Trojaner-Angriff auf die Verwaltung von Neustadt am Rübenberge

Abschalten – Sofort!

Es gibt Tage, die bleiben allen MitarbeiterInnen einer Kommunalverwaltung im Gedächtnis. Die Wahl eines neuen Bürgermeisters etwa, oder aber ein krimineller Angriff. In Neustadt am Rübenberge in der Region Hannover kam dieser lautlos über das Internet.

> Maic Schillack und Kathrin Kühling

Am Morgen des 6. September 2019 bemerkte die IT-Abteilung ungewöhnlich hohe Serveraktivitäten. Als kurz vor sieben Uhr beim Ersten Stadtrat und anderen Verantwortlichen die Telefone klingeln, war es schon zu spät. Unbekannte hatten bereits begonnen, die Server der Kommunalverwaltung anzugreifen. Ein eingeschleuster Krypto-Trojaner verschlüsselte rund eine halbe Millionen Datensätze – E-Mails, Formulare, Bauzeichnungen, Terminkalender, Elterngeldanträge – kaum ein Datensatz war noch brauchbar.

Foto: Tastenlöwe / Wikimedia (CC BY-SA 4.0)

Schnelles Handeln war gefragt

Nach einem ersten Krisengespräch mit der IT-Abteilung war allen Anwesenden klar, dass die Verwaltung Opfer eines systematischen Hackerangriffs von bedrohlichem Ausmaß geworden war. Um den Schaden einzudämmen, blieb nur eine Option: Alles muss vom Netz. Doch zunächst galt es, noch ein wichtiges Detail zu klären – welche Auswirkungen hat ein solch virtueller Shutdown auf das öffentliche Leben? Es folgte schnell eine kleine Erleichterung. Die kritische Infrastruktur, wie Verkehr, elektronische Schließanlagen an öffentlichen Gebäuden oder die Funktion der Kläranlagen wären nicht betroffen, also: Abschalten – sofort!

Die Verwaltung setzte sich umgehend mit weiteren Behörden in Verbindung, wie dem Landesdatenschutzbeauftragten, dem Landeskriminalamt (LKA) oder dem Bundesamt für Sicherheit in der Informationstechnik (BSI). Wir haben uns von Beginn an für eine offene Kommunikation entschieden und uns unmittelbar Hilfe ins Haus geholt. Denn uns war klar, dass wir die Unterstützung von Fachleuten benötigen, um den Schaden so gering wie möglich zu halten.

Ein Trojaner – mit Zeitzünder

Die Ermittlungsbehörden von Polizei und Landeskriminalamt kamen noch am Vormittag ins Haus, und schnell wurde deutlich, dass wir mit dem Trojaner Emotet angegriffen wurden. Dieser Virentyp gilt als gefährlichstes Schadprogrammen, das aktuell im Umlauf ist. Das Tückische an ihm: Virenscanner können das Eindringen ins System bemerken und schlagen in der Regel auch Alarm. Doch nach einem ausführlichen Scan und einer ersten Reinigung der Server ist augenscheinlich keine Schad-

WOCHEN SCHAU VERLAG

Anke Knopp

Das neue digitale Landleben

Smart und innovativ
statt abgehängt und analog

Deutschland ist ländlich geprägt. Mehr als die Hälfte der Einwohner leben im ländlichen Raum. Viele aber zieht es in die Städte. Was hilft gegen die Landflucht? Digitale Strategien können ländliche Räume vitalisieren.

Die Autorin begibt sich auf einen Landspaziergang durch zukünftige digitale Welten: Glasfaser, Offene Daten und Sensoren im Internet der Dinge tauchen ebenso auf wie smarte Mobilität und Roboter in der Gesundheitsvorsorge.

Das Buch ist eine Einladung, den eigenen Platz in der digitalen Welt zu finden im Sinne von Eigenheit, Freiheit und Gemeinwohlorientierung. Denn ohne digitales Land ist auch kein Staat zu machen.

ISBN 978-3-7344-0732-1, 184 S., € 14,90
E-Book: ISBN 978-3-7344-0733-8 (PDF), € 11,99

www.wochenschau-verlag.de

www.facebook.com/wochenschau.verlag

www.twitter.com/Wochenschau_Ver

software im System auffindbar. So erfasst Emotet weitestgehend unbemerkt das gesamte System, bis von außen der Befehl zum Angriff kommt. Dann beginnt die systematische Verschlüsselung der befallenen Dateien und Systemverzeichnisse – so auch in Neustadt am Rübenberge.

Nach einer Telefonkonferenz mit weiteren Sicherheitsbehörden entschieden sich die Verantwortlichen für das vollständige Neuaufsetzen aller Server und Systeme. Nach den Erfahrungen anderer Emotet-Opfer war dies der einzige Weg sicherzustellen, dass der Virus nicht unbemerkt weitere Daten verschlüsselt oder sich irgendwo versteckt, um zu einem späteren Zeitpunkt erneut zuzuschlagen.

Der Arbeitsalltag verändert sich schlagartig

Allen Beteiligten wurde allmählich bewusst, wie tiefgreifend dieser Angriff für uns ist. Der komplette Arbeitsalltag der meisten MitarbeiterInnen veränderte sich schlagartig. Rund 300 Rechner blieben für die nächsten Tage schwarz.

Allein die städtische Homepage, welche extern gehostet wird, stand der Verwaltung als Kommunikationsmedium noch zur Verfügung. Der eingerichtete Krisenstab der Verwaltung entschied sich schnell für eine weitreichende Kommunikation nach außen. Über die Internetseite der Stadt und ein spontan eingerichtetes E-Mail-Konto sowie die angeschlossenen Rechenzentren wurden die BürgerInnen, weitere Behörden und Projektpartner über den Hackerangriff informiert.

Für die Beschäftigten der Verwaltung musste nun eine neue Arbeitsstruktur geschaffen werden. Die PC-Arbeitsplätze in den Büros standen nicht zur Verfügung, Fachanwendungen und auch die Internetleitungen waren abgeschaltet. Mithilfe von Notebooks und Handy-Hot-Spots wurden punktuelle internetfähige Arbeitsplätze innerhalb der Verwaltung geschaffen sowie Arbeitsplätze ins kommunale Rechenzentrum ausgelagert. Homeoffice-Arbeitsplätze waren tabu, da eine Infizierung der Rechner nicht ausgeschlossen werden konnte.

Zurück zum Papier

Alle sich im Umlauf befindlichen Datenträger – USB-Sticks, externe Festplatten et cetera – mussten eingesammelt und in verschlossenen Umschlägen an die IT übergeben werden. Die Organisation der Gremiensitzungen und das Verschicken der Ratspost etwa waren ab sofort nur noch in Papierform möglich. Sämtliche Termine, unter anderem die Trautermine des Standesamtes, waren verloren. Und auch alle digital gespeicherten Kontaktdaten, etwa Adressbücher aus E-Mail-Programmen, standen für die Arbeit der Verwaltung nicht mehr zur Verfügung.

300 Rechner werden von Hand neu aufgesetzt

Parallel begannen die KollegInnen der IT-Abteilung die insgesamt 76 Fachanwendungen zu priorisieren und einen Ablaufplan für das Neuaufsetzen des gesamten EDV-Systems zu erarbeiten. Daraus entstand ein Maßnahmenkatalog, der in den folgenden Tagen akribisch abgearbeitet wurde.

Alle 300 Arbeitsplatzrechner mussten von Hand neu eingerichtet und nach und nach wieder freigegeben werden. Die komplette digitale Infrastruktur des Hauses wurde gemeinsam mit externer Verstärkung neu aufgebaut. Rund 30 TechnikerInnen waren quasi rund um die Uhr im Einsatz, um die Verwaltung wieder ans Netz zu bringen.

Arbeitsergebnisse von Jahren sind verloren gegangen

Das restliche Kollegium versuchte in dieser Zeit die verlorenen Daten anhand analoger Kopien, Akteneinträgen, anderer Behörden und externer Projektpartner zumindest in Teilen wiederzubeschaffen. Viele unserer KollegInnen haben innerhalb weniger Stunden ihre Arbeitsergebnisse der letzten Jahre verloren. Ein regelrechter Schock – man fühlt sich plötzlich ohnmächtig und verwundbar. Der Verwaltungsvorstand hol-

Foto: Michael Geiger / Unsplash

te auch hier externe Hilfe ins Haus, um mithilfe von ArbeitspsychologInnen das Geschehene aufzuarbeiten.

Nach sieben Tagen gingen die ersten Rechner an, die ersten Programme konnten starten und die Fachdienste begannen – so gut es ging – ihre routinemäßigen Aufgaben wieder wahrzunehmen. Wir waren hier tatsächlich sehr schnell. Erfahrungen anderer Unternehmen und Behörden haben gezeigt, dass es mindestens eine Woche braucht, um die Systeme wieder ans Netz zu bekommen – unabhängig davon, für welchen Weg man sich entscheidet. Vor kurzem konnten auch die unverschlüsselten Alt-Daten vollständig bereinigt und wieder in das Netzwerk der Verwaltung importiert werden.

Für uns ist rückblickend klar, dass es in diesem Fall die richtige Entscheidung war, die Server und das gesamte System vom Netz zu nehmen und komplett neu aufzulegen. Auch von Beginn an offen nach außen und innen zu kommunizieren, war das Beste, was wir tun konnten. Wir haben so viel Hilfe von externen Behörden sowie Partnern bekommen und außerdem viel Verständnis von den BürgerInnen erfahren.

Niemand ist je ganz geschützt

Festzustellen ist: Niemand ist jemals zu einhundert Prozent vor solchen Angriffen geschützt. Unser Sicherheitssystem war stets aktuell und absolut zeitgemäß, doch wir haben an einigen Punkten nochmal nachgesteuert. So wurden die Regeln für E-Mail-Anhänge verschärft – alte Office-Formate werden grundsätzlich nicht mehr durchgelassen. Und auch das Netzwerk wurde stärker segmentiert, um einem potenziellen neuen Virus die Ausbreitung zu erschweren. Eine netzwerkunabhängige Sicherung auf Datenbändern wird wöchentlich aktualisiert, anschließend offline in einem Bankschließfach und in einem feuerfesten Tresor der Stadt aufbewahrt. So können wir im Notfall das System schnell und ohne größeren Datenverlust wiederherstellen.

Als betroffene Kommune oder als Unternehmen sollte man auf jeden Fall die Sicherheitsbehörden einschalten. Die ErmittlerInnen sind äußerst sensibel mit der Lage umgegangen und waren bei vielen Fragen eine große Hilfe. Für uns als Stadt war dieser Vorfall die ultimative Awareness-Schulung. Aber wir empfehlen allen Kommunen, sich auf solche Angriffe mit einem gezielten Notfallplan vorzubereiten und die Mitarbeitenden intensiv zu schulen sowie für die Gefahren aus dem Netz zu sensibilisieren. Das ist die beste Prävention, die es gibt.

> Maic Schillack ist erster Stadtrat in Neustadt am Rübenberge. Inzwischen ist er ein gefragter Experte in Sachen Emotet-Angriffe und deren Folgen. Bei diversen Vorträgen und Veranstaltungen hat er von den Erfahrungen in Neustadt am Rübenberge berichtet.

> Kathrin Kühling ist Mitarbeiterin für öffentliche Angelegenheiten im Bürgermeisterreferat in Neustadt am Rübenberge.