Witten
Universitätsstadt an der Ruhr
Amt für Datenverarbeitung

Cyberattacke auf die Stadt Witten

9. Kommunaler IT-Sicherheitskongress 2023

Deutscher Städtetag – Die Stimme der Städte

DEUTSCHER LANDKREISTAG

DStGB – Deutscher Städte- und Gemeindebund

IT-Planungsrat – Digitale Zukunft gestalten

24.04.2023

Witten

- Witten ist eine große kreisangehörige Stadt mit 96.000 Einwohnern
- Witten liegt im südlichen Ruhrgebiet / NRW
- Witten hat immer noch einen industriellen Kern in der örtlichen Wirtschaft.
- Die Verwaltung hat ca. 1.500 Mitarbeitende, über 1000 IT Arbeitsplätze.
- Es gibt 27 Schulen
- Witten ist regelmäßig in der Haushaltssicherung

IT bei der Stadt Witten

- Die IT wird weitgehend eigenständig betrieben.
- Die IT ist als Amt für Datenverarbeitung und Kommunikationstechnik organisatorisch aufgestellt

- Die meisten Fachanwendungen werden selbst gehostet.
  Nur wenige extern.
- Digitalisierung der Verwaltungsarbeit
  ist gut ausgebaut.

Kompetenzzentrum
eBehördenakte EN

- Die eAkte ist an über 90% der Arbeitsplätze eingeführt.
- Kompetenzzentrum eBehördenakte betreut alle Gemeinden des Kreises und in Kürze den Kreis (tlw.)

Der 17.10.2021

- Anruf Feuerwehr beim IT Leiter. Kein Netz, kein Telefon ca. 8.30
- Erst Analyse – Die Platz im SAN (Speichernetzwerk ist erschöpft)
- Einschaltung des Abt.Ltr. Technik
- Gegen Mittag war klar:
  Sämtliche Festplatten der Virtualisierungsumgebung sind verschlüsselt.
- Eine sog. „Ransomnote“ liegt auf jeder virtuellen Platte
- Kontaktaufnahme wird angeboten

Der Sonntag – 17.10.2021

- Vorgehen nach Notfallhandbuch
- Info Dezernent
- Information an den LKA Lagedienst 12:20
- Absprache mit Dezernet und BM
  Einberufung SAE erfolgt ca. 13 Uhr
  Tagung **SAE** -> 15:00 -> 24:00 Uhr
  Besetzung fachbezogen:
  BM, Dezernent, IT, Orga/Personal, Feuerwehr, Ref. Kommunikation
- Einschaltung eine IT Sicherheitsunternehmens
- Auflauf Polizei – Begutachtung des Schadens – Feststellung
  Feuerwehr und Müll laufen. Rest keine kritische Infrastruktur
- Am ersten Tag konnten wir nicht viel unternehmen

Schadensbild – Teil 1

- Komplette Virtualisierung verschlüsselt.
  Virtualisierungsgrad > 95% = Totalausfall der IT inkl. Telefonie

- Für Verwaltung, Feuerwehr, Kulturforum, VHS, Schulen

- Am Montag klar, dass auch die Datensicherung angegriffen wurde.
  Alle Sicherungen auf Festplatten wurden gelöscht.

- **Am Ende besteht die IT der Stadt Witten nur noch aus einer Handvoll Sicherungsbändern !!**

Schadensbild – Teil 2

- Zunächst kein Zugriff auf die Hardware wegen Ermittlungstätigkeit
- Da auch der Sicherungsserver zerstört (gelöscht) war, musste er zuerst wieder aufgebaut werden. **Erst am Donnerstag steht fest, dass die Bänder von der Wochenendsicherung nicht gelöscht waren und auch nicht infiziert.**
- Zu dem Zeitpunkt haben wir noch gedacht nach ein paar Wochen ist das Problem Geschichte. Tatsächlich haben wir bis heute einzelne Baustellen noch nicht abgeschlossen.

Wie es weiterging

- Sonntag ist klar, mindestens 2-3 Wochen keine IT

- Im ersten SAE wurde beschlossen möglichst schnell und umfassend zu informieren.

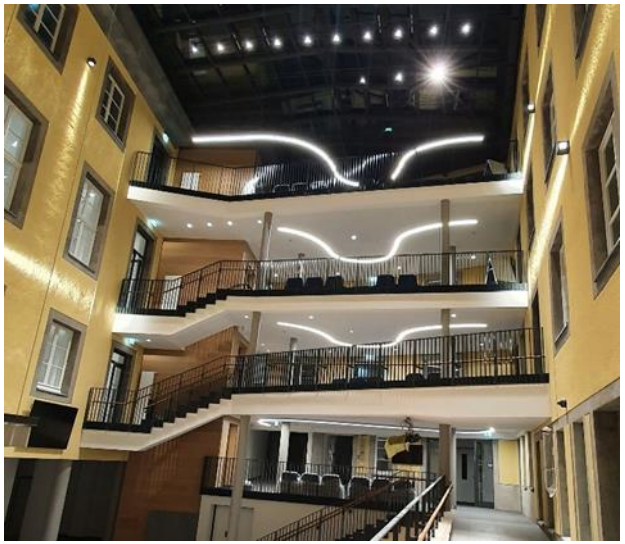
- Die Amtsleitungen wurden unmittelbar am Sonntag Nachmittag informiert. Die Feuerwehr hat eine Kontaktliste mit Rufnummern.

- Montag direkt eine Amtsleiterrunde
  Sachstand + Austausch privater eMail Adressen
  Aufforderung an die Ämter zu prüfen, wie analog weiter gearbeitet werden kann.

Installieren einer Arbeitsmethode

- Tägliche Statusgespräche im SAE – am späten Vormittag
  Wichtige Themen:
  - Priorisierung was zuerst wieder in Betrieb genommen wird
  - Was soll kommuniziert werden
- Referat Kommunikation übernimmt die Kommunikation auf allen Kanälen – Presse, Rundfunk, Internetseite, Facebook, Twitter, Instagram.
- Erste „Pressekonferenz“ noch am Montag. Dienstag erster großer Bericht in der Lokalpresse
- Alle zwei Tage Abstimmung mit den Amtsleitungen.
- Täglicher Kontakt mit der ermittelnden Polizeibehörde in Bochum
- Viele Medienanfragen

Was macht die IT ?



- IT arbeitet 7 Tage die Woche – im ersten Monat
- Tägliche Statussitzungen -> Transport in den SAE
- Kerninfrastruktur ist nach 14 Tagen wieder da. Nach drei Wochen können User in nennenswerter Zahl wieder zugreifen. Wichtige Anwendungen laufen wieder
- Einbindung externer Dienstleister für technischen Wiederaufbau
- Extern gehostete Anwendungen können wieder genutzt werden
- Zahlbarmachung wichtiger Systems konnte gewährleistet werden (Grundsicherung, Unterhaltsvorschuss, Lohn+Gehalt)

Was machen die Ämter ?

- Die Ämtern betreiben „Business Continuity Management“ (BCM) – ohne es zu wissen
- Ämter kümmern sich um alternative Lösungen
  Teilweise sehr kreativ – von Quittungsblocks, über handgestrickte Kopfbogenvorlagen bis hin zu privaten Laptops im WLAN
- Viele Teile der Verwaltung funktionieren auch weiter:
  Müllabfuhr, Feuerwehr, Kulturveranstaltung, Kitas, etc.

- Die Ämter sind aufgefordert einen Plan für eine solche oder ähnliche Katastrophe zu machen. Hat bei der Vorbereitung auf die Energiekrise sehr geholfen.
- Noch haben wir kein formales BCM

Externe Unterstützung - Fehlanzeige

- Polizei/LKA haben schon Sonntag festgestellt – kein KRITIS
- Polizei Bochum übernimmt Ermittlung
- BSI – nicht zuständig
- LDI – hat die Meldung zur Kenntnis genommen
- Keine staatliche Unterstützung !!!

Bundesamt
für Sicherheit in der
Informationstechnik

- NRW hat reagiert. KWID eingerichtet – Task Force im Aufbau
- Unterstützungsangebote benachbarter Kommunen + Kreis
- Wichtig: Unternehmen IT Sicherheit und die langjährigen Dienstleistungspartner sind umgehend da. Alle.

Kommunikation

- Aufgabenteilung ist wichtig
  Referat Kommunikation sammelt die Information und informiert intern und extern auf allen Kanälen.
- Bürgermeister und Dezernent bilden das Gesicht nach außen und übernehmen die Kommunikation mit der Politik
- IT und Orga Leiter liefern die Information, können sich aber sonst auf die Lösung der Aufgaben konzentrieren.
- Amtsleitungen werden durch regelmäßige Sitzungen und Sachstandsberichte auf dem Laufenden gehalten.

- Wichtig - laut sagen, was funktioniert: Müllabfuhr läuft, Feuerwehr funktioniert, Veranstaltungen im Kulturforum finden statt, etc.

Ransomware - Erpresser

- Es gab eine Aufforderung sich zu melden, wenn man die Daten wieder haben will - mit Kontaktdaten
- BM hat schnell entschieden, dass er nicht darauf eingehen will
- Am Donnerstag (Tag 5) Ältestenratsitzung:
  Einstimmig wird beschlossen der Erpressung nicht nachzugeben
- Gespräch dem LKA - Verhandlungsgruppe. LKA wäre durchaus bereit Verhandlungen aufzunehmen. Passiert aber nicht.
- Erpresser veröffentlichen nach vier Wochen einige wenige Daten. Es sind ausschließlich zusammengesuchte einzelne Dokumente.
- Alle Betroffenen werden darüber informiert.
- Rat stellt finanzielle Mittel bereit

Forensik und Wiederaufbau

- Durch externe Fachleute wird in den ersten 14 Tagen begleitend IT Forensik betrieben.
- Als Einfallstor wird bei uns die nicht vollständige Zweifaktorauthentifizierung festgestellt.
- Sogar der wahrscheinliche Ausgangspunkt konnte ermittelt werden.
- Für den Wiederaufbau holen wir alle Firmen an Bord, die uns auch in normalen Zeiten unterstützen. Das klappt hervorragend.

- Das IT Sicherheitsunternehmen berät uns bei der Optimierung des Wiederaufbaus. Speziell zu Netzwerkstrukturen, Härtung der Systeme und Firewalls.

Priorisierung

- Wichtige Anwendungen mussten wieder an den Start. Priorisierung war schon im NHB vorgedacht und im SAE festgelegt:

- Sozial-, Personal- und Standesamtswesen ist extern und war immer bedienbar
- Unterhaltsvorschuss
- Meldewesen
- Finanzwesen
- E-Akte
- E-Mail
- Telefon
- Arbeitsplätze bereit stellen

Status

- Nach ca. vier Wochen liefen die wichtigsten Anwendungen wieder.
- Im Januar waren die meisten Systeme und Arbeitsplätze wieder verfügbar. Ostern war halbwegs normal.
- Zwischenzeitlich gab es umfassende Umbauarbeiten an Netzwerkstrukturen und Serversystemen. I.d.R. mir der vorhandenen Hardware. Das führt zu schlechter Systemperformance, die bis zum Sommer und Einbau einer neuen Firewall bestehen bleibt.
- Nennenswerten Datenverlust gab es nicht. Allerdings haben wir einzelne Anwendungsserver „verloren“. U.a. unser Geodatenportal. Das muss aufwändig wieder hergestellt werden.
- Einzelne Applikation waren auch aus Sicherheitsgründen nicht mehr zu betrieben und mussten ersetzt werden.

Maßnahmen

- Konsequente Zweifaktorauthentifizierung – Yubikey als Smartcard mit Windows Bordmitteln (Zertifikate)
- Netzsegmentierung - Trennung der Segmente über die Firewall - Zero Trust als Ziel.
  Es wird nur benötigter Traffic zugelassen.
- Voraussetzung: Steuerbarkeit der VLAN Zugehörigkeit - Macmon als Netzwerkzugangskontrolle (NAC) eingeführt (>5000)
- AD Härtung über Gruppenrichtlinien
- Neue Datensicherung. CommVault. Übergangslösung von der Caritas. Wir schaffen gerade den dritten Ablageort für die Daten an (Air Gap).

Maßnahmen

- Cyberversicherung - Prüfung läuft noch
- Incident Response Service - wird gerade beschafft
- IT Sicherheitsbeauftragter

- Die SAE Mitglieder und Vertreter werden in Divera eingebunden. (Alarmierungssystem der Feuerwehr)
- Externe Mail für jedes Amt angelegt

DIVERA 24/7

Persönliches Fazit

- Die Cyberattacke war das einschneidende Erlebnis im Beruf
- Die Auswirkungen sind durch massive Veränderungen im Netzwerk und die Veränderung der Arbeitsabläufe unglaublich komplex.
- Die Belastung der MA in der IT, aber auch in vielen Fachbereichen ist sehr hoch. Erholungsphasen sind wichtig.
- IT hat ungefähr ein Jahr verloren. Ist nicht aufzuholen.
- Es ist mehr Arbeit und die Abläufe in der IT sind völlig verändert. Ohne Firewall Know How geht nichts mehr.
- Kommunikation nach intern ist wichtig. Auch heute noch werden Probleme im IT Alltag auf den Hackerangriff geschoben, obwohl es nichts damit zu hat

Persönliches Fazit

- Man kann sich nicht abschließend schützen
- Man kann sich aber besser vorbereiten
- „Notfallhandbücher für alle“ -> Energiekrise
- Prüfen Sie die Datensicherung - Umfang - AirGap - Wiederherstellung des kompletten Systems
- Ansprechpartner BSI / Land /etc. sollten bekannt sein

- Unterstützung übergeordneter staatlicher Ebenen

ENDE

Andreas Hasenberg

Phone: +49 172 2714382
Mail: andhas@gmail.com

Stand: 30.01.2023