Ablauf einer Cyberkrise

Know-how to go – Das Wissensfrühstück zum Thema Cyberkrisen

20.06.2022

Uwe Grams

Uwe Grams

- Experte für Krisenmanagement und Krisenkommunikation
- Unterstützung von Krisenstäben und IT-Leitungen
  - Aufbau von Krisenstäben und Bewältigung von Cyberkrisen
  - Einrichtung eines Notbetriebs
  - internen und externen Kommunikation
- Schwerpunkt außerhalb von Incident Response Einsätzen:
  Präventive Vorbereitung auf Schadensereignisse
  (BCM und Krisenmanagement)

Sophos-Bericht
State of ransomware

66%
wurden Opfer eines Ransomware-Angriffs
(78% Anstieg gegenüber 2020)

812.360 $
durchschnittliche Lösegeldzahlung
(480% Anstieg gegenüber 2020)

73%
konnten durch Backups Daten wiederherstellen

1,4 Mio. $
durchschnittliche Kosten zur Behebung der Angriffs-Folgen

Studienhintergrund:
- 5.600 IT-Entscheider
- 31 Länder
- 100-5.000 Mitarbeiter
- Jan/Feb 2022 für 2021

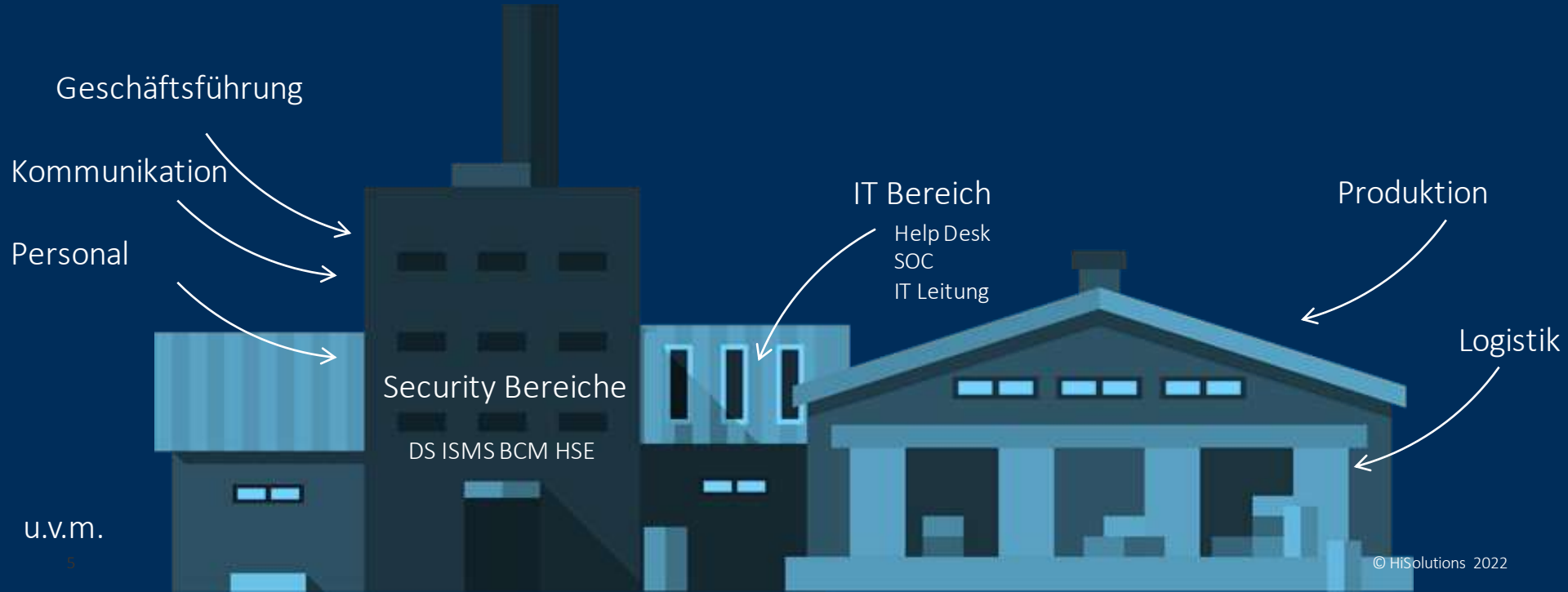
46% zahlen das Lösegeld | **4%** konnten dadurch alle Daten wiederherstellen

1 Monat
durchschnittliche Zeit bis zur kompletten Wiederherstellung

https://www.sophos.com/de-de/whitepaper/state-of-ransomware

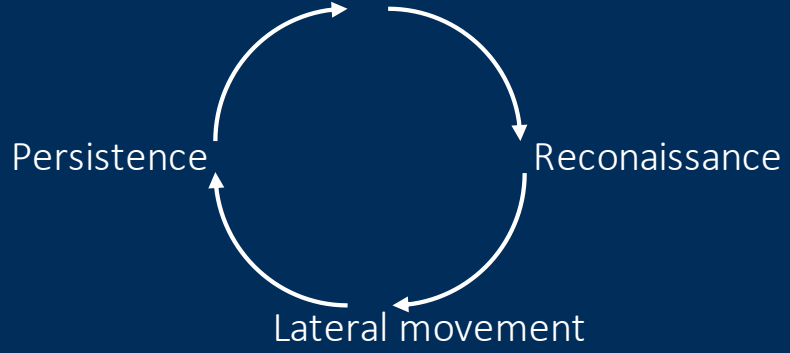
Prototypische Phasen eines Ransomware-Angriffs

Unser Beispielunternehmen



Infizierungsphase z.B. per Mail

Breach Foothold Privilege esc. Data leakage Final Attack



Geschäftsführung

Kommunikation

Personal

u.v.m.

IT Bereich

Help Desk
SOC
IT Leitung

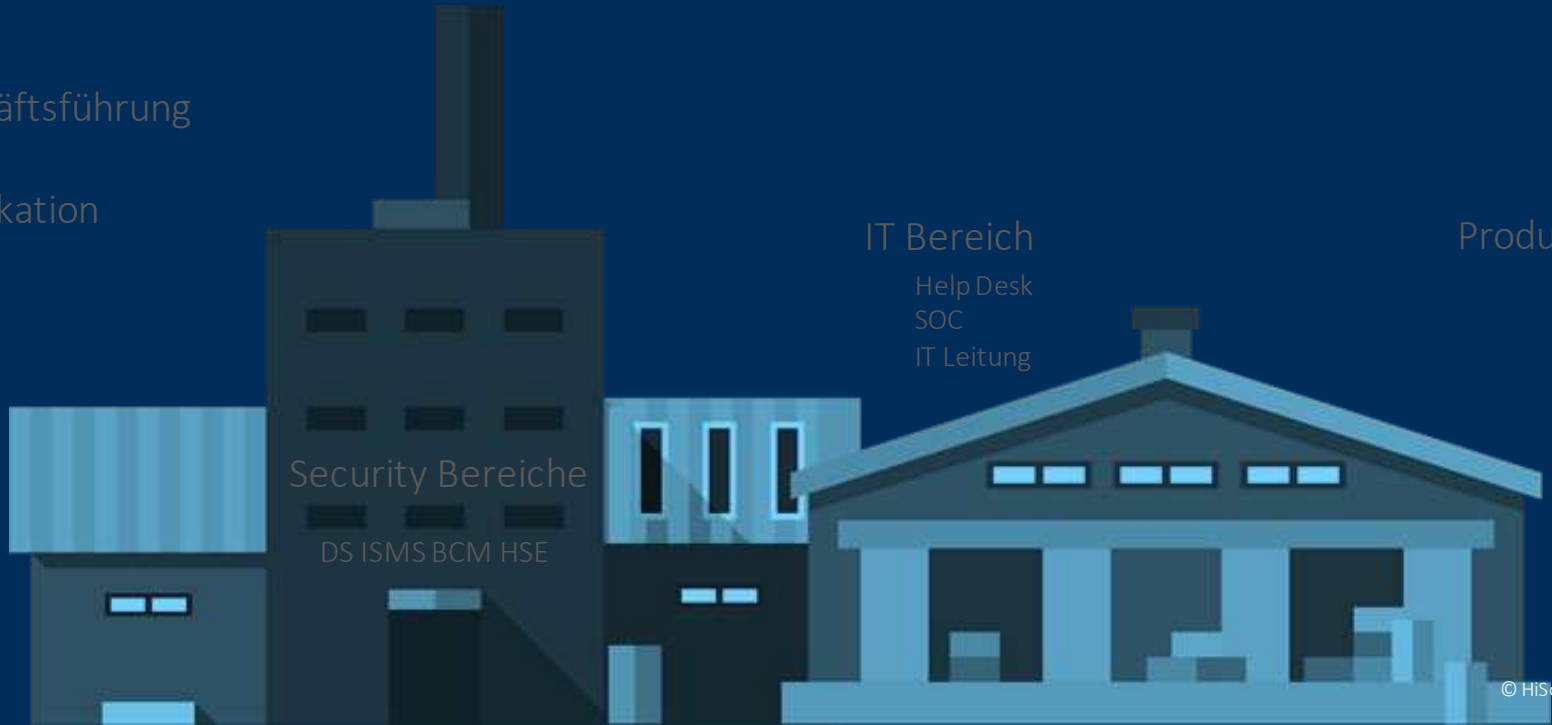
Produktion

Logistik

Security Bereiche

DS ISMS BCM HSE

01:10 Backups/Schattenkopien werden gelöscht und alle im Zugriff befindlichen Daten/Systeme werden verschlüsselt



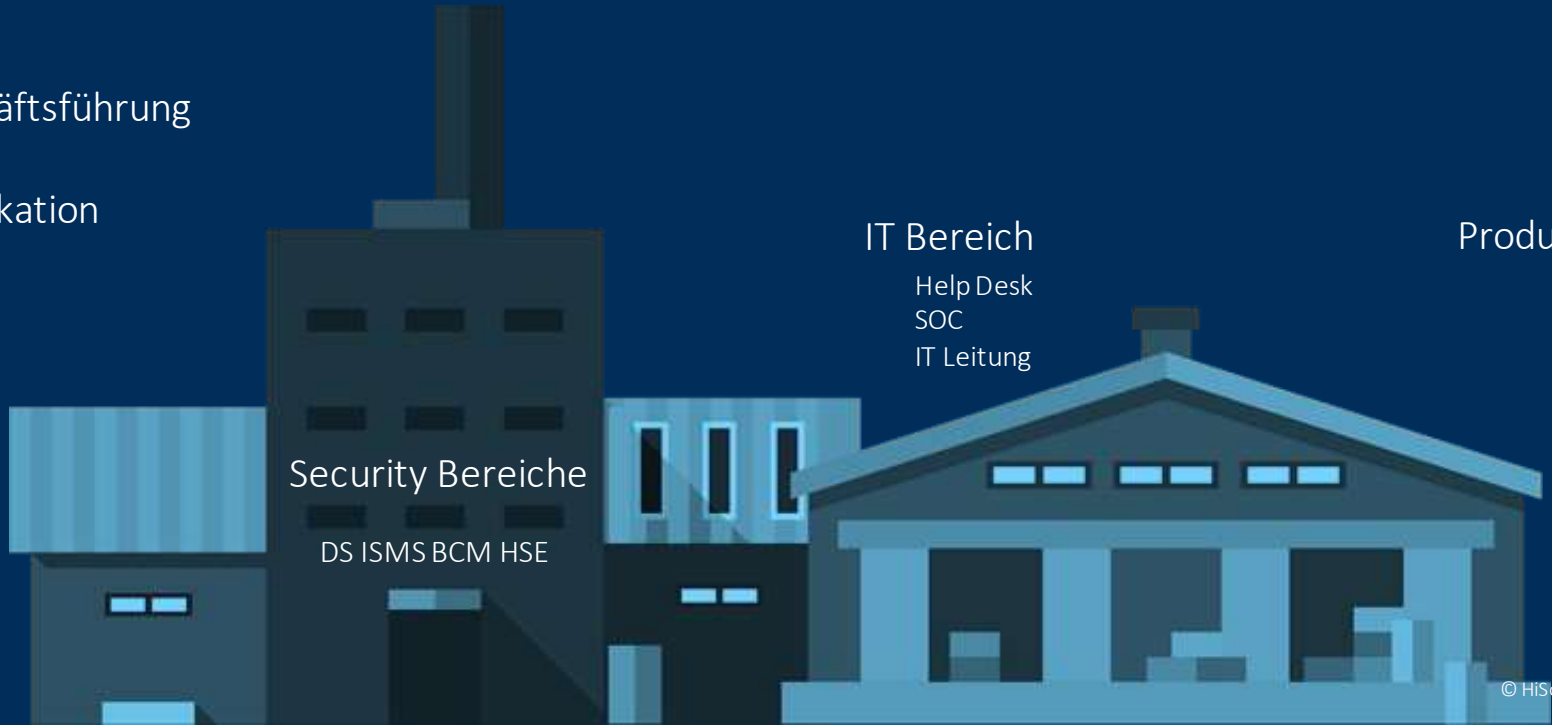
Chaosphase beginnt

Geschäftsführung

Kommunikation

Personal

u.v.m.



Security Bereiche

DS ISMS BCM HSE

IT Bereich

Help Desk
SOC
IT Leitung

Produktion

Logistik

Wir arbeiten als Team

Projektleiter & Krisenmanager

Technischer Einsatzleiter

Forensiker

Krisenkommunikation

Spezialist

IT-Koordinator

Support

Maßnahmen-tracking

Backoffice

Zielstellungen

Ein „Notarzt-Gleichnis“

Krisenmanagement

- Aufbau von Stabsprozessen
- Koordinierte Bewältigung & Kommunikation
- Notbetrieb der kritischen Prozesse

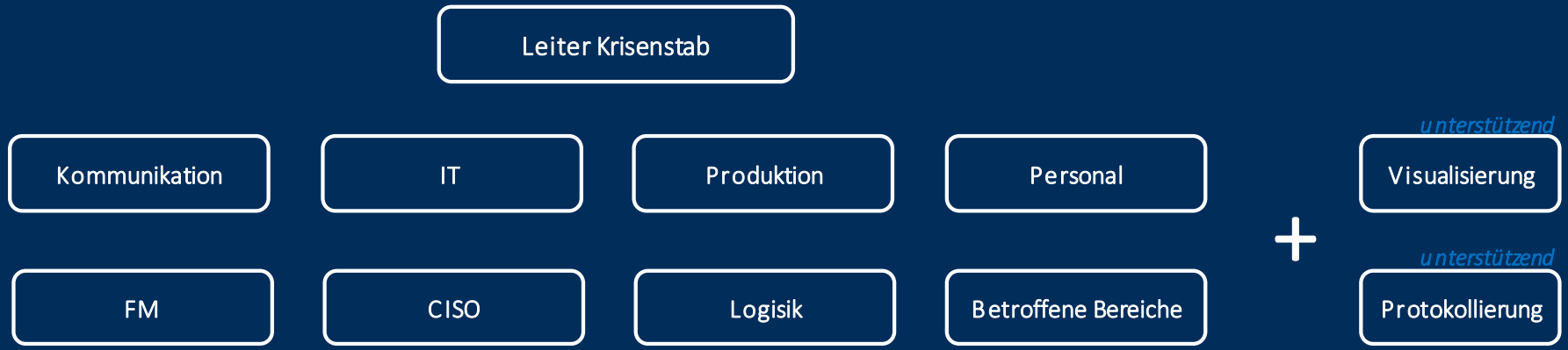
Forensik

- Beweismittelsicherung
- Beantwortung forensischer Fragestellungen
- Forensische Dokumentation

Wiederanlauf

- Notfallumgebung
- Wiederanlauf / Neuaufbau der IT
- Verbesserung der IT-Sicherheit

Chaosphase: Aufbau eines Krisenstabs



Lagebilderfassung

Steuerung von Aufgaben

Fokussierung auf das Wesentliche

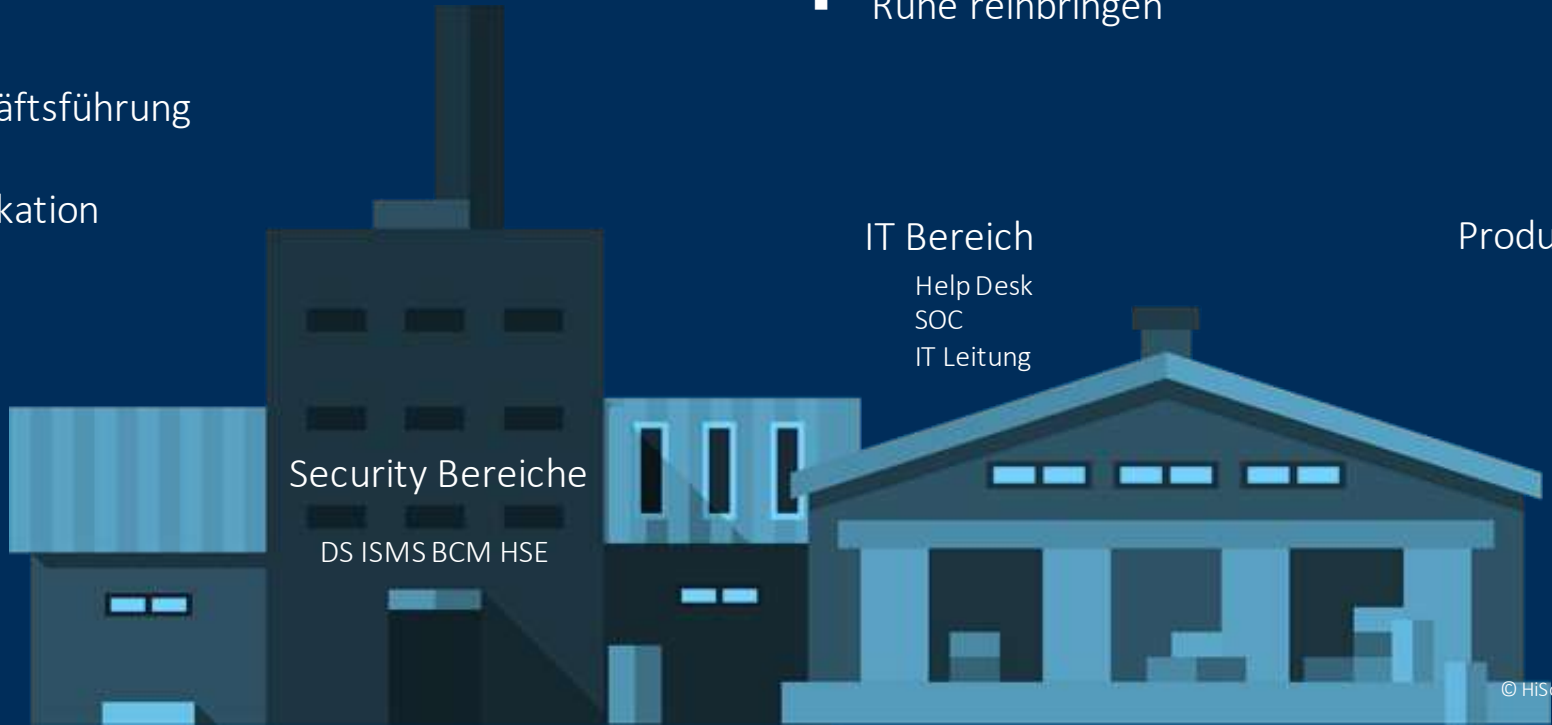
Chaosphase: Struktur gewinnen

- Forensik befähigen
- Transparenz über Ressourcen / Kritikalitäten gewinnen
- Kommunikation aufbauen
- Ruhe reinbringen

Geschäftsführung

Kommunikation

Personal



u.v.m.

Der Führungszyklus: Struktur halten

01 Lagefeststellung

- Was ist passiert?
- Wie ist es passiert?
- Welche Auswirkungen hat es?

02 Planung

- Welche Optionen stehen zur Verfügung?
- Welche Risiken haben die Optionen?
- Welchen Nutzen erreichen die Optionen?

03 Entscheidung

- Abwägen von Risiko und Nutzen
- Festlegen der Lösungsoptionen
- Leiter Krisenstab: Entscheidung treffen

04 Umsetzung

- Umsetzen der Entscheidung
- Anordnen der Maßnahmen
- Steuern der Maßnahmen

05 Kontrolle

- Beobachten der Umsetzung
- Feststellen der Wirksamkeit
- Erneute Lagebildung

Exkurs Krisenkommunikation

Intern

Wer muss erreicht werden?

Welches Interesse besteht für die Krise?

Extern

Wer veröffentlicht?

Grundregeln

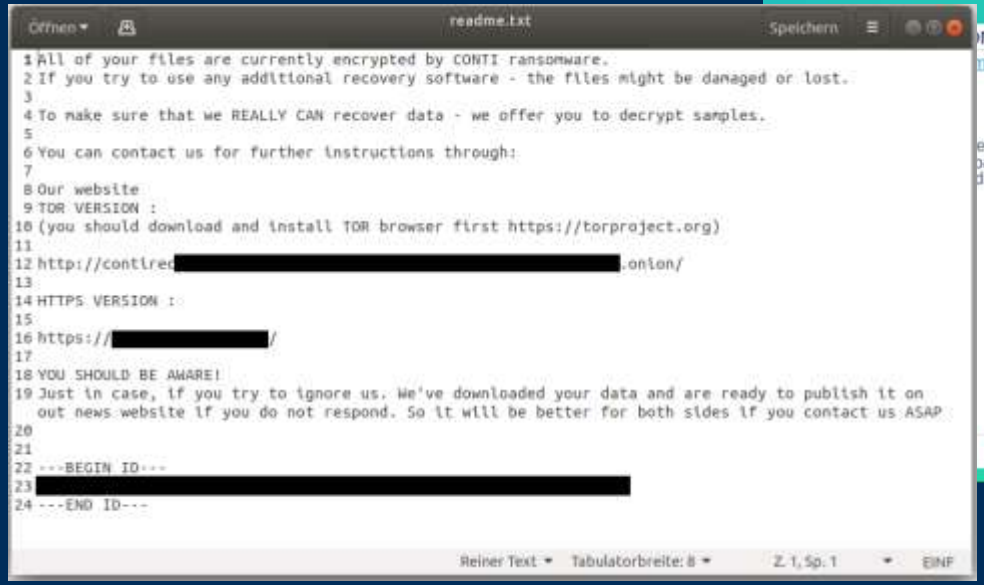
Medienarbeit

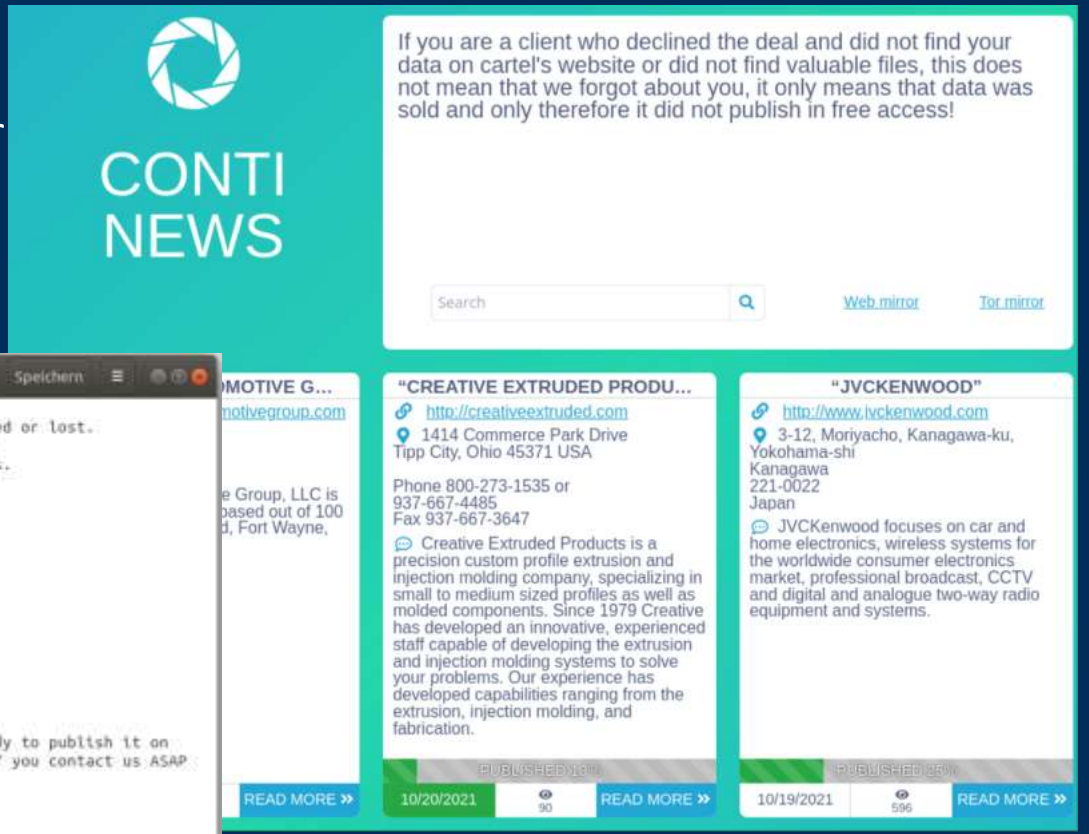
Wer ist verantwortlich?

One Voice Policy

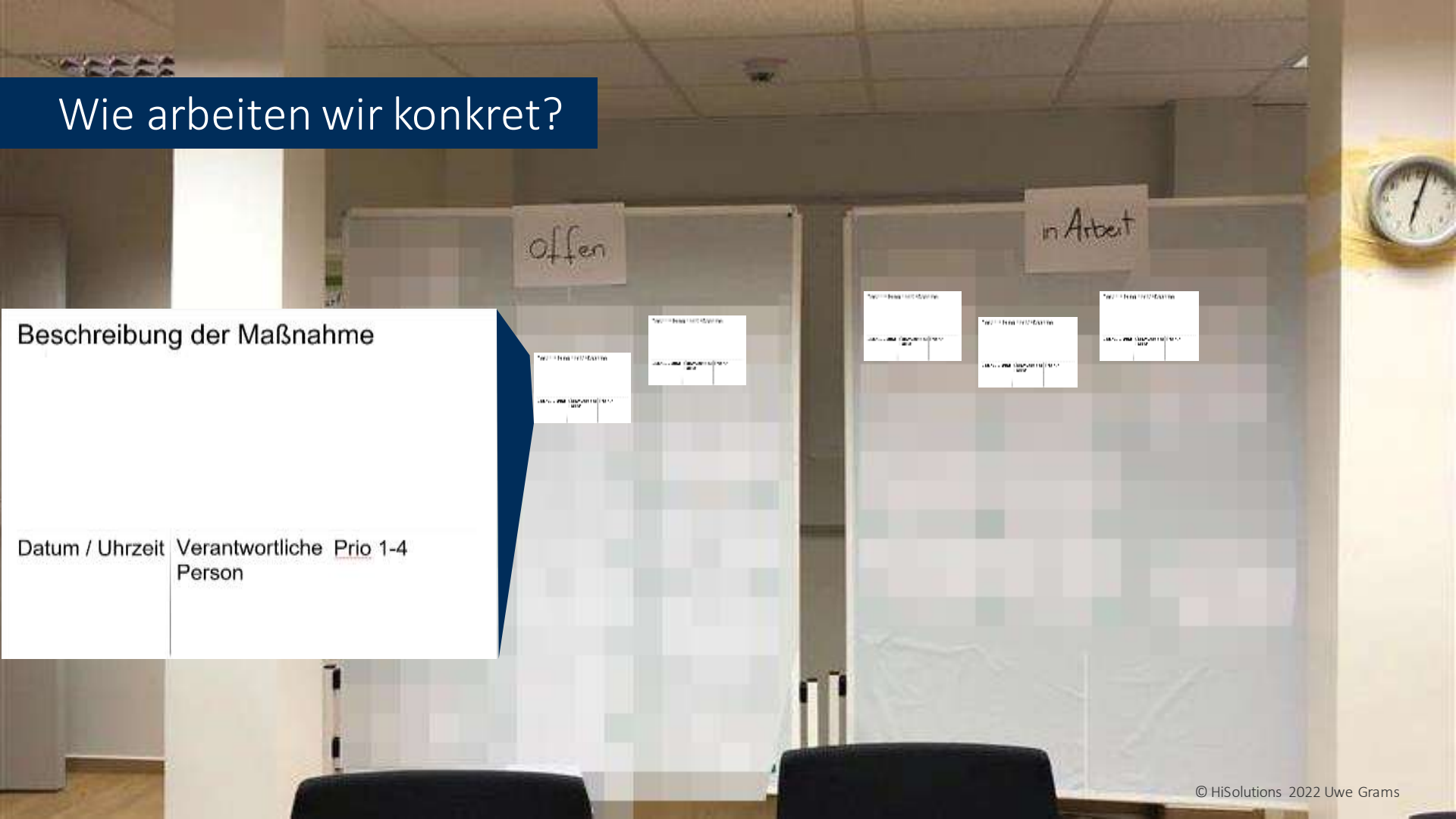
Kommunikationsstrategie

Was hält uns im Chaos
z.B. Backups sind nicht nutzbar
Ransomnote & Angreiferblog

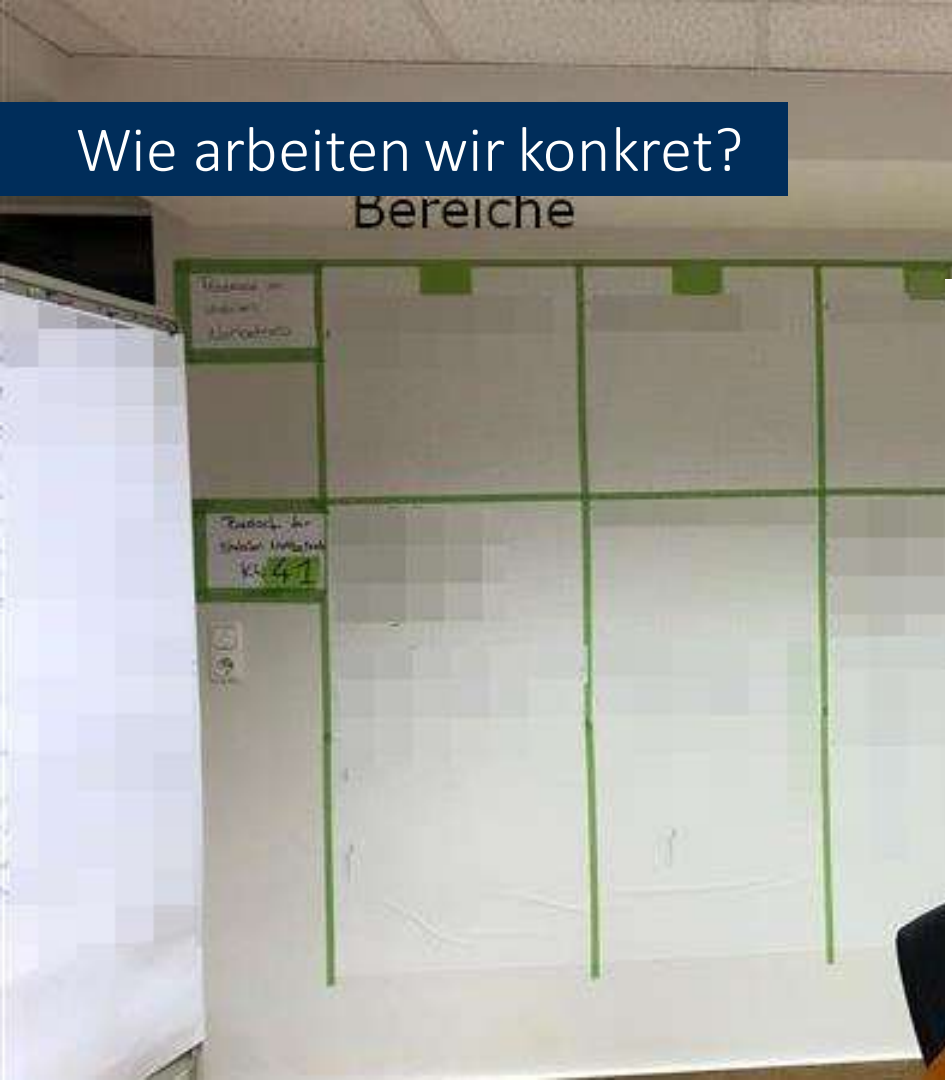




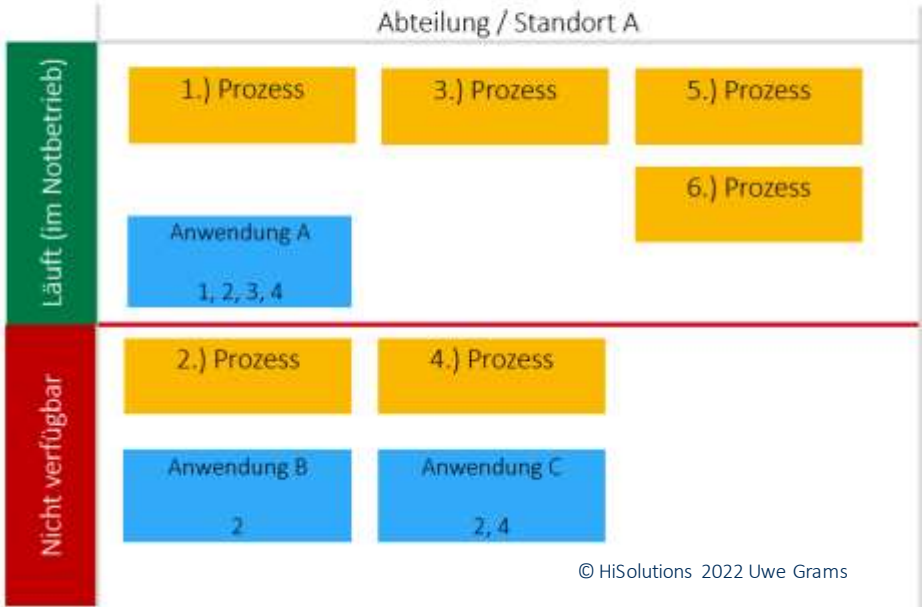
Wie arbeiten wir konkret?



Wie arbeiten wir konkret?



Übersicht von Prozessen und Anwendungen



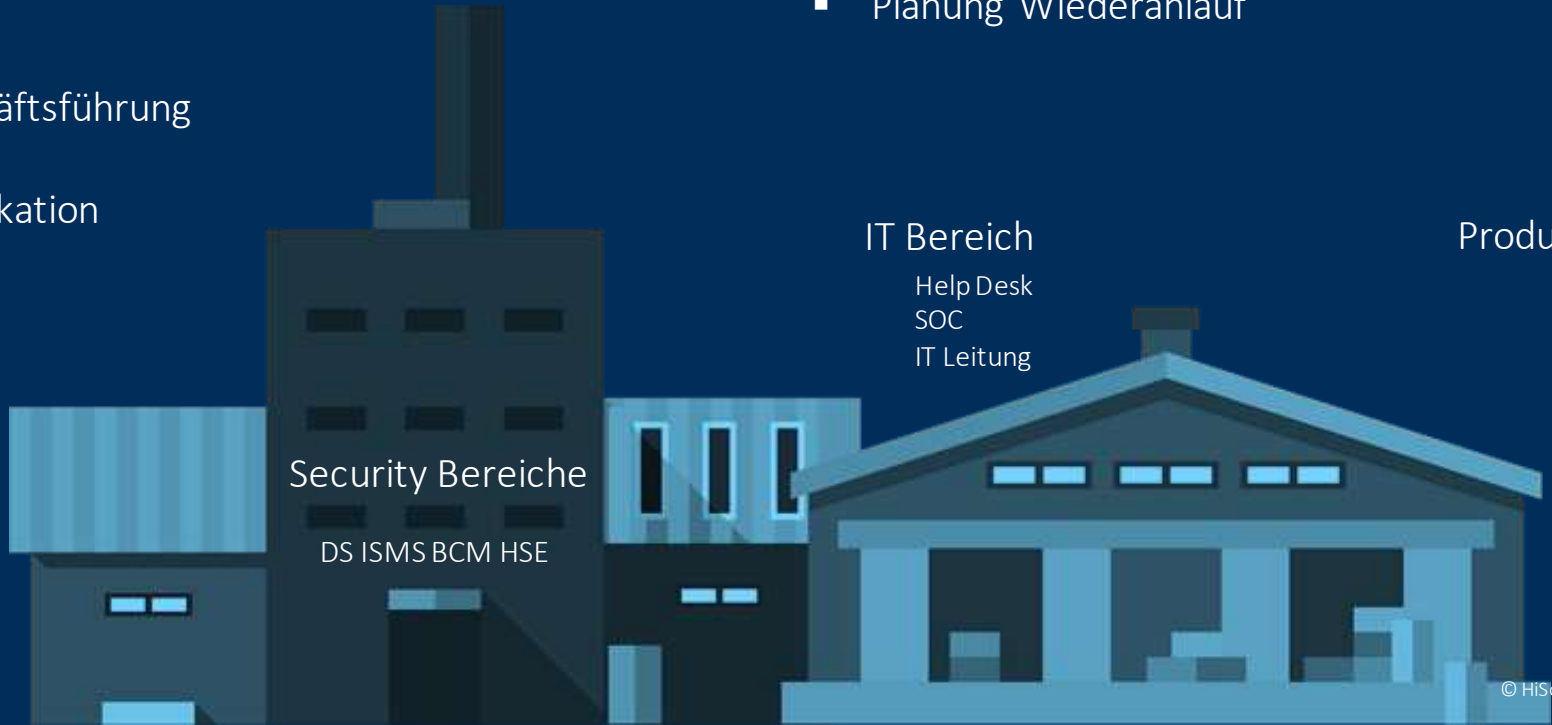
Konstituierungsphase: Es beginnt ein Regelbetrieb

- Forensik liefert Ergebnisse
- Notbetrieb wird aufgebaut
- Ermüdungserscheinungen nehmen zu
- Planung Wiederanlauf

Geschäftsführung

Kommunikation

Personal



u.v.m.

Stabiler Notbetrieb: Der Grundbetrieb läuft

- Der Notbetrieb wird ausgeweitet
- Paralleler (Neu-)Aufbau der IT-Landschaft
- Umsetzung IT-Sicherheit (Quick-Wins)
- Feinarbeiten und Details werden sichtbar

Geschäftsführung

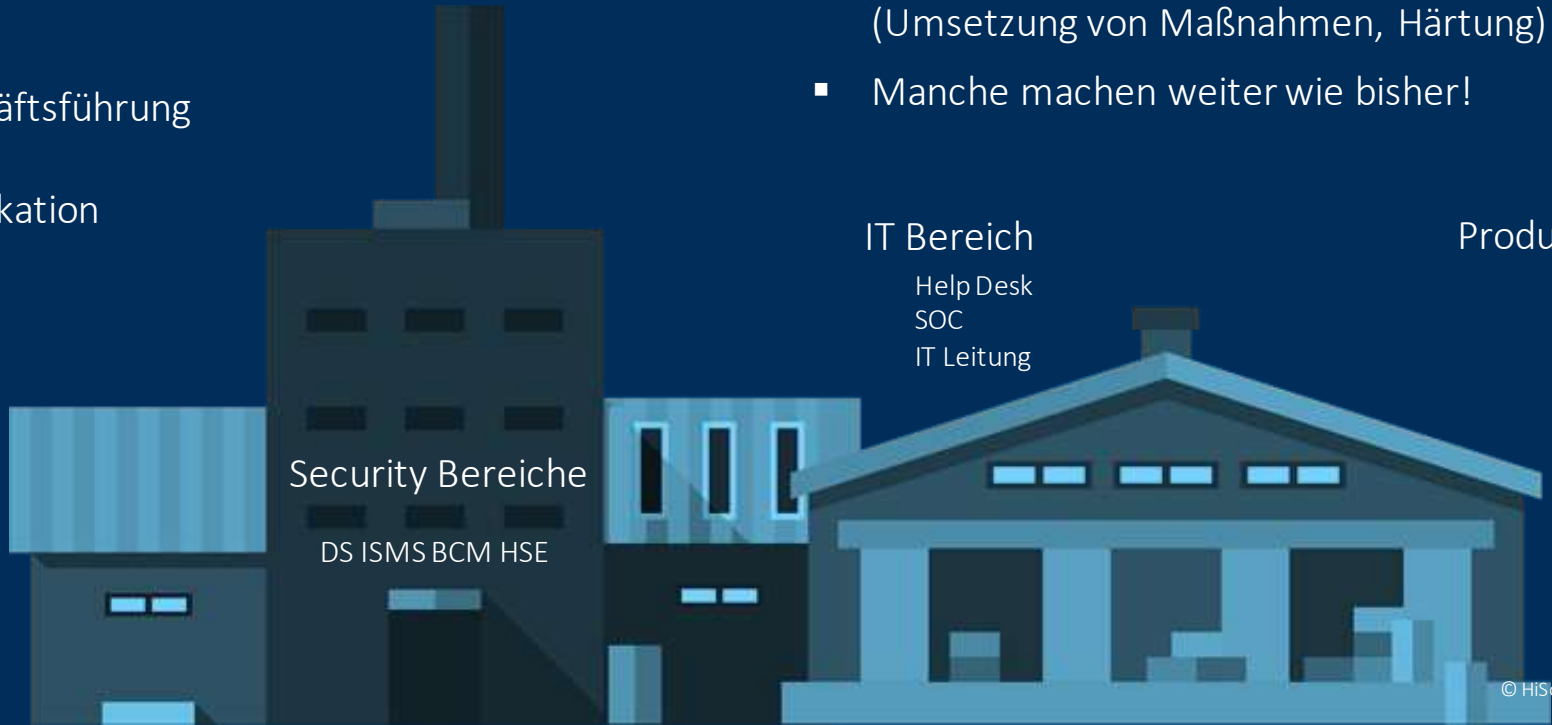
Kommunikation

Personal

u.v.m.

Übergang Normalbetrieb: Die Normalität kehrt zurück

- Kleinarbeiten dauern i. d. R. mehrere Monate
- Hohe Lernkurve/Awareness über die eigene (IT-)Sicherheit
- Verbesserung der IT-Sicherheit, BCM, KM (Umsetzung von Maßnahmen, Härtung)
- Manche machen weiter wie bisher!



Haben Sie Fragen?

Schloßstraße 1 | 12163 Berlin

info@hisolutions.com | +49 30 533 289 0

www.hisolutions.com