Enterprise Risk Management

Crisis Management in the Digital Age

Ing. Rainer Eisenkirchner

ERM-Consult

ERM-Consult

Enterprise Risk Management

- Gegründet 2011 ....
  - .... Teil eines Beraternetzwerks
  - .... Support für über 60 Kunden
  - .... in 13 verschiedenen Ländern

Ing. Rainer Eisenkirchner, CISA, CISSP, CRISC, CBCI

Agenda

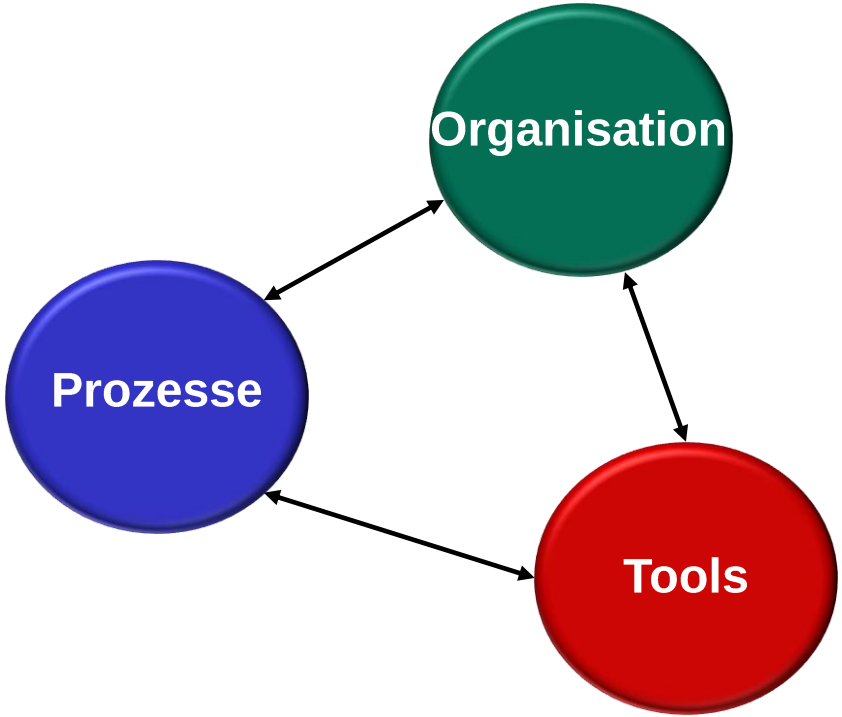
Enterprise Risk Management

ERM Consult

- Krisenmanagement allgemein
- Neue Szenarien
- Auswirkungen
- Maßnahmen

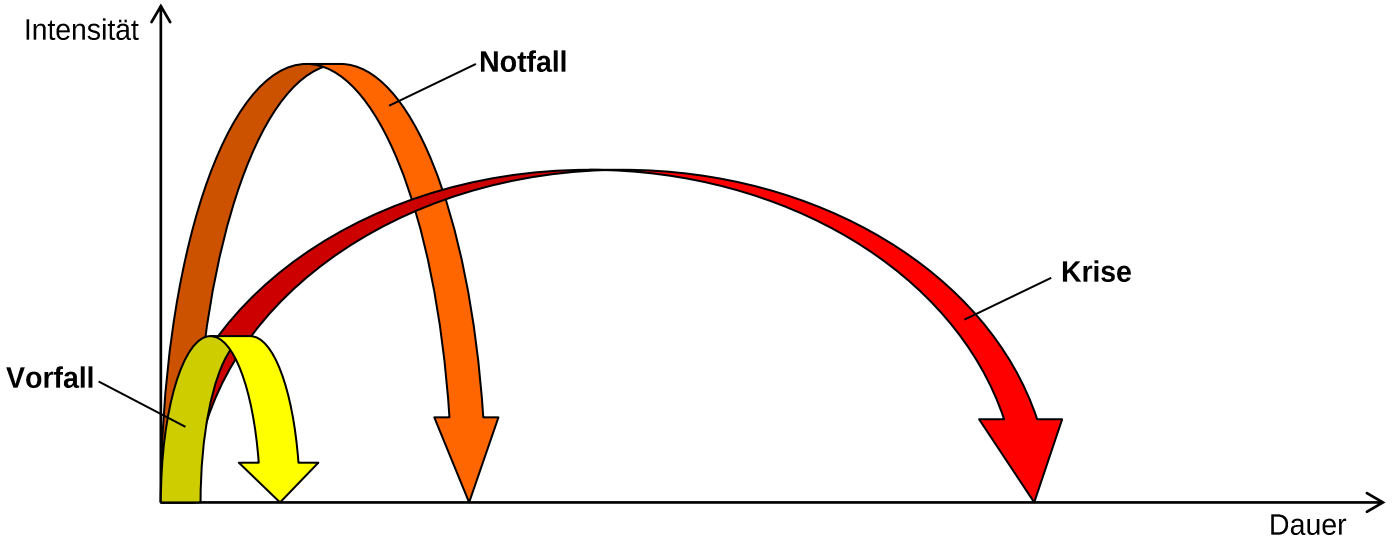
Was ist Krisenmanagement?

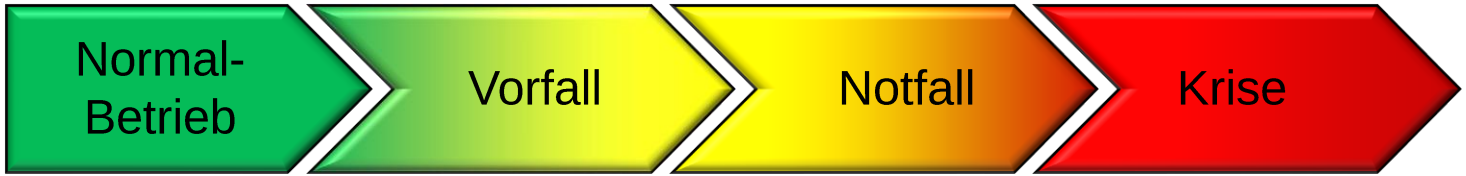
Enterprise Risk Management



Prozesse

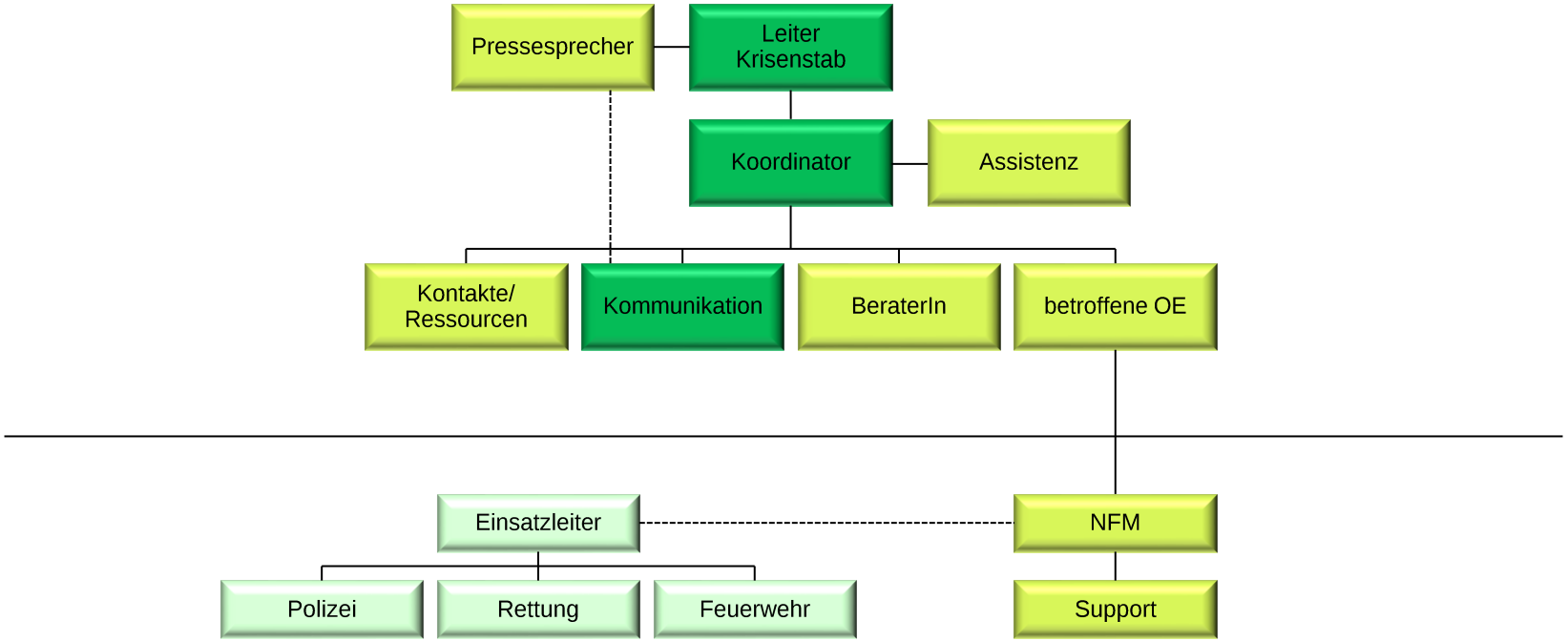
Enterprise Risk Management





Organisation

Enterprise Risk Management



Tools

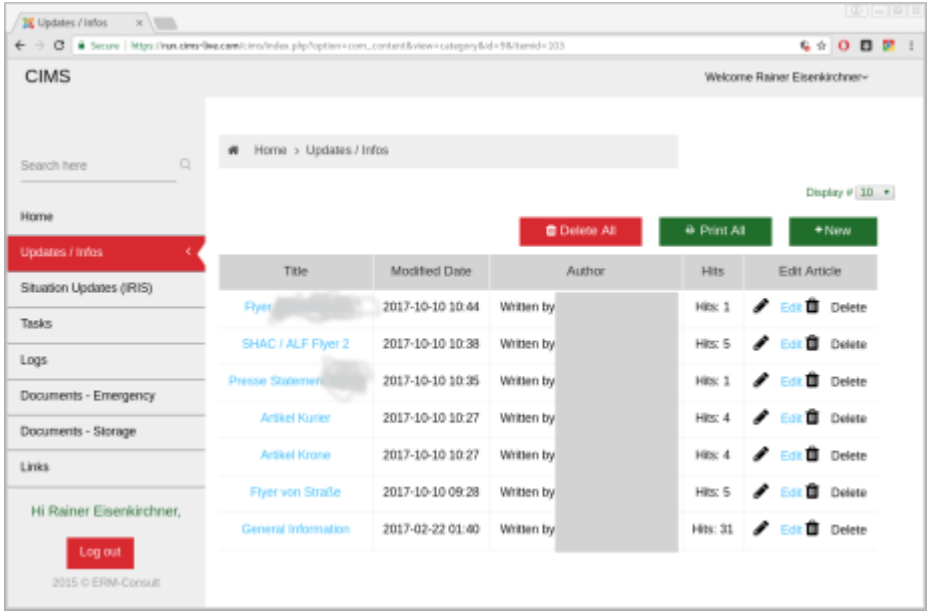
Enterprise Risk Management

Im Krisenstab

- Lagebild / Visualisierungssysteme
- Taskliste
- Logbuch

Im Notfallmanagement

- Notfallpläne
- Aktive Detektions- und Verteidigungs-Systeme
  - SIEM, IDS/IPS, SOC, ….



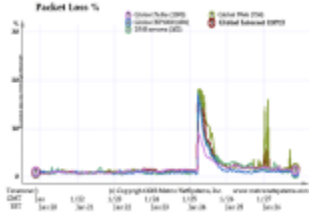
Neue Szenarien … in the Digital Age

Enterprise Risk Management

ERM Consult

Neue Angriffs-Vektoren

- Fast-Infector-Viruses
  - ILOVEYOU (2000), SQL-Slammer (2003), …
  - Cryptolocker (2013), WannaCry (2017), Petya (2017), …
- (D)DOS
  - WinNuke (1997), Mirai (2016)



620GBit/s – Krebs on Security
1 TBit/s – OHV

Neue Auswirkungen

- Social Media Response
  - Twitter, Facebook

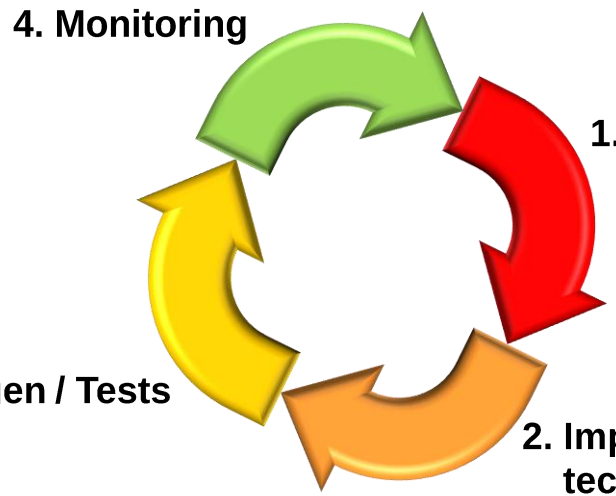
WM 2012

- Information Disclosure
  - Kedi RAT (2017), …

Quellen: F-Secure, Computerbild, Incapsula, Sophos

Maßnahmenkatalog

Enterprise Risk Management

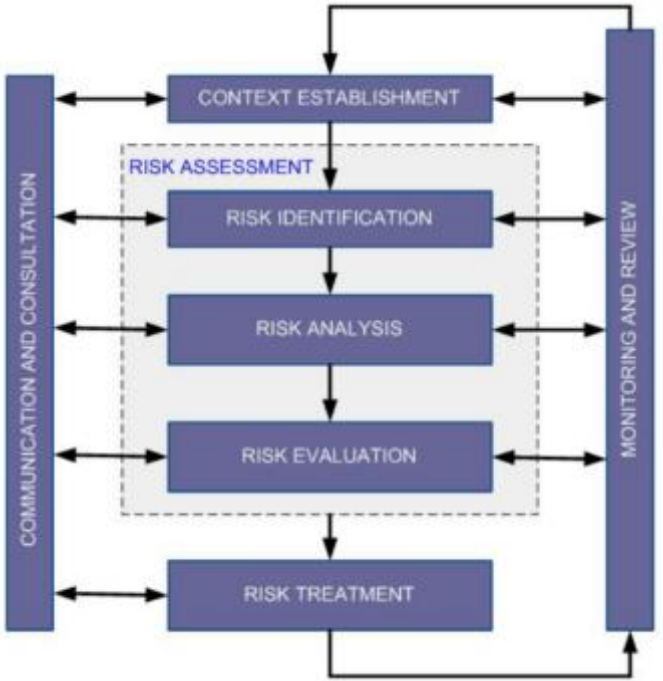


Risikoanalyse

Enterprise Risk Management

- **ISO/IEC 27005**
  - Risk Identification
    Assets, Threats, existing Controls, Vulnerabilities, Consequenences
  - Risk Analysis
  - Risk Evaluation

- **Risikoliste**
  - Bewertung nach Eintrittswahrscheinlichkeit und Auswirkung



Implementierung

Enterprise Risk Management

ERM Consult

Organisatorisch

Technisch

- DDoS Protection
- IDS/IPS
- FIM
- Vulnerability Mgmt
- SIEM
- Identity Management
- SOC
- Privileged Account Management
- Social Media Monitoring

Notfallpläne - Aufbau

Enterprise Risk Management

ERM Consult

In der Situation

Nr	Maßnahme	Wer
1	Server abschalten	OPS
2	Krisenstab verständigen	NFM
●		..
3		..

Unmittelbar danach

Nr	Maßnahme	Wer
1	Mitarbeiter informieren	PR
2		KO
●		..
3		..

Zusammenarbeit mit den Einsatzkräften

Nr	Maßnahme	Wer
1	Beweissicherung koordinieren	NFM
2		KO

Mögliche Notfallpläne:

- DDOS
- Virenbefall
- Data Loss
- Loss of Infrastructure
- Power Failure
- Shitstorm
- Hacker Attack
- ….

Tests

Enterprise Risk Management

ERM Consult

Test	Intervall	Teilnehmer	Test-Art
Krisenmanagement	1 x jährlich	KS-Kernteam + weitere	Boxed-Training
BCM-Test	1 x jährlich	Ausgewählte Bereiche	Wiederanlauf
Penetration Test	1 x jährlich	OPS + externe Tester	Pentest Watching
Technische Tests	t.b.d.	Notfall Organisation	Simulation
PR-Übungen	1 x jährlich	PR-Team	Simulation
…	…	…	…

Monitoring & Review

Enterprise Risk Management

ERM Consult

Themen

- Technologie
- Bedrohungen
- Angreifer Szene

Quellen

- Internet
- Branche
- Fachkonferenzen

Enterprise Risk Management

ERM Consult

Fragen, Anmerkungen, Kommentare?

Kontakt

office@erm-consult.com