Cyber Defence Like A Firefighter

Vorfälle und Krisen bewältigen

INVASE
SECURITY IN BUSINESS

Agenda

- Vorstellung
- Szenarien
- Herausforderungen bei Einsätzen / Vorfällen
- Parallelen
- Unterschiede
- Fazit

INVASE

Der Referent

- Jahrgang 1984, gelernter Informationselektroniker
- Militärzulieferer (NATO & Bündnispartner)
- Finanzinstitute
- Produzierende Industrie (Chemie, Pharma)
- Telekommunikation
- Kritische Infrastrukturen (KRITIS)
- Feuerwehr Nettetal

Cyber Defence & Resilience

Security Incident Response

Cyber Risk Management

IT-Outsourcing

INVASE

- Es ist 2:00 Uhr morgens
- Sie werden zu einer Ölspur alarmiert
- Kein Grund für Hektik
- Sie verfolgen die Ölspur bis zur Kurve…

INVASE

- Eine kleine Holzhütte brennt (Vollbrand)
- Alleinstehend auf einem Feld
- Sie befehlen den Löschangriff
- Brand wird trotzdem intensiver
- Eigentümer nicht auffindbar

Die Herausforderung

Security Incident Response ist oft Mangelverwaltung

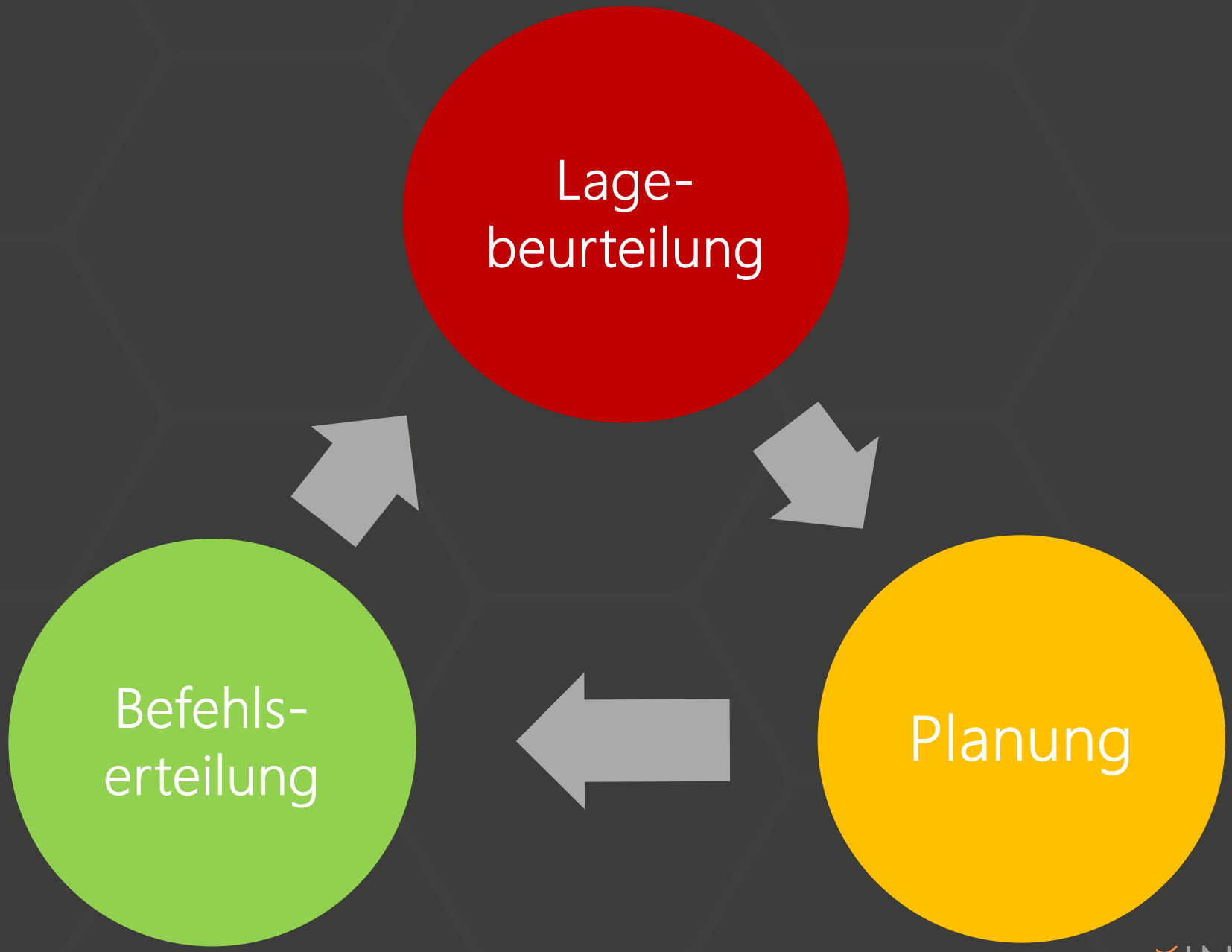
- Informationen
- Einsatzkräfte / Personal
- Material
- Zeit

INVASE

Vor die Lage kommen!

INVASE

Führungskreis



INVASE

Ablauf

1. Erkunden und Lagefeststellung

   Was ist bedroht?
   Wie wird bedroht?

2. Priorisieren und Koordinieren

   Einsatzabschnitte definieren
   Ressourcen einteilen
   Ziele befehlen

3. Ablaufüberwachung

   Strategie / Taktik angemessen?
   Lage unter Kontrolle?
   Eskalation unwahrscheinlich?

4. Gefahren beobachten

   Beeinflussen (neue) Faktoren die Lage?

INVASE

Grundsätze

1. Ruhe bewahren
2. Lage möglichst präzise sondieren
3. Fakten und Vermutungen differenzieren
4. Auf Methodik, Erfahrung, Konventionen verlassen
5. Szenario abstrahieren
6. Pragmatismus statt Hektik
7. Vorbereitung ist Trumpf!

INVASE

Die Unterschiede

- Gesetzlicher Brandschutz unterstützt auch bei der Feuerbekämpfung / kein Adäquat in der Cyber Defence (außer bei regulierten Branchen, KRITIS)
- Hierarchien, Organisationen (BOS, BBK) bestehen bereits seit Jahrzehnten
- Cyber Risiken sind abstrakt - intuitiv schwer zu erfassen
- 3 Lines of Defence
- Cyber-Bedrohungen durch Menschen gemacht (kriminell, organisiert…)
- Bedrohungen können sich täglich ändern (TTP)

INVASE

Cyber Kill Chain

Reconnaissance

Weaponization

Delivery

Exploitation

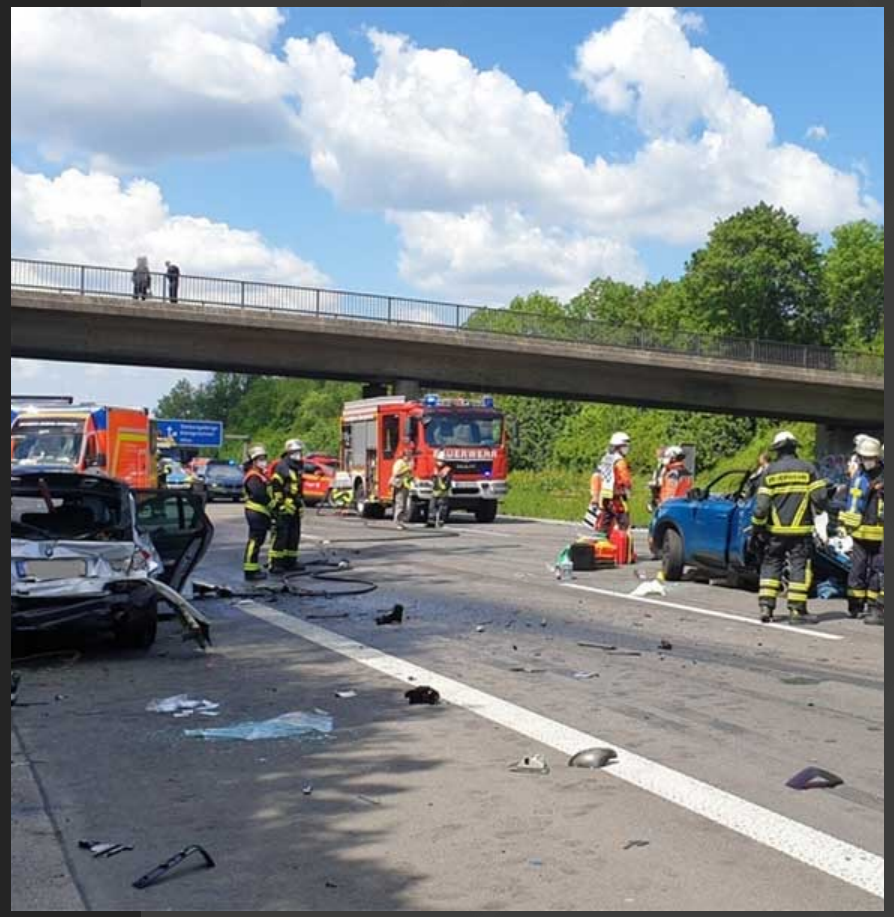
Installation

C&C

Actions on Objectives

INVASE

Neugeborenen-Heimfahrt



Sie fahren eine Mutter mit ihrem Neugeborenen nach Hause.

Sie haben die Wahl zwischen

einer Strecke über Landstraße und

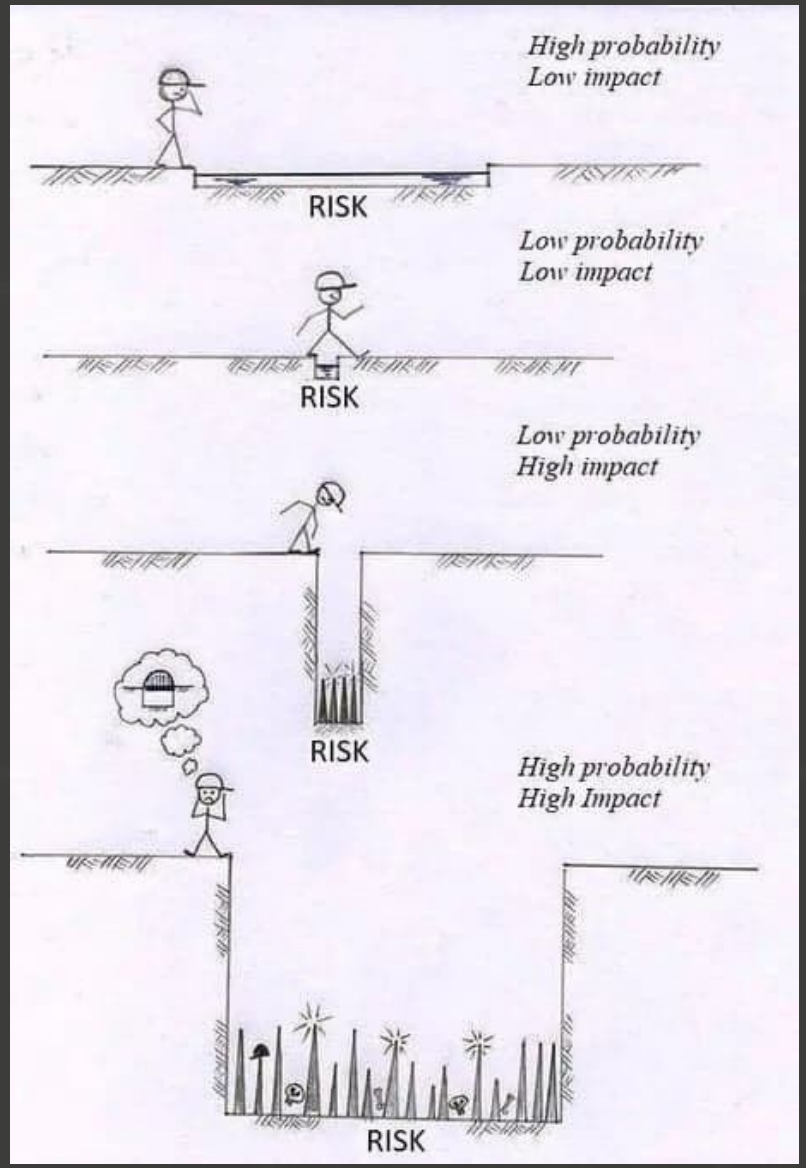
einer Strecke über Autobahn.

<u>Landstraße</u>
Unfälle seltener, häufiger tödlich

<u>Autobahn</u>
Unfälle häufiger, seltener tödlich

INVASE

Umgang mit Risiken



Statistiken unterstützen lediglich etwaige *Prognosen*.

Autobahnunfälle sind seltener tödlich, aber häufig mit *permanenten Folgeschäden*.

Landstraßenunfälle sind seltener, aber dafür häufiger tödlich
(u.a. wegen Frontalkollisionen mit anderen Fahrzeugen oder Hindernissen).

Auf Landstraßen, beispielsweise in der Eifel, sind Unfälle häufiger und schwerwiegender.

INVASE

Aus Katastrophen lernen

Aus Katastrophenszenarien zu Lernen ist nicht neu.

In Asien nimmt man sich die Natur als Vorbild, auch für betriebswirtschaftliche Themen.

Im Business Continuity Management (BCM) gibt es zahlreiche Erkenntnisse, die nach 9/11 erlangt wurden.

Auch aus der COVID-Pandemie kann man sinnvolle Erkenntnisse gewinnen.

Schwachstelle „Mensch“

Menschen suchen Komfort.

INVASE

Die Konsequenz?

Ungeschulte Menschen sind *einfache* Ziele.

INVASE

Risikomanagement und abstrakte Bedrohungen

- Abstrakte Bedrohungen schwer greifbar, aber durchaus messbar
- Wahrscheinlichkeit & Wahrnehmung
- Unwahrscheinlich vs Unmöglich
- Methodik gewinnt weiter an Bedeutung

Härtefall Pandemie

- Einer einzigen Ursache wurde global/regional unterschiedlich begegnet
- Zusätzlich: Informationsmangel verschärft Situationen
- Corona-Pandemie war ein Katalysator für Probleme *und* Lösungen

INVASE

Uns ist noch nie etwas passiert.

„Es entspricht der allgemeinen Lebenserfahrung, dass mit der Entstehung eines Brandes praktisch jederzeit gerechnet werden muss.

Der Umstand, dass in vielen Gebäuden jahrzehntelang kein Brand ausgebrochen ist, beweist nicht, dass keine Gefahr besteht, sondern stellt für die Betroffenen einen Glücksfall dar, mit dessen Ende jederzeit gerechnet werden muss.“

(Aus dem Gerichtsurteil des OVG Münster, Az 10A 363/86 vom 11.12.1987)

INVASE

INVASE
SECURITY IN BUSINESS

E-Mail: contact@invase.io

https://www.invase.io

TEL: +49 (0) 2153 9704160