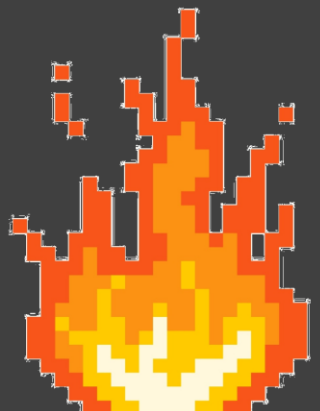
Umgang mit dem Cyberangriff auf den Landkreis Anhalt-Bitterfeld


WE ARE
EXPERIENCING
TECHNICAL
DIFFICULTIES

Angriff

- mehrstufiger Angriff / verschlüsselte Rechner
- Verschlüsselung von Hand ausgelöst, aber keine Aussagen möglich, wann sich der Angreifer im System angemeldet hat, Logs fehlen
- Angreifer hat sich wahrscheinlich bewusst auf den Systemen umgesehen
- Verschlüsselung läuft sehr schnell, richtet großen Schaden an



Maßnahmen

- alle kritischen Systeme vom Netz getrennt, um weiteren Datenabfluss zu unterbinden und um Ausbreitung der Schadsoftware verhindern
- Informationspflichten (Landesdatenschutz, Landesdatennetz)
- Backups sichten, Server überprüfen
- Hilfe / Unterstützung beim Land angefragt
- Ausrufen Katastrophenfall
- **keine Lösegeldzahlung - Wiederaufbau**

Unterstützung

- Ministerium der Finanzen Land Sachsen-Anhalt (Abordnung IT-SiBe) mit CERT Nord
  - Forensik, Datenwiederherstellung, Projektmanagement
  - IT-Projektkoordinator Wiederaufbau
- BSI - Krisenteam entsendet (Forensik, Datenrettung
- Bundeswehr – technische Amtshilfe

- *beratend vor Ort: Hochschule Harz via damaliger Staatssekretär für Digitalisierung*

Wiederaufbau

- Notbetriebsnetz
  - physisch von der bisherigen Infrastruuktur getrennt
- Zwischeninfrastruktur
  - ausschließlich hoch priorisierte Fachverfahren
  - Aufbau in isoliertem Netzbereich
  - Datenbestände problematisch
- Zielinfrastruktur
  - Aufbau, dann Kopplung mit Zwischeninfrastruktur

Veränderungen

- Technisch
  - BSI-Grundschutz
  - Backups und Dokumentationen
  - Incident Response
  - Personalaufwuchs
- Resilienz
  - dokumentierte Prozesse, Fallback-Mechanismen
- Organisatorisch
  - Fachbereich Informationstechnik und Digitalisierung
  - Benennung IT-Sicherheitsbeauftragte*r
  - Dienstanweisungen
  - Wiederanlaufpläne / Notfallpläne
- Bedarfe formulieren
  - CHW
  - SOC, ggf. auf Landesebene
  - Kommunales Lagebild

Wissenstransfer

- Expertengremium (Uni Magdeburg, BSI, CIR BW, SNV, AG KRITIS, MID LSA)
- Vorträge mit unterschiedlichem Fokus
- Seminare in verschiedenen Formaten
- Beteiligung in Arbeitsgruppen und Dialogformaten
- Interviews für Studierende
- Gastvorlesungen
- Forschungsprojekte
- Handreichung

Vielen Dank

Sabine Griebsch
CDO (ext.) Landkreis Anhalt-Bitterfeld
cdo@anhalt-bitterfeld.de