Städtisches Klinikum Wolfenbüttel

Cyberattacke: Praxisbericht aus einem betroffenen Unternehmen

Geschäftsführer Axel Burghardt

Präsentation: IT-Leiter Skalski und Verwaltungsdirektor Keunecke

28.11.2023

Themen:

Städtisches Klinikum Wolfenbüttel

- Ausgangssituation
- Ablauf
- Angriff
- Gewinne / Verluste
- Fazit

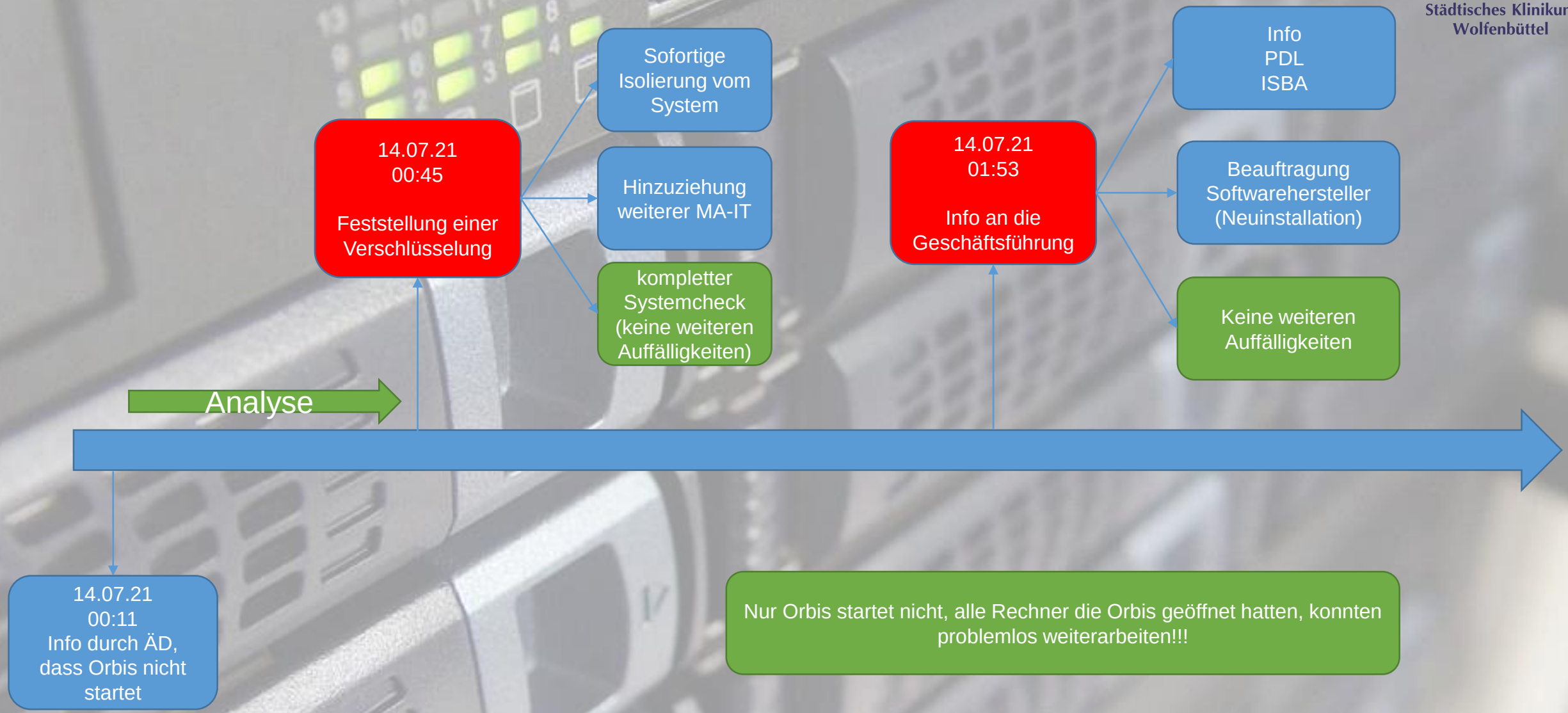
Ausgangssituation

Städtisches Klinikum Wolfenbüttel

- Mehrtägige Gap-Analyse (2017) mit nahezu komplett abgearbeitetem Maßnahmenplan
- dabei externe mehrjährige Begleitung analog Anforderungen an Kritische Infrastrukturen
- Verfeinerung Sicherheitskonzept
- Parallel weiterer IT-Ausbau und Digitalisierung
- Digitalisierungsgrad im Jahr der Cyberattacke 2021

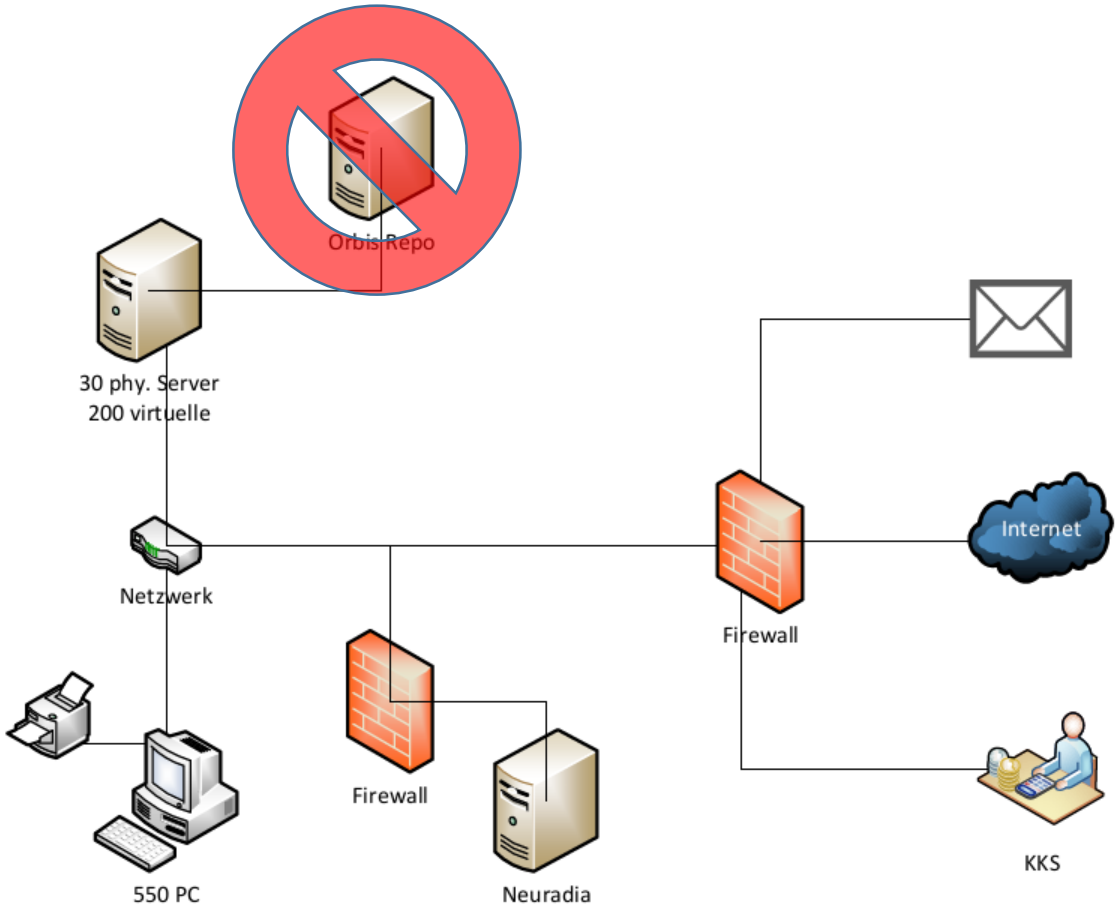
Chronologischer Ablauf

Städtisches Klinikum Wolfenbüttel



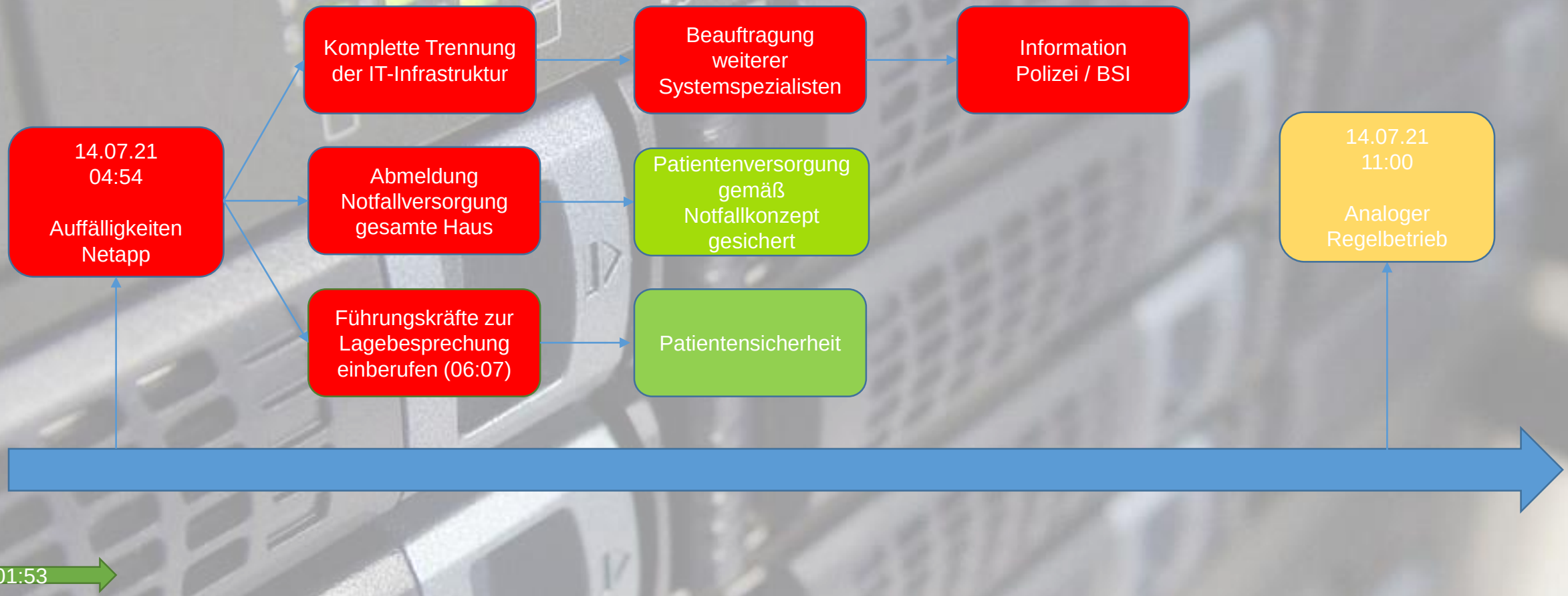
Überblick

Städtisches Klinikum Wolfenbüttel



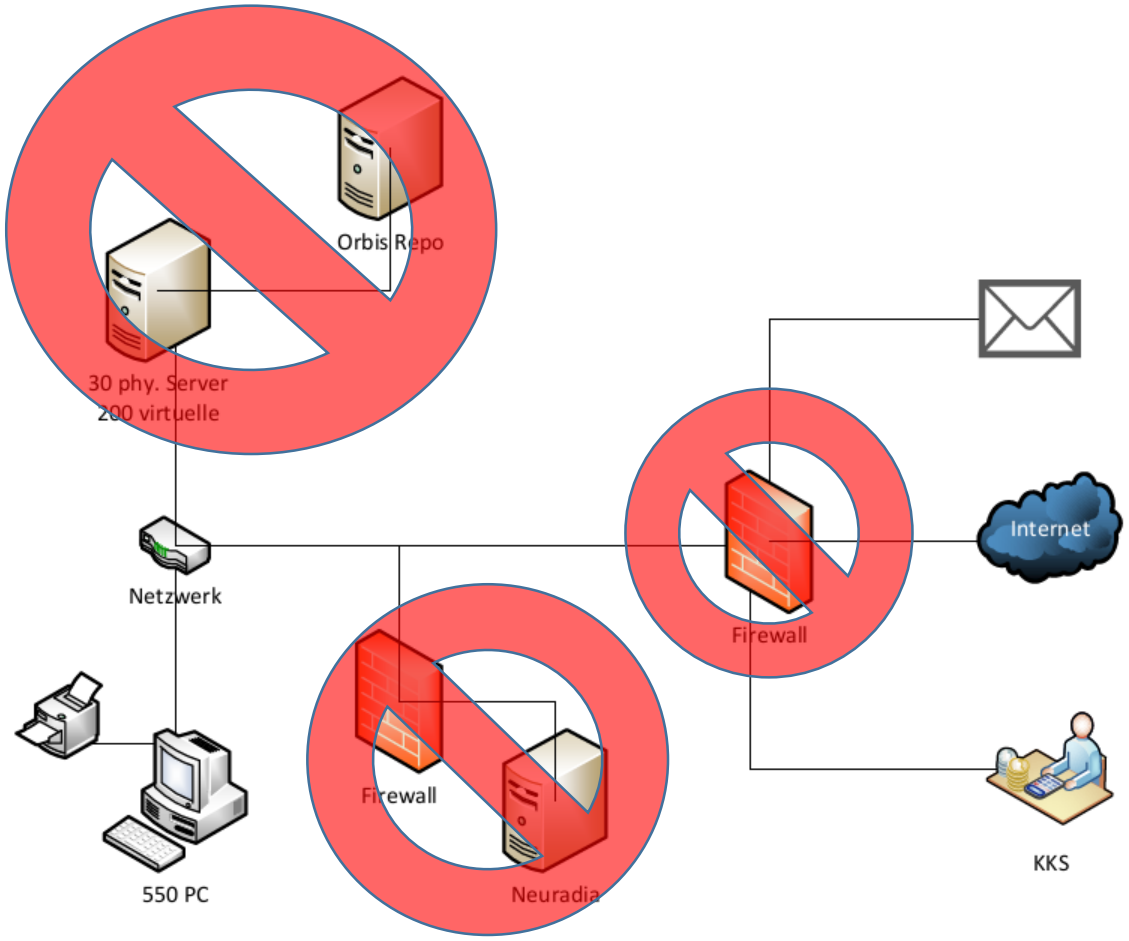
Chronologischer Ablauf

Städtisches Klinikum Wolfenbüttel



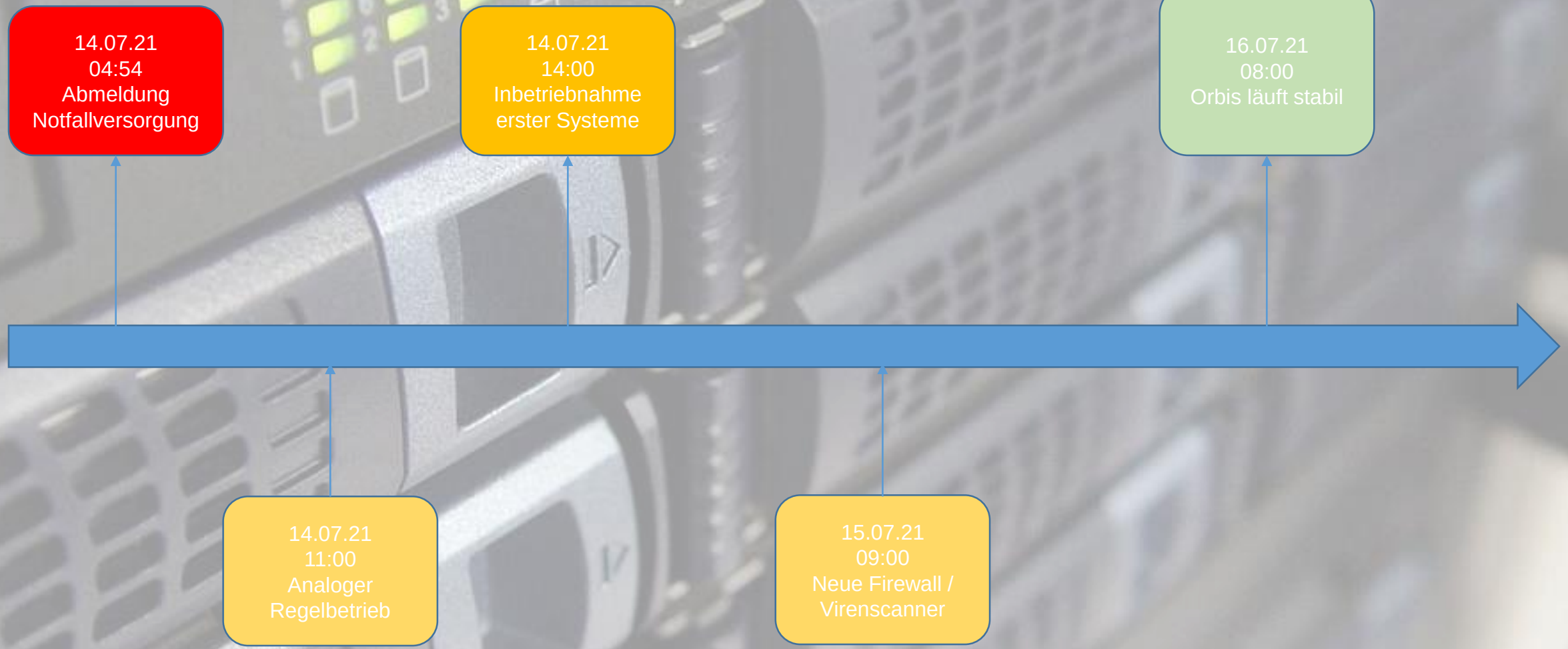
Überblick

Städtisches Klinikum
Wolfenbüttel



Zusammenfassung

Städtisches Klinikum Wolfenbüttel



Ablauf des Angriffes

Städtisches Klinikum Wolfenbüttel

13.07.21 22:38

- Unbekannte Täter verschaffen sich über einen gehackten Mitarbeiteraccount Zutritt auf die Citrixfarm des Klinikums

13.07.21 23:05

- Der/Die Täter installieren eine Schadsoftware zur Ausspähung weiterer Accounts

13.07.21 23:36

- Durch einen Adminaccount wird die Ransomware auf einem Backupserver gestartet.

14.07.21 00:11

- Information durch diensthabenden Arzt der Intensivstation

Gewinne / Verluste

Städtisches Klinikum Wolfenbüttel

Verluste

- 1 x komplett verschlüsseltes Backup
- 2 Tage ohne elektronische Dokumentation
- Kosten ca. 213 T€ (Dienstleistungen (276Std.), Lizenzen, Response Team)

Gewinne

- Krisenmanagement funktioniert
- TEAM Klinikum Wolfenbüttel

Fazit und Maßnahmen

Städtisches Klinikum Wolfenbüttel

- Frühzeitige Erkennung durch 24/7 Betrieb <-> IT-Rufdienst
- Führungs- und Stabsteam hat funktioniert (GF/VD/PD/Stabstellen/Krisenstab)
- Kurze Wege / Entscheidungen
- Gute Lieferantenbeziehungen
- Wichtigste Maßnahmen:
  - Abschluss Zwei-Faktor-Authentifizierung
  - Demilitarisierte Zone

Städtisches Klinikum
Wolfenbüttel

Haben Sie Fragen???

Vielen Dank für Ihre Aufmerksamkeit!