkeiten Rettungskräfte und Organisationen
- Training und Ausbildung
- Fragen und Antworten

Was passiert bei einem Notruf 110 / 112

- Die 5 “W” Fragen
- Leitstelle Alarmiert Rettungsmittel gemäß Stichwort nach der Alarm und Ausrückordnung (AAO)
- Einsatzkräfte rücken aus
- Notfall wird abgearbeitet

Anruf beim Helpdesk

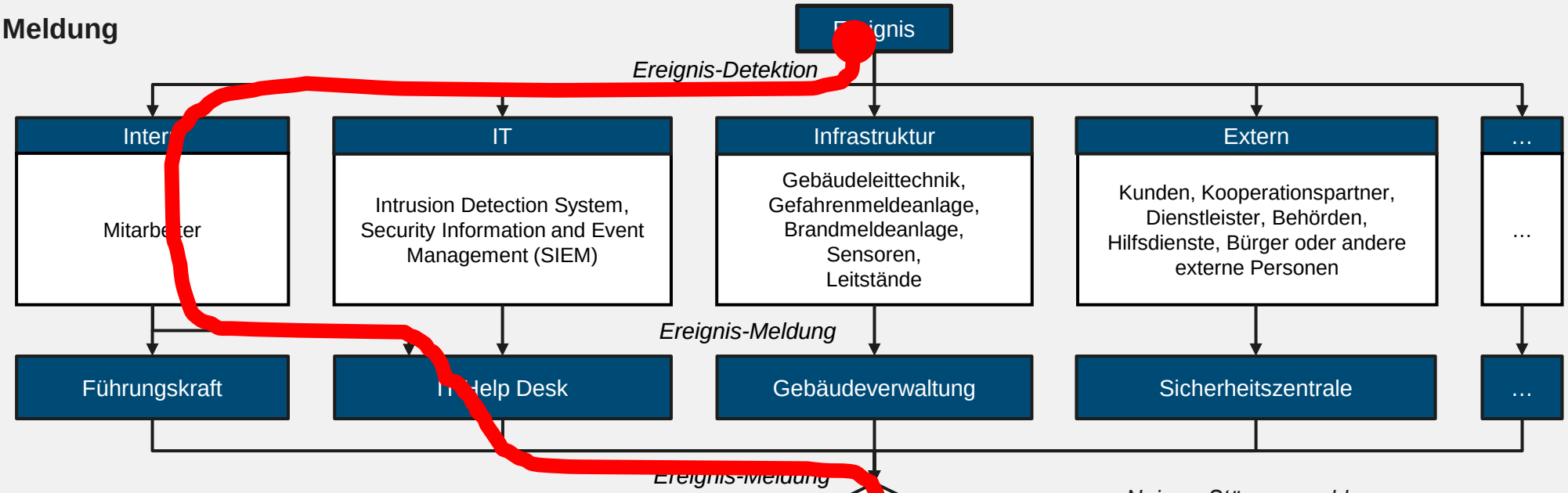
- IT/OT Personal wird zur Störung gerufen

Zeitraum zur Erkennung ob Störung oder größeres Ausmaß hängt maßgeblich vom Personal ab

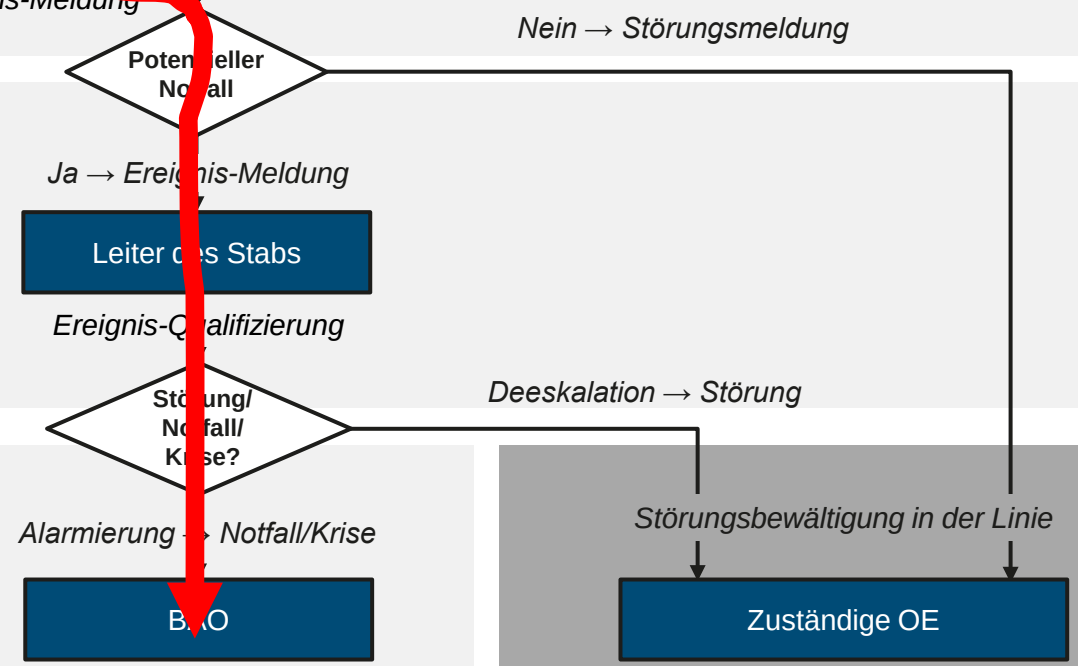
Notfallpläne für verschiedene Notfälle sparen Zeit in der Bewältigung

BSI-Standard 200-4 | Beispiel eines Alarmierungs- und Eskalationspfads

Schritt 1: Detektion und Meldung



Schritt 2: Einstufung der Ereignismeldung und Entscheidung



Zentrale Entscheidungsinstanz:

Schritt 3: Alarmierung der BAO

Notfallmamagement – Definition & Standards

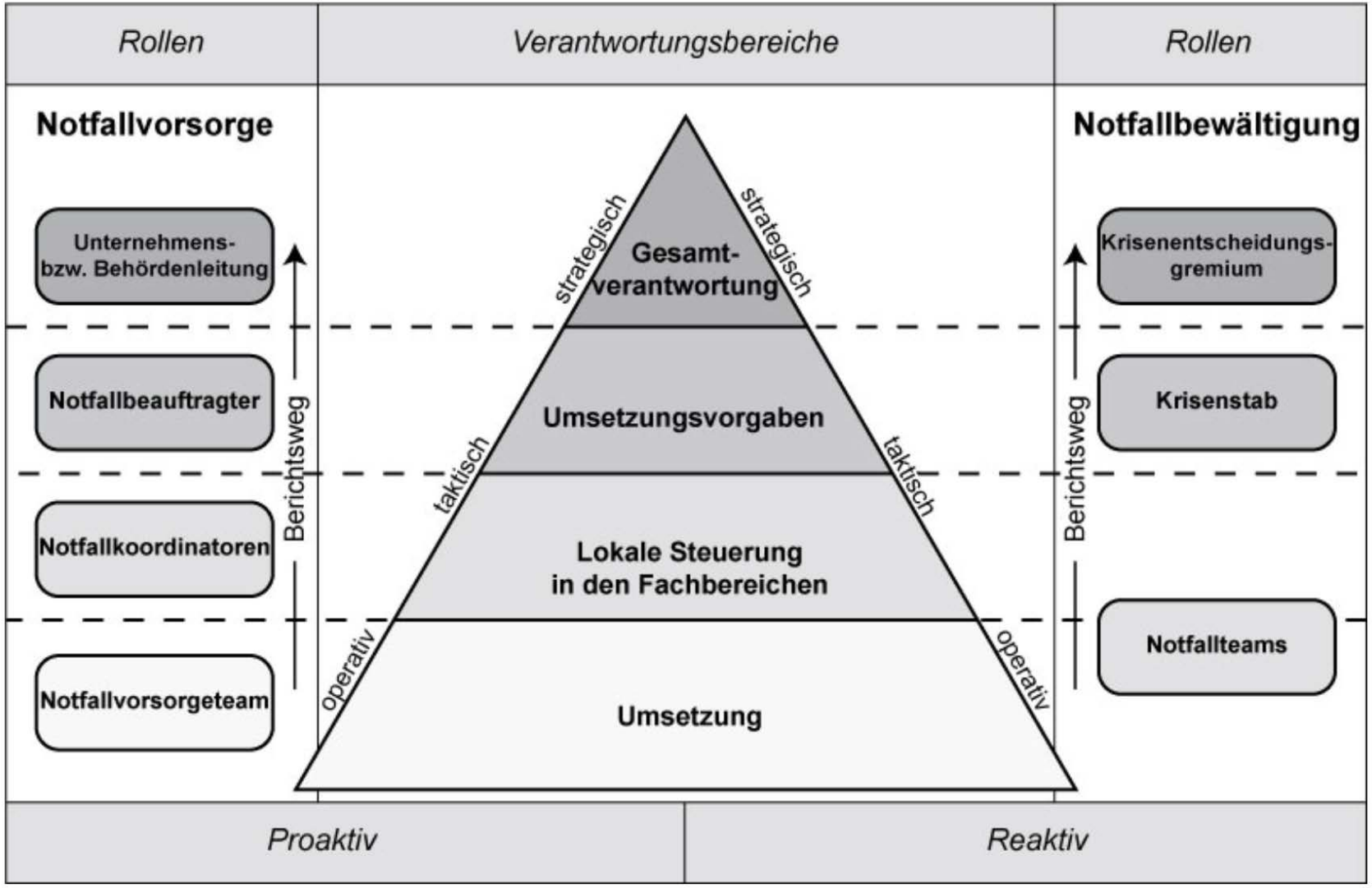
~~BSI-Standard 100-4~~	~~„Notfallmanagement“~~	
BSI-Standard 200-4	„Business Continuity Management“	(BCM)
ISO IEC 27035 – Teil 1-3	„Security Incidence response Management”	
NIST SP 800-61 r2	„Computer Security Incident Handling Guide”	
~~BS 25999-1 / BS 25999-2~~	~~„Business Continuity Management – Part1: Code of Practice“~~	

Das “letzte Glied der Kette”

- Von “ist nicht so schlimm” bis “Katastrophe
- Kann mit einer phishing E-Mail starten und in der Insolvenz enden
- Wichtiger Teil des “Business continuity” , “disaster recovery” usw.

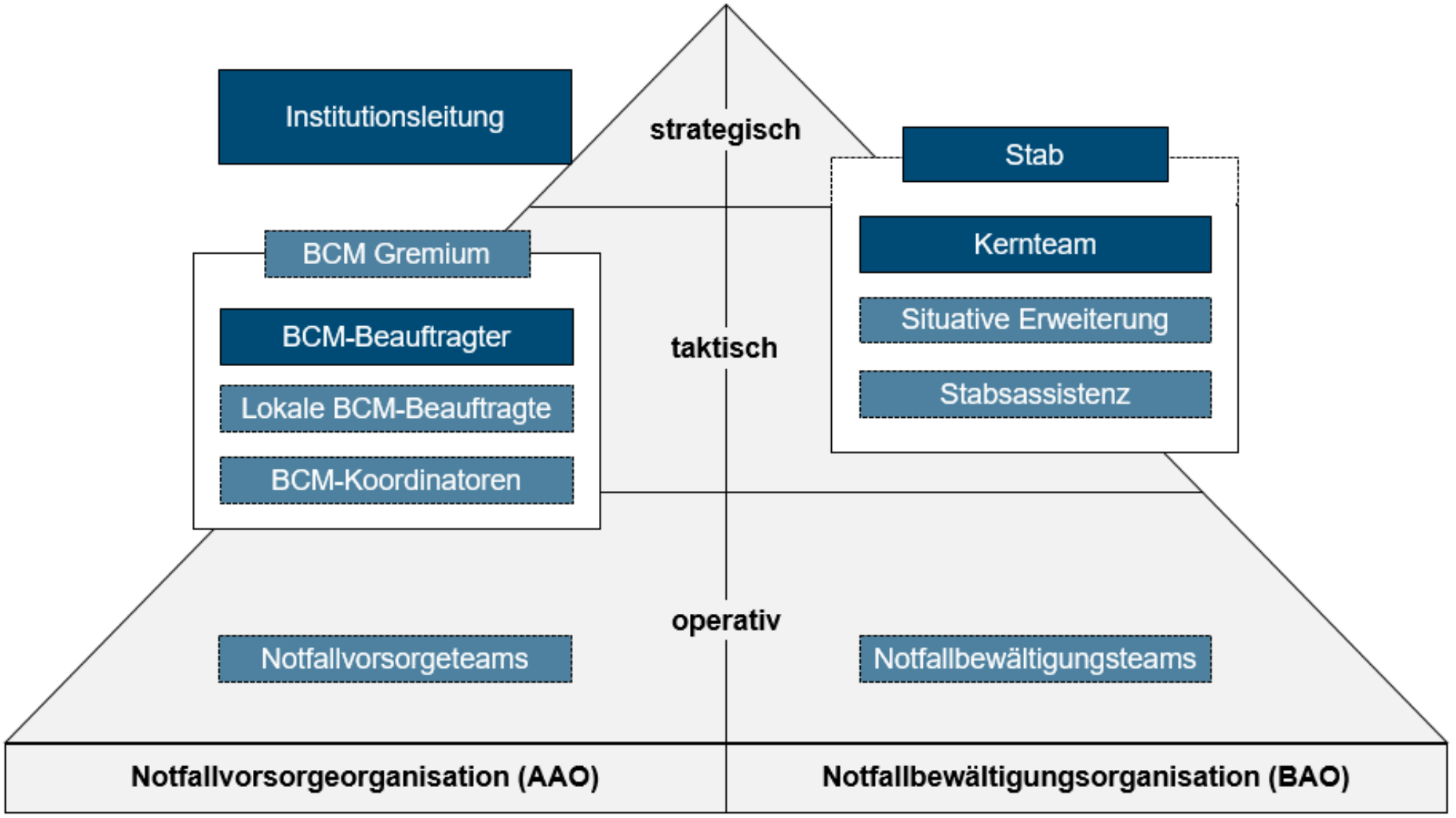
Leider zu oft nur ein lästiger Punkt auf der ToDo Liste

BSI Standard 100-4 Notfallmanagement



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

BSI-Standard 200-4 | Beispiel einer BCM-Organisation (editierbar)



Oft wird in Unternehmen eine Führungsperson als Notfall Manager bestimmt

Empfohlen:

- Nach Eignung und nicht nach Hierarchie

Im Rettungswesen erfolgt dies nach klaren Hierarchien

- Für jede Funktion ist ein entsprechender Ausbildungsstand nötig
- Krisenstab Funktion = min. 3 Monate Vollzeit Ausbildung
- Als Einsatzleiter mindestens Gruppenführer Qualifikation

3.1.2 Leitung (FwDV100)

„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.

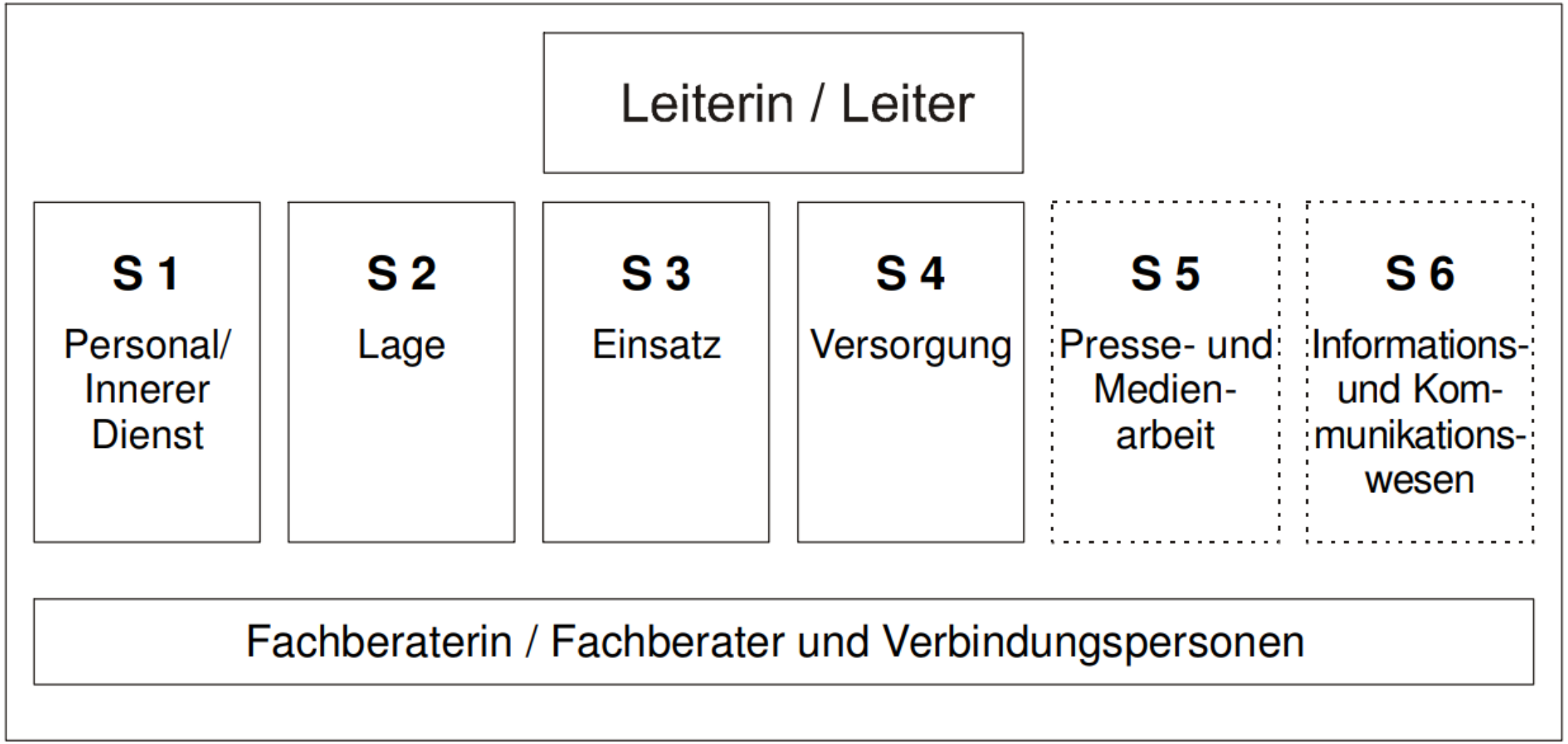
Wer die Einsatzleitung hat, bzw. diese übernehmen kann, ergibt sich aus den gesetzlichen Regelungen.

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“

Krisenstab bei der Feuerwehr



Wird aus:

- Krisenstabsleiter
- 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

Presse und Medienarbeit (S5)

Training und Übungen

Feuerwehr

- Wöchentliche Übungen
- gemäß Feuerwehrdienstvorschrift
- Sonderdienste und Übungen

Unternehmen:

- BSI 100-4 “regelmäßige Tests und Übungen”
- Gemäß des Notfallplans

Feuerwehr

- Wöchentliche Übungen
- gemäß Feuerwehrdienstvorschrift
- Sonderdienste
- Übungen
- Brandsicherheitswachen

Unternehmen:

- “regelmäßige Tests und Übungen”
- Gemäß des Notfallplans

Training = Kosten ?

Warum Training dennoch Kosten sparen kann:

- Flaschenhälse werden Identifiziert
- Geschäftsprozesse werden im Notfalltraining auf Funktionalität geprüft
- Teamauswahl und Material ist im Vorfeld bestimmt
- Kein Zeitverlust durch Vorbereiten im Fall X
- Entscheidungsbefugnisse sind klar definiert
- Usw.

„Eine gute Vorbereitung spart im Fall der Fälle Zeit und Geld !“

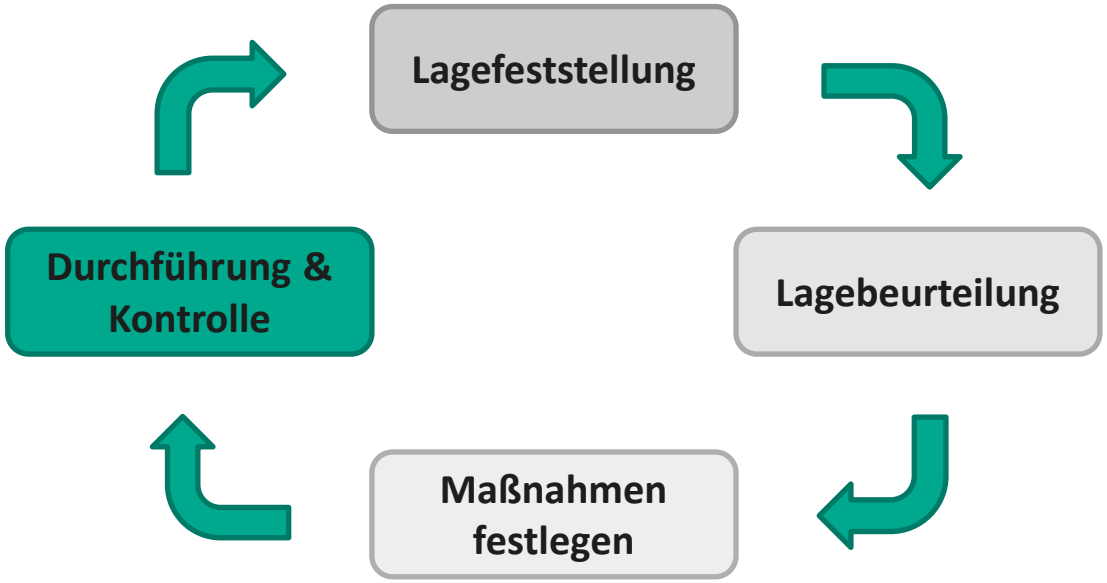
Notfallplanung

Notfallplanung beinhaltet all diese Punkte:

- Benachrichtigung / Verständigung
- Äußere Erkennungsmerkmale?
- Qualifikationen
- Ausbildung
- Urlaubsvertretung
- Eskalation
- Externe Kräfte
- Budget / Kostenregelung
- Etc.

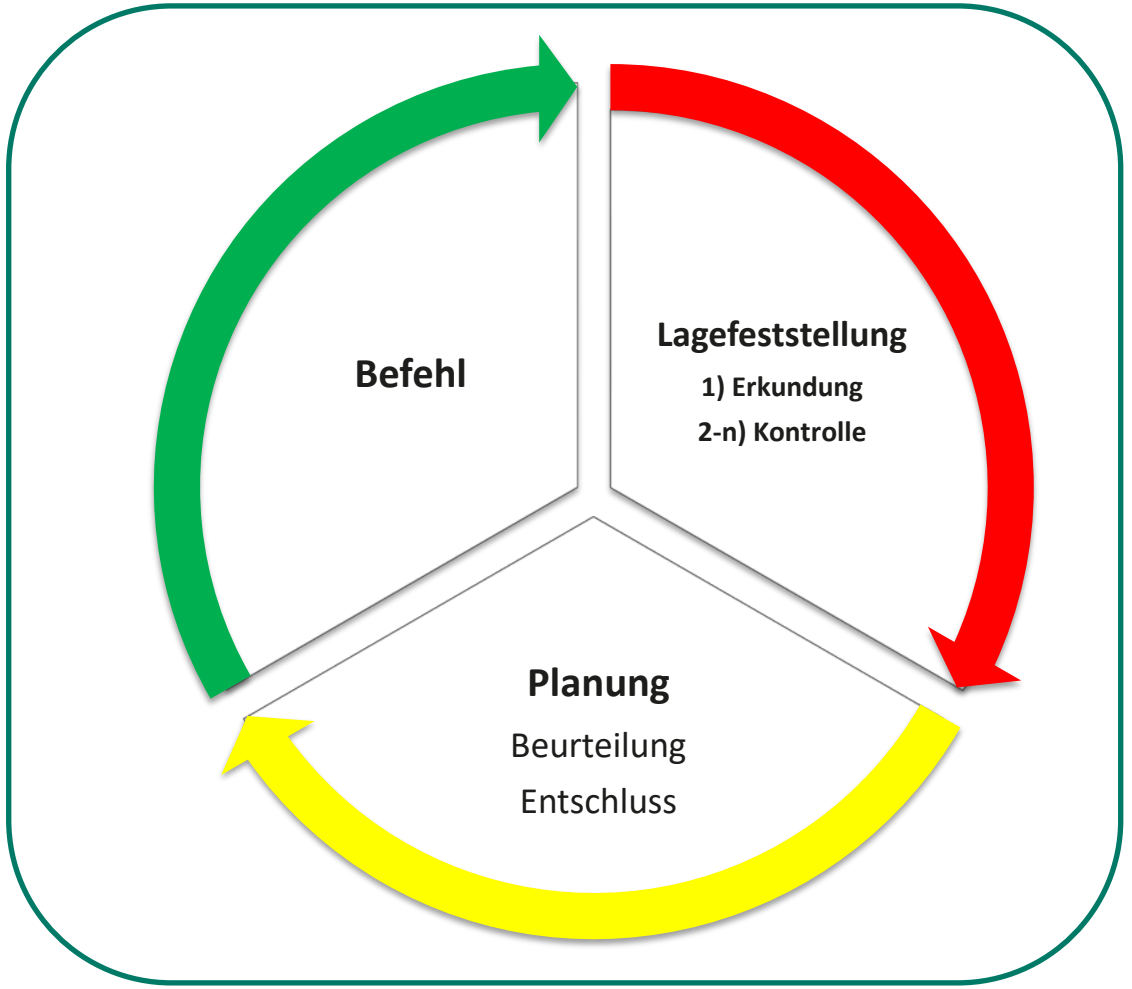
Entscheidungsfindung

Führungsvorgang



BSI 100-4

vs.



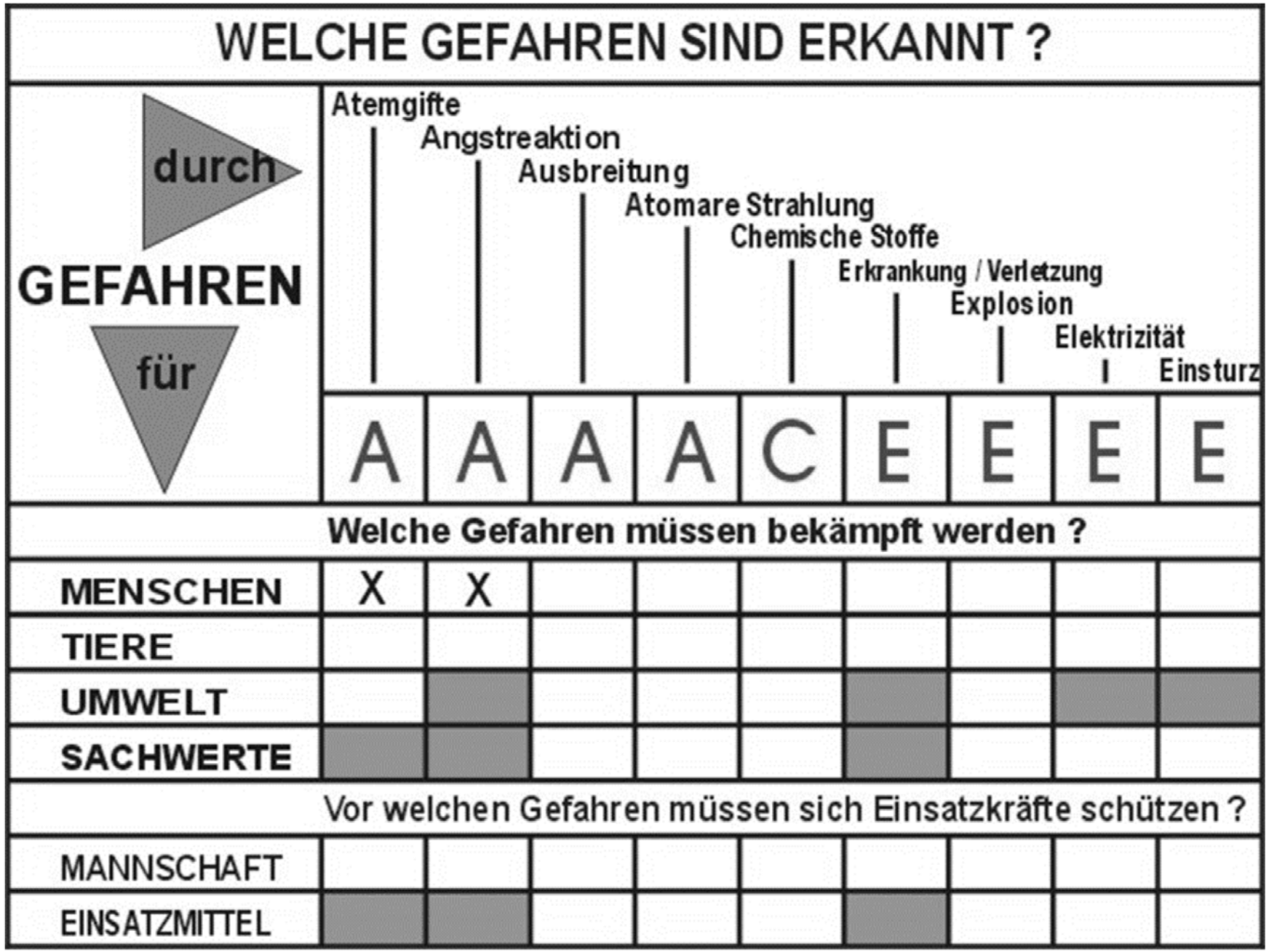
Feuerwehr

Lagefestellung

Lage/Auftrag

Planung

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	


WELCHE GEFAHREN SIND ERKANNT ?
durch
GEFAHREN
für
Atemgifte
Angstreaktion
Ausbreitung
Atomare Strahlung
Chemische Stoffe
Erkrankung / Verletzung
Explosion
Elektrizität
Einsturz
A A A A C E E E E
Welche Gefahren müssen bekämpft werden ?
MENSCHEN X X
TIERE
UMWELT
SACHWERTE
Vor welchen Gefahren müssen sich Einsatzkräfte schützen ?
MANNSCHAFT
EINSATZMITTEL

Erfolgreiches Notfallmanagement hängt maßgeblich ab von:

- Planung und Regelmäßiges Üben
- Standardisierte Vorgehensweise und Trainings
- Focus auf den Notfallmanager
- Nicht nur an IT Notfälle denken (IT ist automatisch Teil des BCM)
- Prozess übergreifenden Abhängigkeiten erkennen

Links to external material

BSI 100-4 Notfallmanagement
https://www.bsi.bund.de/dok/6782544

BSI 200-4 Business Continuity Management
https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/BSI-Standard-200-4-Business-Continuity-Management/bsi-standard-200-4_Business_Continuity_Management_node.html

BSI 200-4 Hilfsmittel
https://www.bsi.bund.de/dok/12857498

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

ISO 27035 Teil 1 bis 3
https://www.iso.org/obp/ui/fr/#iso:std:iso-iec:27035:-2:ed-1:v1:en

Vielen Dank!

Stephan Gerling

Senior Security Researcher
Kaspersky ICS-CERT
Stephan.Gerling@Kaspersky.com

@obiwan666

kaspersky