Ransomware: Cyberangriff auf den Landkreis Anhalt-Bitterfeld

Sabine Griebsch, CDO (ext.) Landkreis Anhalt-Bitterfeld

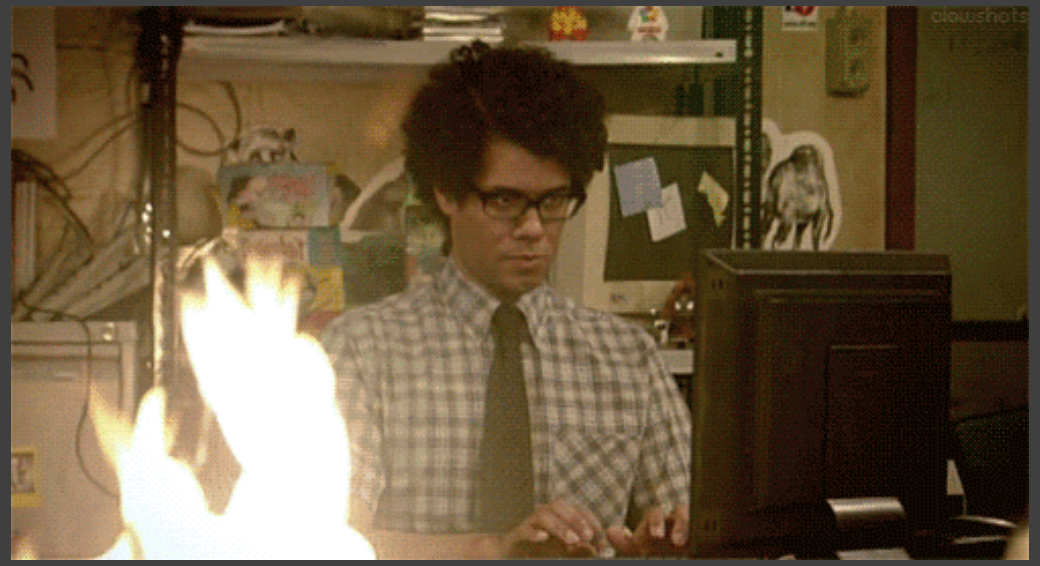
Sicherheitsvorfall

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

Krisenmanagement

- Trennung kritischer Systeme vom Netz (weiteren Datenabfluss unterbinden, weitere Ausbreitung der Schadsoftware zu verhindern)
- Informationspflichten
- Backups sichten / Server überprüfen

- Katastrophenfall (SAE, Unterstützung Land, TEL 1 und 2, Amtshilfeersuchen) und Unterstützung durch Externe
- Wiederaufbau der gesamten IT-Systeme
  - noch nicht vollständig wiederaufgebaut



IT-Sicherheit

- technische Maßnahmen und finanzielle Mittel
  - Grundlegendes IT-Sicherheitskonzept (Rechte, Rollen On-/Offboarding)
  - erneuertes Backup-Konzept
  - Überwachung der Infrastruktur
  - Multi-Faktor-Authentifizierung
  - → BSI-Grundschutz

- Routinen (auch analog verfügbar)
  - Wiederanlaufpläne
  - Ansprechpartner, Kenntnis der Angebote und der Akteure

Lessons Learned 1/2

- organisatorische Maßnahmen
  - Ressourcen IT-Infrastruktur, Stärkung IT, IT-SiBe, aktuelle Dienstanweisungen
- Bewusstsein für IT-Sicherheit
  - Awareness-Schulungen, transparente Informationen
  - Zusammenarbeit, frühzeitig organisieren, Ebenen übergreifende Arbeitsgruppen

Lessons Learned 2/2

- nachhaltige Digitalisierung
  - sichere IT-Infrastruktur / sichere Fachverfahren / Entwicklungen auf Bundesebene
  - Vertrauen, darauf dass digitale Infrastruktur morgen noch funktionsfähig ist
- resiliente Infrastrukturen
  - Backups und Dokumentationen
  - Dokumentierte Prozesse und Fallback-Mechanismen
- Lagebild / SOC
  - nichtkommerzielle Erste Hilfe (CHW), spezialisiert auf behördliche Strukturen