ITV-SH Forum
Cyberattacke auf die Stadt Witten

Ein Erfahrungsbericht

Andreas Hasenberg

Neumünster, 03.06.2026

Vorstellung

- **Andreas Hasenberg**
  Verwaltungsdirektor a.D.
  Jahrgang 1958
- **Stadt Witten**
  Ab 1975 Ausbildung zum Stadtinspektor
  Abschluss: Dipl. Verwaltungswirt

  1981 Sachbearbeiter Bauordnung
  1988 Wechsel in die EDV
  2011-2023 Leiter des Amts für Datenverarbeitung und Kommunikationstechnik

Schwerpunktthemen:

Verwaltungsdigitalisierung
Bürgerservices
Informationssicherheit

Einfach mal einfach machen

Witten

- Witten ist eine große kreisangehörige Stadt mit ca. 96.000 Einwohnern
- Witten liegt im südlichen Ruhrgebiet / NRW im Ennepe-Ruhr-Kreis
- 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
- VHS, Kulturforum, Stadtmarketing und Stadtsportverband
- Witten ist „überschuldet“ und regelmäßig in der Haushaltssicherung

IT der Stadt Witten

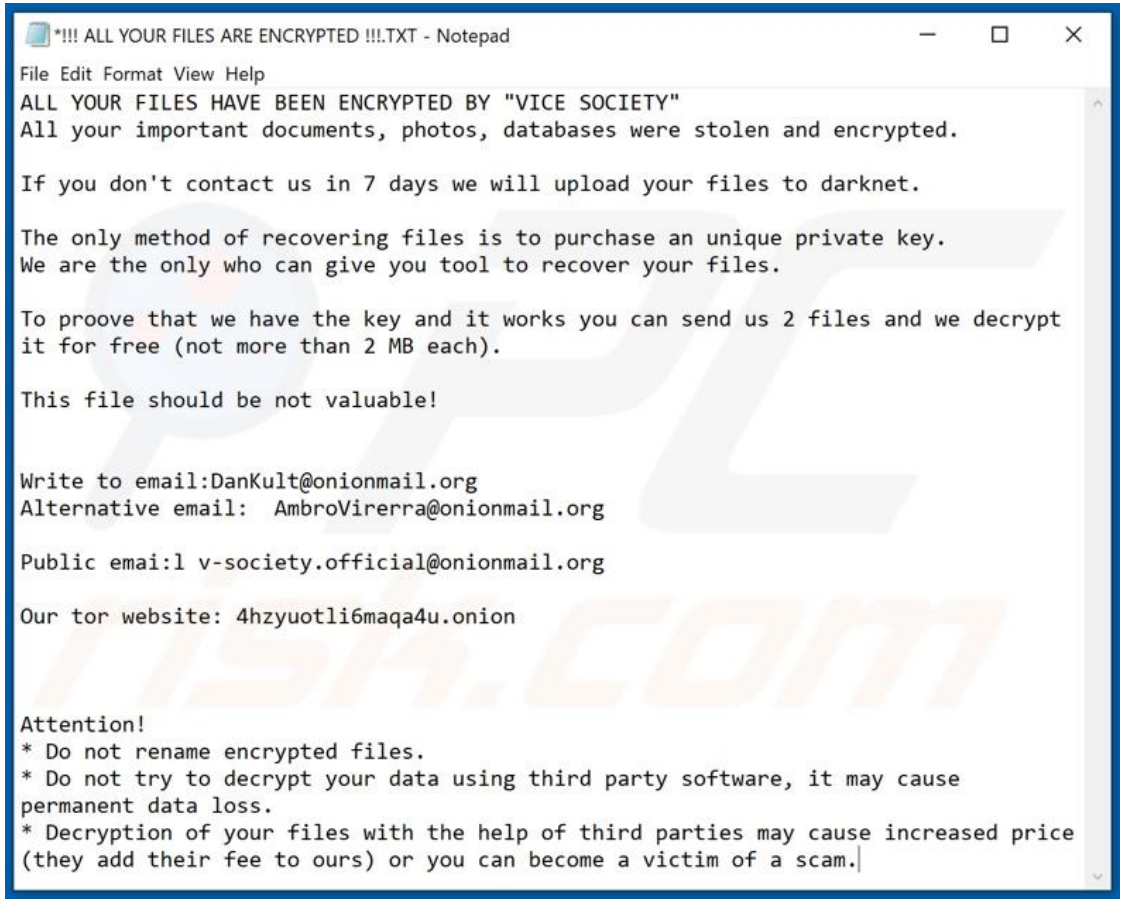
- Die IT wird weitgehend eigenständig betrieben.
- Die IT ist als Amt für Informationstechnik organisatorisch aufgestellt
- Personell mit ca. 50 MA ganz gut besetzt

- Die meisten Fachanwendungen werden selbst gehostet.
- Digitalisierung der Verwaltungsarbeit ist gut ausgebaut.
- Die eAkte ist in über 95% der Arbeitsbereiche eingeführt !
- Kompetenzzentrum eBehördenakte betreut fast alle Gemeinden des Kreises und den Kreis (tlw.)
- Aktuell entsteht ein Kompetenzzentrum Finanzwesen

Der 17.10.2021 - Sonntag

- Anruf Feuerwehr beim IT Leiter.
  Kein Netz, kein Telefon ca. 8.30 Uhr
- Erste Analyse – Kein Platz im SAN
  (zentrales Speichernetzwerk ist erschöpft)
- Einschaltung des Abt.Ltr. Technik
- Gegen Mittag war klar:
  Sämtliche Festplatten der
  Virtualisierungsumgebung sind verschlüsselt.

- Eine sogenannte „Ransomnote“ liegt auf jeder virtuellen Platte des SAN
- Kontaktaufnahme wird angeboten
  Es gibt Links zu Webseiten und Mailadressen



Der Sonntag – hektische Betriebssamkeit

- Vorgehen nach Notfallhandbuch
- Info Dezernent
- Information an den LKA Lagedienst 12:20
- Absprache mit Dezernent und BM
  Einberufung SAE erfolgt ca. 13 Uhr (Stab außergewöhnliche Ereignisse)
  Tagung **SAE** -> 15:00 -> 24:00 Uhr
  Besetzung fachbezogen:
  BM, Dezernent, IT, Orga/Personal, Feuerwehr, Ref. Kommunikation
- Einschaltung eines 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, Schule
- Am Montag wird klar, dass auch die Datensicherung angegriffen wurde.
  Alle Sicherungen auf Festplatten wurden gelöscht.

- **Die Verwaltung ist nicht mehr arbeitsfähig !!!**

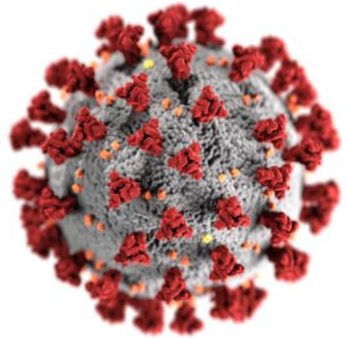
Am Ende besteht die IT der Stadt Witten nur noch aus einer Handvoll Sicherungsbändern !!

Schadensbild – Teil 2

- Zunächst kein Zugriff auf die Hardware wegen Ermittlungstätigkeit
- Der Sicherungsserver ist auch zerstört (gelöscht). Er musste zuerst wieder aufgebaut werden. **Erst am Donnerstag steht fest, dass die Bänder von der Wochenendsicherung nicht gelöscht waren und auch nicht kompromitiert.**
- Zu dem Zeitpunkt haben wir noch gedacht nach ein paar Wochen ist das Problem Geschichte. Tatsächlich gab es sehr lange Folgewirkungen, die teilweise bis heute nachwirken.

Wie es weiterging

- Schon Sonntag ist klar, mindestens 2-3 Wochen keine IT
  Keine IT bedeutet auch, keine Verwaltungstätigkeit !!!
  Kein Ausweis, keine Termine, keine Bescheide, etc.

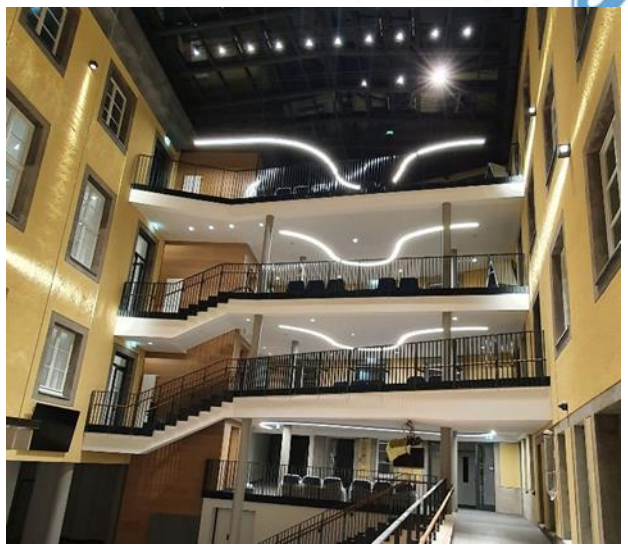


- Im ersten SAE wurde beschlossen möglichst schnell
  und umfassend zu informieren.
- Die Amtsleitungen wurden unmittelbar am Sonntagnachmittag informiert.
  Die Feuerwehr hat eine Kontaktliste mit Rufnummern.
- Montag wird direkt eine Amtsleiterrunde vor Ort einberufen
  Sachstand + Austausch privater 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 – WAZ (Funke Medien Gruppe)
- Alle zwei Tage Abstimmung mit den Amtsleitungen. Virtuell.
- 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 Systeme konnte gewährleistet werden
  (Grundsicherung, Unterhaltsvorschuss, Lohn+Gehalt)

- Fortsetzung folgt

Was machen die Ämter

- Die Ämter 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, Kulturveranstaltungen, Kitas, etc.

- Die Ämter wurden aufgefordert einen Plan für eine solche oder ähnliche Katastrophe zu machen.
  Das hat bei der Vorbereitung auf die Energiekrise Herbst 2022 sehr geholfen.
- Ein formalisiertes BCM gibt es bis heute nicht.

Externe Unterstützung - Fehlanzeige

- Polizei/LKA haben schon Sonntag festgestellt – kein KRITIS
- Polizei Bochum übernimmt Ermittlung
- BSI – nicht zuständig
- LDI – Meldung fristgemäß gemacht
- Keine staatliche Unterstützung

- NRW hat reagiert. Verschiedene Infoangebote und seit 2025 -> Digi-SOS = Soforthilfe
- 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) Ältestenratssitzung:
  Einstimmig wird beschlossen der Erpressung nicht nachzugeben
- Gespräch mit 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.
- Letzteres dauert viele Monate !!!

Priorisierung

- Wichtige Anwendungen mussten wieder an den Start. Priorisierung war schon im Notfallhandbuch vorgedacht.
  - Es gibt technische Zwänge. Basistechnik muss funktionieren. Server, Netzwerke, Benutzerverwaltung
  - Im SAE wird beraten, welche System Priorität haben
  - Ganz vorne natürlich Systeme, die existenzsichernd sind
- Sozial-, Personal- und Standesamtswesen ist extern und war immer bedienbar
- Unterhaltsvorschuss
- Meldewesen
- Finanzwesen
- E-Akte
- E-Mail + Telefon
- Arbeitsplätze bereit stellen
- Ratsinformationssystem !

Was macht die IT - Fortsetzung

- Wichtige Entscheidungen fallen:

- Alle PCs werden neu installiert (Freitag)
- Alle Kennwörter werden zurück gesetzt – inkl. „Golden Ticket“
- Die Datensicherung hat funktioniert. Die Wiederherstellung ist aber unglaublich langsam und bei spezifischen Systemen nur mit dem Support aus Indien lösbar.
- Die Hardware kann vollständig weiter genutzt werden.

- Alle Server und PC aus den Schulen werden geprüft und neu installiert.

Status nach einem Dreivierteljahr

- Nach ca. vier Wochen liefen die wichtigsten Anwendungen wieder.
- Im Januar waren die meisten Systeme und Arbeitsplätze wieder verfügbar.
- **Ostern war es halbwegs normal. Zu diesem Zeitpunkt haben wir intern den Katastrophenmodus beendet. Ich habe dazu einen langen Artikel im Intranet verfasst.**
- 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 blieb.
- 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 betreiben und mussten ersetzt werden.

Wichtige Maßnahmen

- Konsequente Zweifaktorauthentifizierung ✓
  Yubikey (Fido2) als Smartcard mit Windows Bordmitteln (Zertifikate)
- Neues Datensicherungssystem ✓
- Incident Response Service ✓
- Cyberversicherung – Nein ☠
- Die SAE Mitglieder und Vertreter werden in Divera eingebunden. (Alarmierungssystem der (freiwilligen) Feuerwehr)

Begleiteffekt:

- Fax abgeschafft ☺ Die Stadt Witten ist seit 2021 per Fax nicht mehr erreichbar

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.
- Es ist mehr Arbeit und die Abläufe in der IT sind völlig verändert.
  Ohne Firewall Know How geht nichts mehr.
- 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.
- Kommunikation nach intern ist wichtig. Auch mehr als ein Jahr danach wurden Probleme im IT Alltag auf den Hackerangriff geschoben, obwohl es nichts damit zu hat.
- Man kann sich nicht abschließend schützen

ENDE

Andreas Hasenberg

Verwaltungsdirektor a.D
Leiter Amt für Datenverarbeitung Stadt Witten
bis Juli 31.07.2023

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

Stand: 03.06.2026