Rebuilding Landkreis Anhalt-Bitterfeld

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

Manuel Atug, AG KRITIS

vor 16 Monaten…

- 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

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

Rebuilding Landkreis Anhalt-Bitterfeld

- **Katastrophenfall (SAE, Unterstützung Land, TEL 1 und 2, Amtshilfeersuchen) und Unterstützung durch Externe**
- Wiederaufbau der gesamten IT-Systeme
  - Notnetz, Zwischeninfrastruktur (←Konzept→) Zielinfrastruktur
  - noch nicht vollständig wiederaufgebaut
- Schadensbilanz
  - 2 Mio €
  - Datenverlust, Ausfallzeiten, Mehraufwand
  - Datenveröffentlichung, Vertrauensverlust

Maßnahmen 1/3

- 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

Maßnahmen 2/3

- 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

Katastrophenfall

„Dieser Angriff hat auf alle Bereiche des Leistungsspektrums des Landkreises unmittelbare Auswirkungen und betrifft somit auch Anliegen der BürgerInnen, die zurzeit nicht bearbeitet werden können. Zudem sind zum gegenwärtigen Zeitpunkt weitere Folgen nicht absehbar.“

- neue Herausforderungen: IT, Organisation und Recht im Fokus
- Resilienz!

Maßnahmen 3/3 - übergeordnet

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

Cyber-Hilfswerk

- Das CHW soll die existierenden Bewältigungskapazitäten für Großschadenslagen durch Cybervorfälle bei Kritischen Infrastrukturen kooperativ ergänzen

Cyber-Hilfswerk

- Wiederherstellung der Versorgung der Bevölkerung
- IT-Sicherheit verbessern reicht nicht mehr, wir brauchen Incident Response und Krisenbewältigungs-kapazitäten!
- Ehrenamtliche digitale KatastrophenschutzhelferInnen

Cyber-Hilfswerk

- CHW Konzept Version 1.1
  mit umfangreichen Erweiterungen
  veröffentlicht:

https://ag.kritis.info/2022/11/09/update-des-cyberhilfswerk-konzept/

Cyber-Hilfswerk: Update v1.1

- MIEVS: Mobile Internet-Erstversorgungsstationen
- Erste Überlegungen einer europäischen Ebene
- Gemeinsamer Lenkungskreis der AG KRITIS mit dem THW zur aktiven und praktischen Ausgestaltung eines CHW im THW