CORPORATE TRUST
business risk & crisis management

Ransomware-Angriff bestätigt?

Sofortmaßnahmen ergreifen

- Netzwerk isolieren
  - Außenstellen sichern
- Backup sichern
- Verschlüsselung stoppen
- Externe Passwörter ändern

- Team zusammenrufen
- Erste Planung Kriseneinsatz

- OSINT Ransomware
- Schaden feststellen
- Krise organisieren

IT-Notfallstab, CSIRT

- Notbetrieb aufbauen
- Wiederherstellung planen
- Forensik
  - Säubern
- Neu-aufbau
- Forensik

Krisenstab, CMT

- Täterkommunikation
- Erpressungs-zahlung
- Krisenkommunikation
- Stakeholder-Management
- Polizei
- Versicherung
- Datenschutz

Erste Stunden

Erster Tag

Tag zwei bis Krisenende (~8-12 Wochen)

- ○ Sofortmaßnahmen umgesetzt.
- ○ Notwendige Expertise an Bord.
- ○ Schadensumfang bestimmt.
- ○ Erste Infos zu Tätern vorhanden.
- ○ Erste Sitzung CMT durchgeführt.
- ○ Offline Notbetrieb entschieden.
- ○ Erste Infos an MA & Kunden verteilt.
- ○ Kommunikations-prozesse definiert.
- ○ Erste IT-Systeme laufen wieder.
- ○ 80% Business läuft im Notbetrieb.
- ○ Beweise für die Forensik gesichert.
- ○ Wiederherstellung durchgeplant.
- ○ CMT aufgelöst, Aufgaben verteilt.
- ○ 80% Business läuft im Normalbetrieb.
- ○ Lessons Learned durchgeführt.