Erfahrungsbericht

Wir wurden gehackt, was nun?

[05.10.2023] Andreas Hasenberg war bis vor Kurzem Leiter des Amts für Datenverarbeitung der Stadt Witten. Im Oktober 2021 wurde die Kommune Opfer einer Cyber-Attacke. Wie er diesen Vorfall erlebt hat, schildert Hasenberg in einem persönlichen Erfahrungsbericht.

Bei der Verwaltungsdigitalisierung ist die nordrhein-westfälische Stadt Witten im Ennepe-Ruhr-Kreis gut aufgestellt. Sichtbar wird das beim Thema E-Akte: Hier kann die Wittener Verwaltung vorne mitspielen. Die IT wird weitgehend selbstständig betrieben. Als am Sonntag, den 17. Oktober 2021 gegen 8:30 Uhr die Feuerwehr bei mir als Wittener IT-Leiter anrief, war gleich klar, dass dies nichts Gutes bedeuten kann. Die Feuerwehr berichtete mir, dass sie Probleme mit ihren Daten habe und auch das Telefonieren nicht wirklich gut funktioniere. Zu diesem Zeitpunkt konnte ich mich noch auf unsere städtischen Systeme aufschalten und nach dem Fehler suchen. Auf den ersten Blick war zu sehen, dass unser zentrales Speichersystem (SAN) voll und dort kein Platz für weitere Daten war. Gemeinsam mit dem Abteilungsleiter Technik versuchte ich herauszufinden, was den kompletten Speicher verbraucht haben könnte.
Schnell fanden sich dann auf dem SAN neben jeder virtuellen Festplatte so genannte Ransom Notes. In diesen wurde uns mitgeteilt, dass unsere Daten verschlüsselt worden waren. Es folgte eine E-Mail-Adresse, an die wir uns wenden sollten, wenn wir unsere Daten wiederhaben wollen. In einem solchen Augenblick ist das Leben als IT-Leiter nicht mehr schön.

Notfallhandbuch war vorhanden

Für die Stadt Witten existiert ein Notfallhandbuch, das verschiedene Szenarien beschreibt. In diesem wurde zwar nicht unser konkreter Störfall geschildert, aber zumindest war dort aufgelistet, wer zu informieren und wie generell vorzugehen ist. Diesem Ablauf folgend habe ich also zunächst den zuständigen Dezernenten angerufen, dieser wiederum hat den Bürgermeister informiert, der dann den „Stab für außergewöhnliche Ereignisse – SAE“ einberufen hat. Diesem Krisenstab der Stadt Witten gehören neben dem Bürgermeister der zuständige Dezernent, die Organisations- und Personalchefin, die Pressestelle, die IT und die Feuerwehr an, welche die Organisation des SAE übernommen hat.
Parallel wurde der LKA-Lagedienst von mir über den Vorfall informiert. In der Folge erschienen im Laufe des Tages verschiedenste Polizeidienststellen in Witten. Zusätzlich habe ich Kontakt zu einem IT-Sicherheitsunternehmen aufgenommen, da mir schon zu diesem Zeitpunkt klar war, dass die Stadt bei der Ursachenanalyse sowie der Wiederherstellung ihrer Systeme Unterstützung benötigen würde.
Die polizeilichen Maßnahmen beschränkten sich im Wesentlichen auf die Sicherstellung von Beweismaterial. Am Sonntagabend war dies weitgehend abgeschlossen – und endete mit der Feststellung, dass unser Fall nicht die Kritische Infrastruktur (KRITIS) beträfe. Die polizeilichen Maßnahmen wurden daher an die zuständige lokale Dienststelle abgegeben. Durch die Feststellung, dass wir nicht als KRITIS einzustufen sind, war dann auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) nicht für uns zuständig. Tatsächlich waren am Ende die einzig Zuständigen wir selbst – es gab keinerlei externe behördliche Unterstützung.

Umfassendes Schadenbild

Das Schadenbild war absolut umfassend. Denn die IT der Stadt Witten ist nahezu vollständig virtualisiert. Alle Daten liegen auf dem SAN. Die Cyber-Attacke hatte also zur Folge, dass sämtliche Daten und Systeme verschlüsselt und nicht mehr funktionsfähig waren. Auch die Datensicherung wurde angegriffen – es waren nur noch die Daten auf den Magnetbändern vorhanden. Die Stadt Witten hatte somit von einem Tag auf den anderen keine IT-Systeme mehr. Wie soll eine Verwaltung in einem solchen Fall reagieren? Eine erste wichtige Frage lautete, wie wir den Angriff kommunizieren wollen. Noch am Sonntag fiel die Entscheidung, mit der Situation offen umzugehen. Die Öffentlichkeit wurde daher über unsere Website – die extern gehostet ist – sowie die städtischen Social-Media-Kanäle darüber informiert, dass das Rathaus am Montag geschlossen bleiben muss.
Für Montagmorgen war dann eine Amtsleiterrunde einberufen, wo den Kolleginnen und Kollegen die Situation erklärt wurde. Sie wurden gebeten, alle Maßnahmen – gerne auch unkonventionelle – zu ergreifen, damit der Dienstbetrieb irgendwie weitergehen kann. Denn es war zu diesem Zeitpunkt bereits klar, dass es einige Tage, wenn nicht gar Wochen dauern würde, bis in Witten wieder alles funktioniert. Wichtig für den weiteren Ablauf war es dann, eine verlässliche Arbeitsmethode zu installieren, die auch der sehr dynamischen Lage gerecht wurde. Der SAE hat täglich, meist am späten Vormittag, getagt. Zu den wichtigsten Themen zählten dabei stets die folgenden Fragen: Wie ist der aktuelle Stand bei der Technik? Was muss priorisiert werden? Was können wir kommunizieren?

Kommunikation ist äußert wichtig

In der Rückschau lässt sich konstatieren, dass das Thema Kommunikation – und eine sinnvolle Arbeitsteilung dabei – im Fall eines Cyber-Angriffs äußerst wichtig ist. In Witten etwa war das Referat Kommunikation dafür zuständig, alle verfügbaren Informationen zu sammeln und auf allen Kanälen – intern und extern – zu verbreiten. Der Bürgermeister und der Dezernent bildeten das Gesicht nach außen, nahmen die Termine mit Presse, Funk und Fernsehen wahr und kommunizierten mit den politischen Gremien. Die Organisations- und Personalchefin und ich als IT-Leiter lieferten natürlich alle notwendigen Informationen, konnten uns ansonsten aber darauf konzentrieren, die IT wieder zum Laufen zu bekommen.
Die Wittener IT-Abteilung war im Zuge der Aufarbeitung des Cyber-Angriffs stark gefordert. Die komplette Infrastruktur musste neu aufgebaut werden – das war nur durch den hohen persönlichen Einsatz aller Beteiligten möglich. Mehr als zwei Wochen dauerte es, bis erste Dinge wie E-Mails, E-Akte und Telefon wieder funktionierten – und ungefähr einen Monat, bis wieder wichtige Dienstleistungen in nennenswerter Zahl verfügbar waren. Die Ämter fanden teilweise zwar kreative Lösungen, um ihre Aufgaben zumindest teilweise erledigen zu können, viele Dienste konnten in Witten jedoch lange Zeit nicht oder nur eingeschränkt erbracht werden. Immer gewährleistet war hingegen die Zahlbarmachung wichtiger Leistungen; teilweise wurden Zahlungen aus dem Vormonat schlicht wiederholt. Wichtig war der Stadt, die Menschen nicht ohne finanzielle Mittel dastehen zu lassen.

Wiederaufbau der IT-Systeme hat rund ein Jahr gedauert

Auf die Forderungen der Erpresser ist Witten übrigens nicht eingegangen. Der Bürgermeister hatte dazu eine klare Haltung, die vom Rat einstimmig mitgetragen wurde. Als klar war, dass es zwar dauern würde, die städtischen Daten aber auf jeden Fall aus eigener Kraft wiederhergestellt werden könnten, wurde erst gar kein Kontakt mit den Erpressern aufgenommen. Als Einfallstor für die erfolgte Cyber-Attacke machte die Stadt bei der Ursachenrecherche aus, dass im Zuge der Ausweitung der mobilen Arbeit aufgrund der Corona-Pandemie nicht konsequent auf eine Zwei-/Multi-Faktor-Authentifizierung (MFA) geachtet worden war. Jeder Verwaltung ist daher dringend zu empfehlen, keinerlei Remote-Zugriff ohne MFA zuzulassen. Ohne jede Ausnahme.

Der Wiederaufbau ihrer IT-Systeme hat die Stadt Witten insgesamt rund ein Jahr gekostet. Das war allerdings der Tatsache geschuldet, dass die Systeme und Netze dabei auch gleich auf den aktuellen Stand der Sicherheitstechnik gebracht wurden, was bei einem Kernsystem mit circa 1.000 Arbeitsplätzen, vielen Standorten und 27 Schulen naturgemäß sehr zeitaufwendig ist.

()

Dieser Beitrag ist in der Ausgabe Oktober 2023 von Kommune21 im Schwerpunkt IT-Sicherheit erschienen. Hier können Sie ein Exemplar bestellen oder die Zeitschrift abonnieren.

Stichwörter: IT-Sicherheit, Witten, Cyber-Security, Cyber-Angriff