

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)

66%

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

812.360 \$

durchschnittliche Lösegeldzahlung
(480% Anstieg gegenüber 2020)

73%

konnten durch Backups Daten
wiederherstellen

Sophos-Bericht

State of ransomware

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

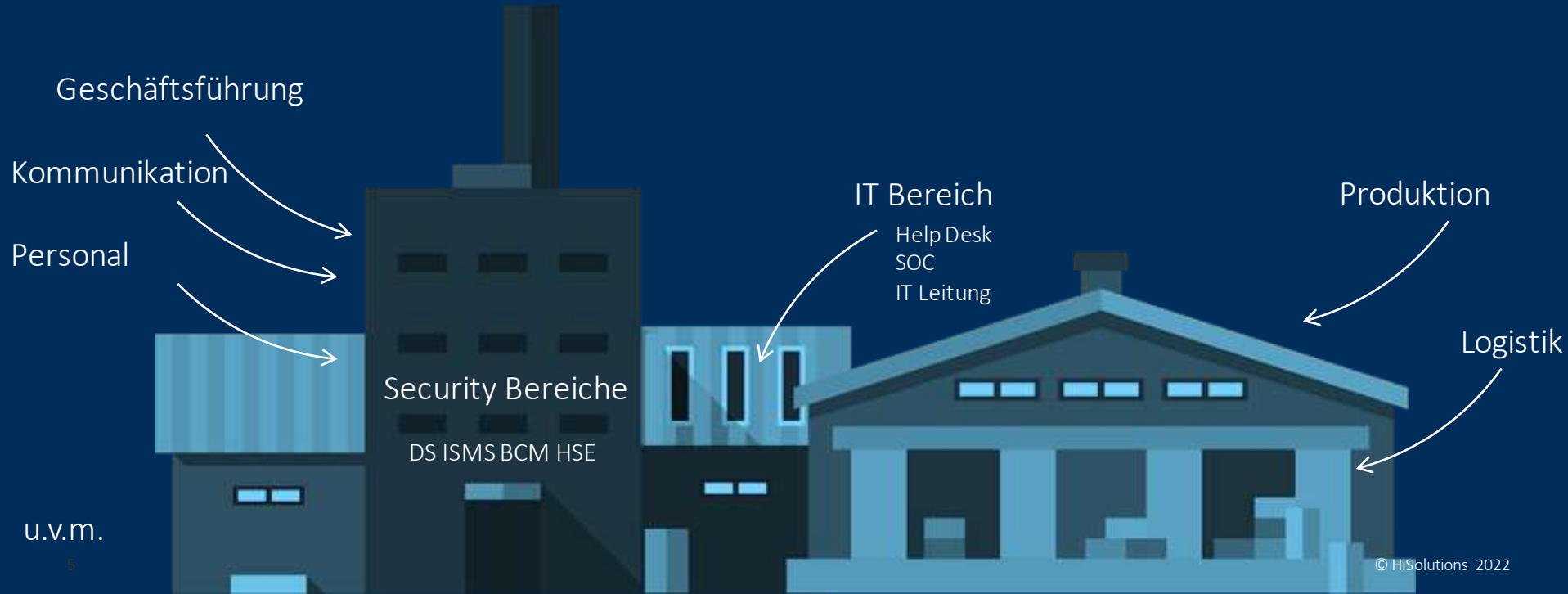
1 Monat

durchschnittliche Zeit bis zur
kompletten Wiederherstellung

Prototypische Phasen eines Ransomware-Angriffs



Unser Beispielunternehmen



Infizierungsphase
z.B. per Mail



Breach

Foothold

Privilege esc.

Data leakage

Final Attack

Persistence

Reconnaissance

Lateral movement

Geschäftsführung

Kommunikation

Personal

IT Bereich

Help Desk
SOC
IT Leitung

Produktion

Logistik

Security Bereiche

DS ISMS BCM HSE

u.v.m.

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

Geschäftsführung

Kommunikation

Personal

IT Bereich

Help Desk
SOC
IT Leitung

Produktion

Security Bereiche

DS ISMS BCM HSE

Logistik

u.v.m.

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

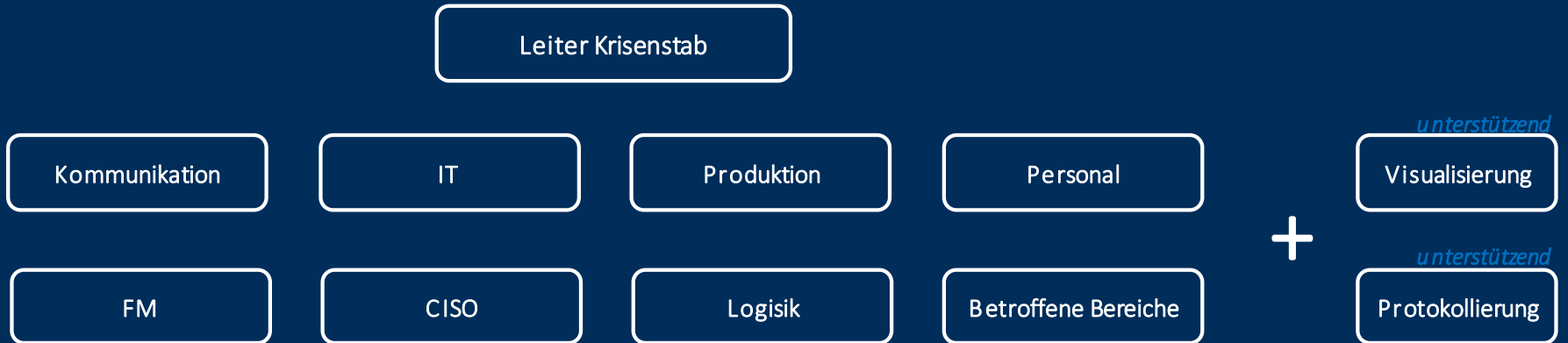
Forensik

- 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

IT Bereich

Help Desk
SOC
IT Leitung

Produktion

Security Bereiche

DS ISMS BCM HSE

Logistik

u.v.m.

Der Führungszyklus: Struktur halten

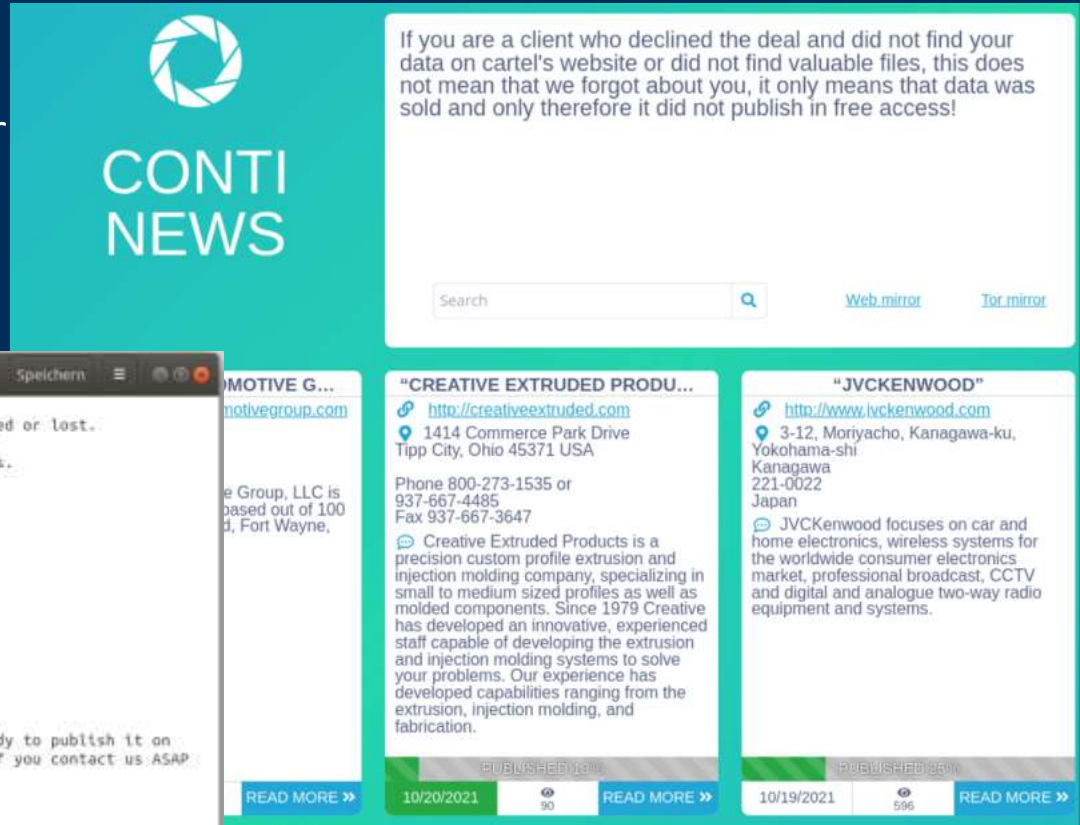


Exkurs Krisenkommunikation



Was hält uns im Chaos

z.B. Backups sind nicht nutzbar
Ransomnote & Angreiferblog



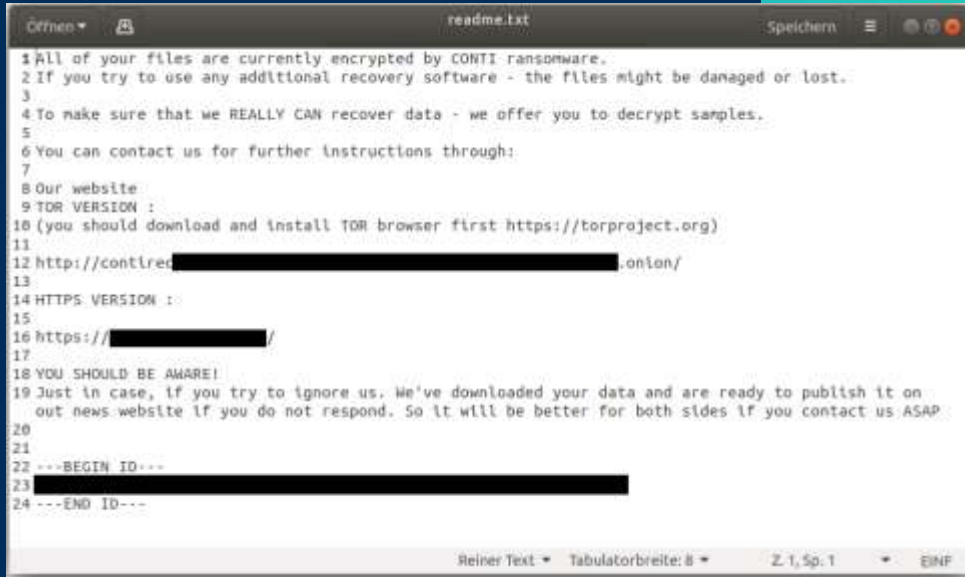
The image shows a screenshot of the CONTI NEWS website. At the top left is the CONTI NEWS logo, which consists of a camera shutter icon above the text "CONTI NEWS". Below the logo is a search bar and two links: "Web mirror" and "Tor mirror".

The main content area displays a ransom note on the left and a list of articles on the right. The ransom note is as follows:

```
1 All of your files are currently encrypted by CONTI ransomware.
2 If you try to use any additional recovery software - the files might be damaged or lost.
3
4 To make sure that we REALLY CAN recover data - we offer you to decrypt samples.
5
6 You can contact us for further instructions through:
7
8 Our website
9 TOR VERSION :
10 (you should download and install TOR browser first https://torproject.org)
11
12 http://contiread[REDACTED].onion/
13
14 HTTPS VERSION :
15
16 https://[REDACTED]/
17
18 YOU SHOULD BE AWARE!
19 Just in case, if you try to ignore us. We've downloaded your data and are ready to publish it on
   out news website if you do not respond. So it will be better for both sides if you contact us ASAP.
20
21
22 ---BEGIN ID---
23 [REDACTED]
24 ---END ID---
```

The article list on the right includes:

- "CREATIVE EXTRUDED PRODU..."**
Link: <http://creativeextruded.com>
Address: 1414 Commerce Park Drive, Tipp City, Ohio 45371 USA
Phone: 800-273-1535 or 937-667-4485
Fax: 937-667-3647
Description: Creative Extruded Products is a precision custom profile extrusion and injection molding company, specializing in small to medium sized profiles as well as molded components. Since 1979 Creative has developed an innovative, experienced staff capable of developing the extrusion and injection molding systems to solve your problems. Our experience has developed capabilities ranging from the extrusion, injection molding, and fabrication.
Published: 10/20/2021, 90 views, READ MORE >>
- "JVCKENWOOD"**
Link: <http://www.jvckenwood.com>
Address: 3-12, Moriyacho, Kanagawa-ku, Yokohama-shi, Kanagawa 221-0022, Japan
Description: JVCKenwood focuses on car and home electronics, wireless systems for the worldwide consumer electronics market, professional broadcast, CCTV and digital and analogue two-way radio equipment and systems.
Published: 10/19/2021, 596 views, READ MORE >>



The image shows a Notepad window titled "readme.txt" with the following text:

```
1 All of your files are currently encrypted by CONTI ransomware.
2 If you try to use any additional recovery software - the files might be damaged or lost.
3
4 To make sure that we REALLY CAN recover data - we offer you to decrypt samples.
5
6 You can contact us for further instructions through:
7
8 Our website
9 TOR VERSION :
10 (you should download and install TOR browser first https://torproject.org)
11
12 http://contiread[REDACTED].onion/
13
14 HTTPS VERSION :
15
16 https://[REDACTED]/
17
18 YOU SHOULD BE AWARE!
19 Just in case, if you try to ignore us. We've downloaded your data and are ready to publish it on
   out news website if you do not respond. So it will be better for both sides if you contact us ASAP.
20
21
22 ---BEGIN ID---
23 [REDACTED]
24 ---END ID---
```

Wie arbeiten wir konkret?

offen

in Arbeit

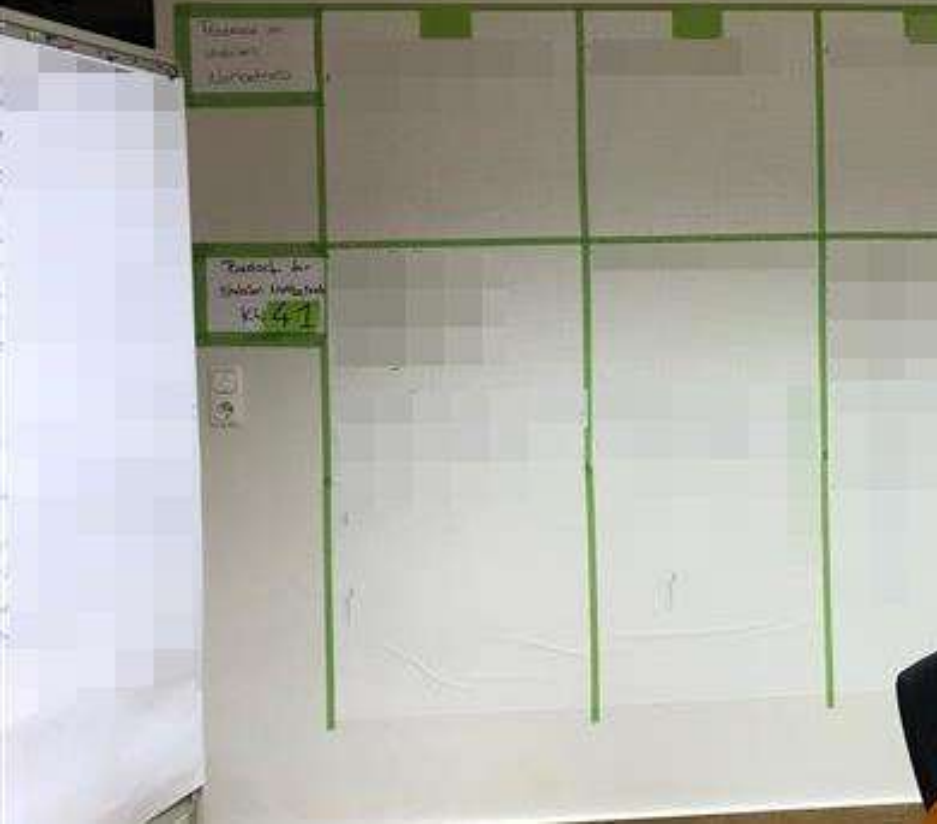


Beschreibung der Maßnahme

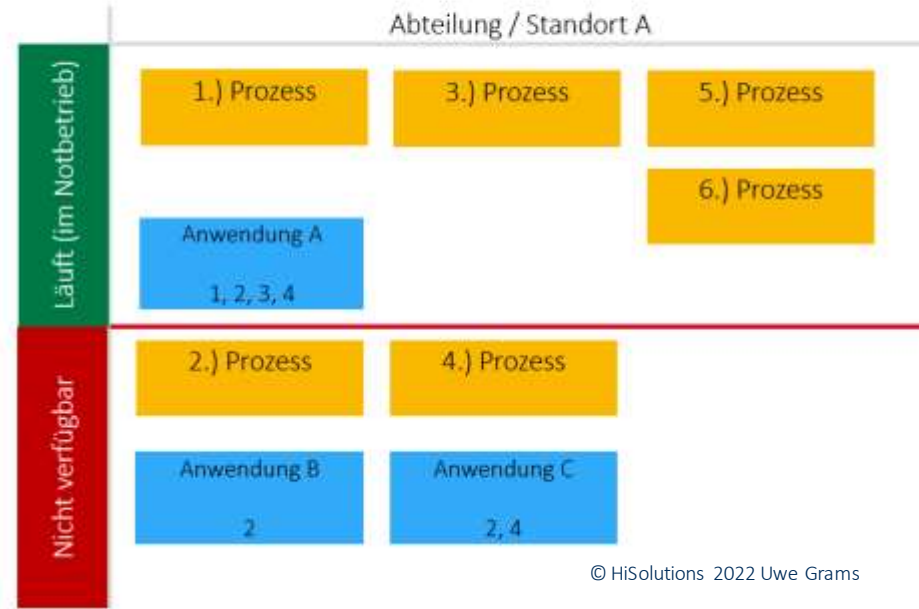
Datum / Uhrzeit Verantwortliche Prio 1-4
Person

Wie arbeiten wir konkret?

Bereiche



Übersicht von Prozessen und Anwendungen



Konstituierungsphase: Es beginnt ein Regelbetrieb

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

Geschäftsführung

Kommunikation

Personal

IT Bereich

Help Desk
SOC
IT Leitung

Produktion

Security Bereiche

DS ISMS BCM HSE

Logistik

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

IT Bereich

Help Desk
SOC
IT Leitung

Produktion

Security Bereiche

DS ISMS BCM HSE

Logistik

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!

Geschäftsführung

Kommunikation

Personal

IT Bereich

Help Desk
SOC
IT Leitung

Produktion

Security Bereiche

DS ISMS BCM HSE

Logistik

u.v.m.

Haben Sie Fragen?



Schloßstraße 1 | 12163 Berlin

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

www.hisolutions.com