

Security Incident Response

Was wir von der Feuerwehr lernen können

FEUER- UND RETTUNGSWACHE 2

BOCHUM-INNENSTADT

FEUER & FLAMME

Übersicht

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

Alarmierung der Feuerwehr

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

IT-Notfall im Unternehmen

Anruf beim Helpdesk

- ▶ IT/OT Personal wird zur Störung gerufen

Zeitraum zur Erkennung ob Störung oder größeres Ausmaß hängt maßgeblich vom

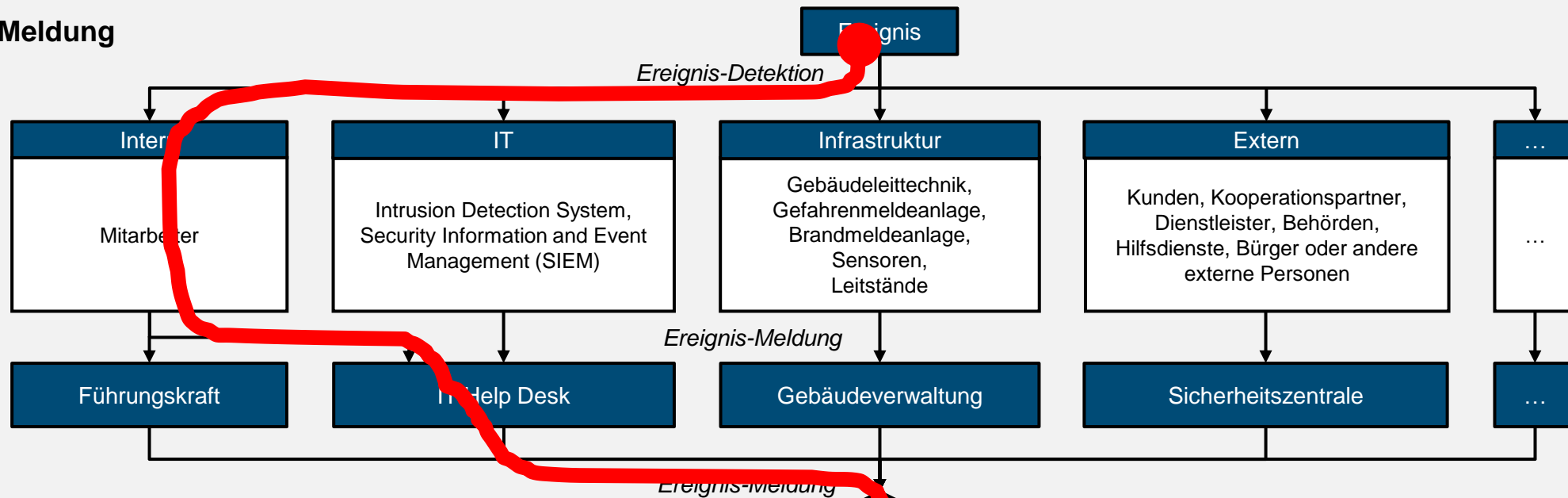
Personal ab

Notfallpläne für verschiedene Notfälle sparen Zeit in der Bewältigung

Schritt 1: Detektion und Meldung

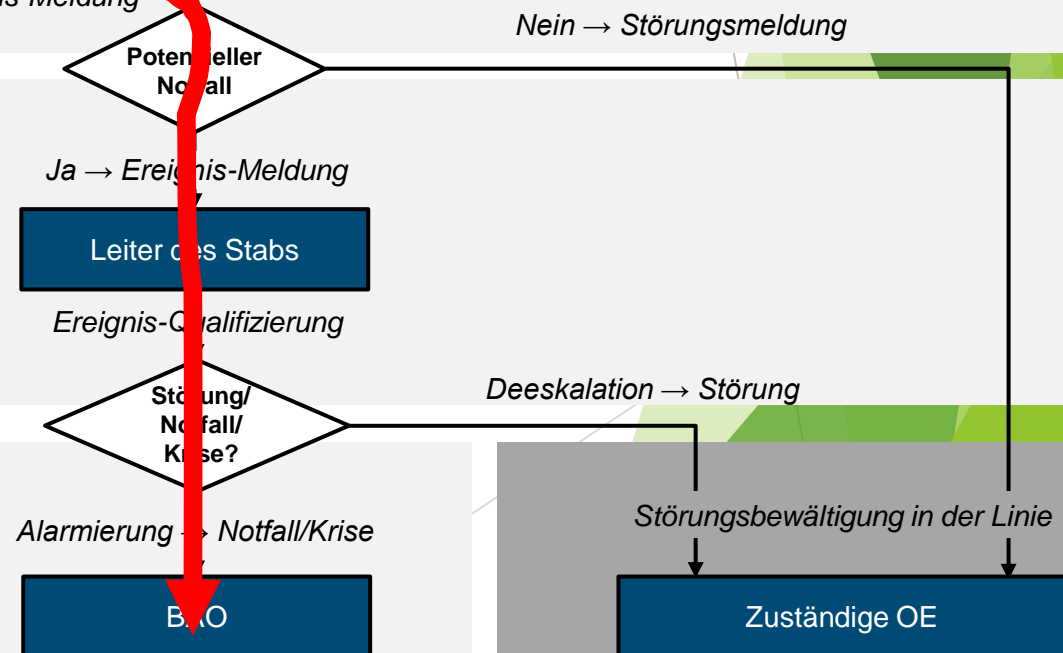
Meldequellen:

Meldestellen:



Schritt 2: Einstufung der Ereignismeldung und Entscheidung

Zentrale Entscheidungsinstanz:



Schritt 3: Alarmierung der BAO

Incident response - 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“

Incident response - Definition & Standards

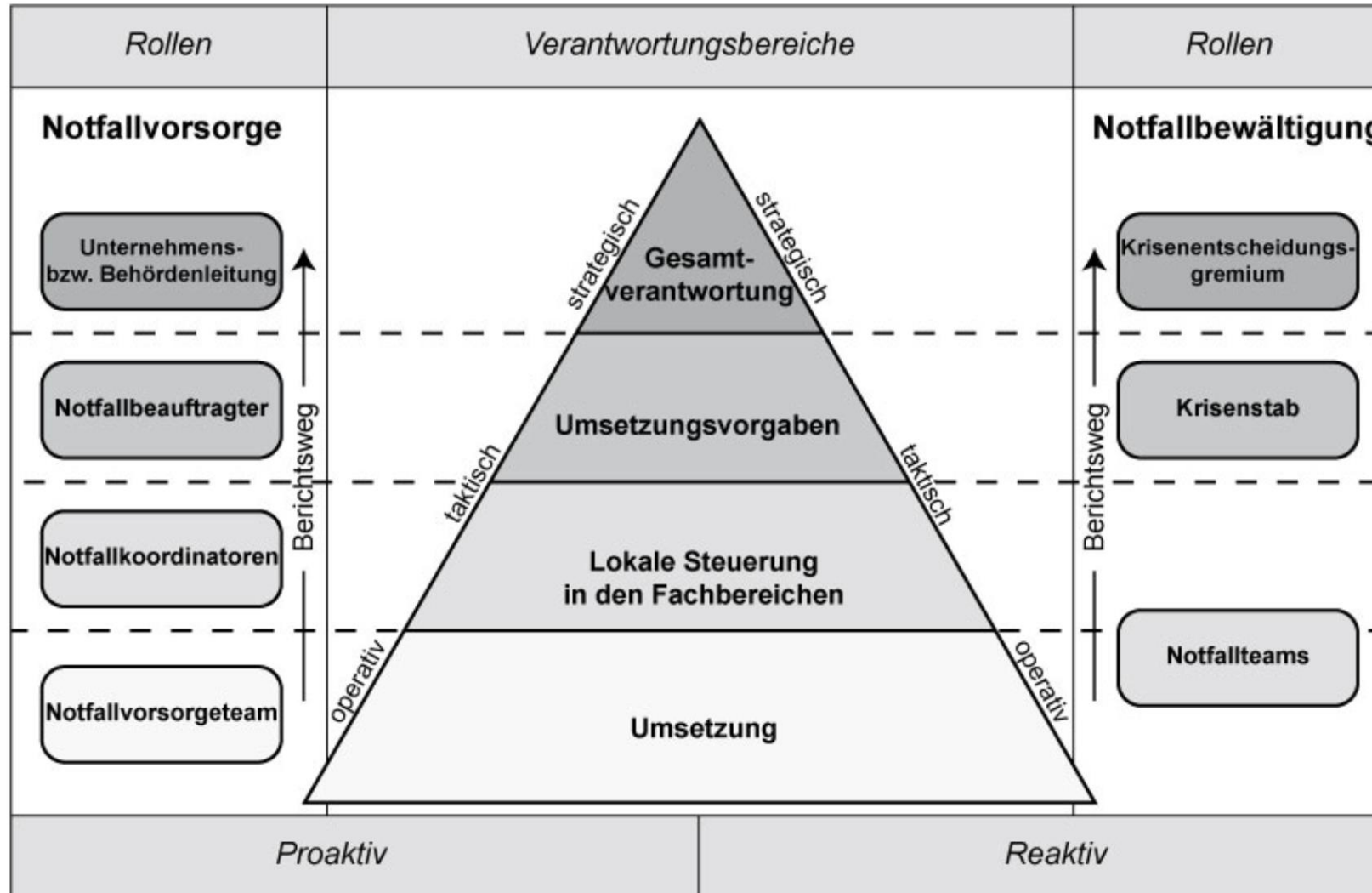
Incident response - Die Reaktion auf Vorfälle

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



Notfall Manager vs. Einsatzleiter

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

Zuständigkeiten 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.

Zuständigkeiten

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 in Unternehmen

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

Leiterin / Leiter

S 1

Personal/
Innerer
Dienst

S 2

Lage

S 3

Einsatz

S 4

Versorgung

S 5

Presse- und
Medien-
arbeit

S 6

Informations-
und Kom-
munikations-
wesen

Fachberaterin / Fachberater und Verbindungspersonen

Presse und Medienarbeit (S5)

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

Ein Beispiel wie es nicht gemacht wird

- <https://www.youtube.com/watch?v=RtOxYOBqUkM>

Training und Übungen

Feuerwehr

- ▶ Wöchentliche Übungen
- ▶ gemäß Feuerwehrdienstvorschrift
- ▶ Sonderdienste und Übungen

Unternehmen:

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

Wie kann Üben Kosten sparen?

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.

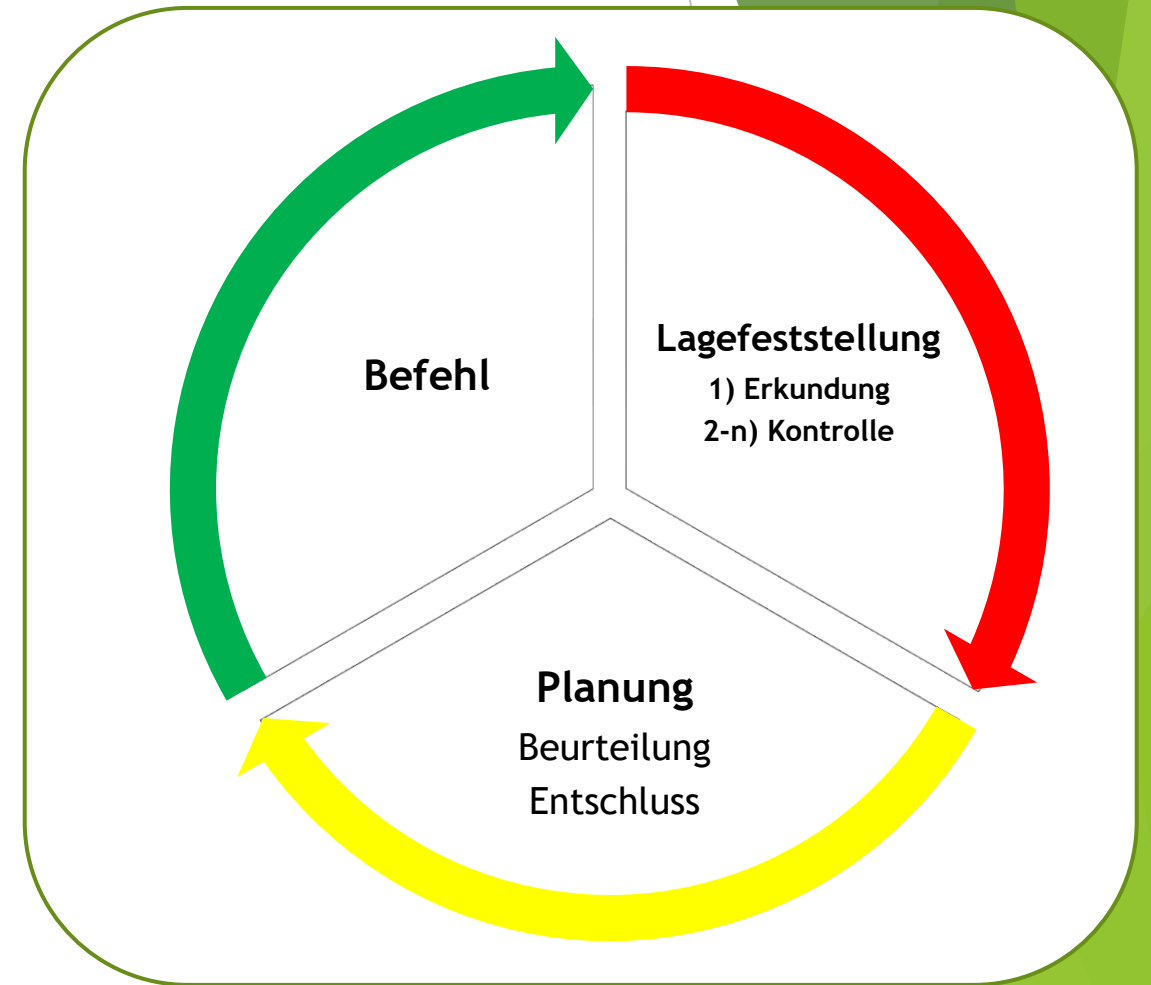
Entscheidungsfindung

Bewältigungsprozess vs. Führungsvorgang



BSI 100-4

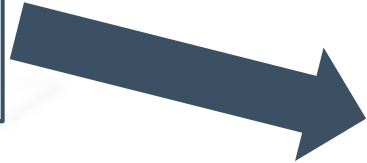
vs.



Feuerwehr

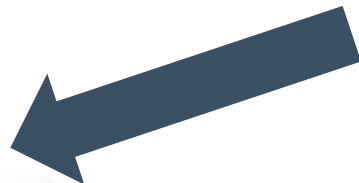
Lagefeststellung

Lage/Auftrag




Ort	Zeit	Wetter
Schadenereignis / Gefahrenlage Schaden <ul style="list-style-type: none">- Schadenart- Schadenursache	Schadenabwehr / Gefahrenabwehr Führung <ul style="list-style-type: none">- Führungsorganisation- Führungsmittel	
Schadenobjekt <ul style="list-style-type: none">- Art- Größe- Material- Konstruktion- Umgebung	Einsatzkräfte <ul style="list-style-type: none">- Stärke- Gliederung- Verfügbarkeit- Ausbildung- Leistungsvermögen	
Schadenumfang <ul style="list-style-type: none">- Menschen- Tiere- Umwelt- Sachwerte	Einsatzmittel <ul style="list-style-type: none">- Fahrzeuge- Geräte- Löschmittel- Verbrauchsmaterial	

Planung



Hilfsmittel

WELCHE GEFAHREN SIND ERKANNT ?									
 GEFAHREN	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									

[illegible]

Sind Sie vorbereitet?

Echte Beispiele:

- ▶ 30.000 Clients und 2.500 Server mit Lösch-Schadsoftware (wiper) befallen?
- ▶ Brand in einer Nuklearen Fertigungsstätte?
- ▶ Brand im Rechenzentrum eines Hosting Anbieters, inkl. des Backup?
- ▶ Mysteriös Virus Infektionen bei Mitarbeitern nach Dienstreise?

Schlüssel zum Erfolg

Planung und Regelmäßiges Üben

Standardisierte Vorgehensweise und Trainings

Focus auf den Notfallmanager

Business Continuity Management (BCM) ist wichtig

Nicht nur an IT Notfälle denken (IT ist automatisch Teil des BCM)

Links to external material

BSI 100-4 Notfallmanagement

<https://www.bsi.bund.de/dok/6782544>

BSI 100-4 Notfallmanagement

<https://www.bsi.bund.de/dok/6782544>

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>

May the force be with u

Twitter: @ObiWan666

Stephan.Gerling@web.de

<https://www.github.com/obiwan666/Vorträge>