Best Practice

Cybersicherheit dank guter Prävention & richtiger Reaktion: Lernen Sie von Mössingen

Wie bei einem Cyberangriff die richtige Reaktion der Betroffenen und die Teamarbeit von kommunaler Verwaltung, Behörden und IT-Dienstleistern Schäden minimieren kann, hat der Sicherheitsvorfall in Mössingen im November 2023 eindrucksvoll gezeigt. Am 17. November 2023 wurde die IT-Infrastruktur der Stadt Mössingen von Cyberkriminellen angegriffen. IT-Systeme und Daten einer großen Kreisstadt mit knapp über zwanzigtausend Bürgerinnen und Bürgern – ein attraktives Ziel für Hacker. Mit Hilfe des professionellen Krisenmanagements der dortigen Verwaltung konnte Schlimmeres verhindert werden.

Schnelle und besonnene Reaktion

Dank des ebenso schnellen wie besonnenen Verhaltens der Mitarbeitenden, der IT-Leitung und des Oberbürgermeisters war die Gegenwehr der Verwaltung erfolgreich. Dies ist auf die sehr gute Präventionsarbeit in der Kommunalverwaltung zurückzuführen. „Uns war immer bewusst, dass es keine hundertprozentige Sicherheit gibt. Die Frage ist nicht ob, sondern wann ein Hackerangriff kommt. Deshalb haben wir uns auf eine Cyberattacke vorbereitet“, erklärt Michael Bulander, Oberbürgermeister von Mössingen.

Bei der Prävention gibt es drei Aspekte zu beachten. Zum einen ist es erforderlich, dass die Mitarbeitenden geschult werden. Sie sollten beispielsweise Phishing-Mails und andere Cyberangriffsformen möglichst frühzeitig erkennen können und die richtigen Meldewege kennen. Zum anderen ist die regelmäßige Fortbildung der IT-Fachkräfte hinsichtlich aktueller Angriffsmuster und -methoden zu gewährleisten. Es ist wichtig, dass auch auf technischer Ebene die Sicherheitsmechanismen in der IT ständig an die sich ändernden Angriffsszenarien angepasst werden. Es müssen ferner Notfallpläne vorliegen und regelmäßig erprobt werden, damit diese sofort greifen, wenn es zu einem IT-Sicherheitsvorfall kommt. Dabei gilt es insbesondere, Informationsketten zu bilden, also Ablaufschemata, wer in welcher Reihenfolge zu informieren ist, intern wie extern.

Mössingen hat bei den ersten Anzeichen des Angriffs alles richtiggemacht. Nach der internen Meldung, dass es eine mutmaßliche Cyberattacke gab, wurde die IT der Verwaltung unmittelbar vom Internet getrennt. Unverzüglich kam der Krisenstab der Stadtverwaltung zusammen, wie im Notfallplan vorgesehen. Das Team bestand unter anderen aus dem Oberbürgermeister, der IT-Leitung, der Datenschutzbeauftragten und den Mitarbeiterinnen der Öffentlichkeitsarbeit.

Gemäß den Ablaufplänen wurden die Cybersicherheitsagentur Baden-Württemberg (CSBW), das Landeskriminalamt Baden-Württemberg (LKA BW), das Polizeipräsidium Reutlingen (PP RT), der

Landesbeauftragte für den Datenschutz und die Informationsfreiheit (LfDI), das Cyber Security Incident Response Team (CSIRT) der kommunalen IT-Dienstleisterin Komm.ONE, der IT-Dienstleister der Stadt sowie die Mitarbeitenden informiert.

„Bei einem Cyberangriff zählt oft jede Minute, um größeren Schaden und eine Ausweitung des Angriffs zu verhindern. Daher raten wir Betroffenen immer, sich so schnell wie möglich zu melden. Im Falle von Mössingen konnte wenige Minuten nach der Meldung am Nachmittag ein Erstgespräch zwischen unserem Abteilungsleiter Detektion & Reaktion, Björn Schemberger, und Oberbürgermeister Michael Bulander geführt werden. Unmittelbar im Anschluss wurde unser mobiles Vorfallteam (MIRT) nach Mössingen entsandt, um vor Ort zu unterstützen“, so Anika Sturm, Vorfallmanagerin der Cybersicherheitsagentur Baden-Württemberg.

Akribische Forensik und abgestimmte Kommunikation

In enger Abstimmung besprachen alle internen und externen Mitwirkenden in gemeinsamen Kommunikationsrunden das weitere Vorgehen. Ergänzend fanden Abstimmungen auf technischer Ebene statt. Die CSBW übernahm die Vorfallsteuerung, das heißt, sie plante und koordinierte die notwendigen Abstimmungsrunden sowie den Informationsfluss zwischen den Beteiligten. Das Polizeipräsidium Reutlingen und die Cybersicherheitsagentur Baden-Württemberg übernahmen in Abstimmung mit dem Landeskriminalamt Baden-Württemberg die forensische Analyse. Gleichzeitig untersuchten die Expertinnen und Experten, unter Einhaltung höchster Sicherheitsstandards, die attackierten Systeme. Aus dem Anfangsverdacht wurde schnell Gewissheit: Mehrere Systeme der Verwaltung waren betroffen.

„Es vergeht kaum ein Tag, an welchem unserer Zentralen Ansprechstelle Cybercrime (ZAC) beim LKA BW nicht mindestens ein massiver Cyberangriff gemeldet wird. Waren es in der Vergangenheit hauptsächlich Wirtschaftsunternehmen, die sich in solchen Fällen an uns gewandt haben, so verzeichnen wir über die letzten Jahre immer häufiger Kontaktaufnahmen von Kommunen und Städten. Die Bandbreite der hierbei registrierten Cyberangriffe deckt das gesamte Spektrum an Cybercrime-Phänomen ab. Auf der Tagesordnung stehen: Phishingangriffe, Internetbetrugsmaschen wie Business-E-Mail-Compromise, Fake-President oder Ransomwareangriffe, um nur einige zu nennen. Diese sind mit teils erheblichen volkswirtschaftlichen Schäden verbunden“, so LKA-Präsident Andreas Stenger.

Durch das sofortige Herunterfahren der entsprechenden Netzwerk- und Internetkomponenten hatte Mössingen jedoch Schlimmeres verhindert. Aus Sicherheitsgründen setzte der IT-Dienstleister mit Beratung der Cybersicherheits-Fachleute der Behörden die gesamte IT-Infrastruktur der Mössinger Verwaltung vollständig neu auf.

„Das LKA BW, das Landesamt für Verfassungsschutz BW und die CSBW befinden sich bezüglich der Bedrohungslagen in einem permanenten Austausch. Wir stehen der Wirtschaft sowie dem öffentlichen Sektor in Baden-Württemberg mit unseren zielgruppenspezifischen Angeboten jederzeit beratend und unterstützend zur Seite“, ergänzt Stenger.

Auch die Kommunikation an die Bürgerinnen und Bürger und die Mitarbeitenden der Stadtverwaltung galt es zu koordinieren. Dies erfolgte ebenfalls in Absprache aller Beteiligten. Hier mussten die Besonderheiten berücksichtigt werden, die sich aus den kriminalpolizeilichen

Ermittlungen ergaben sowie die technischen Einschränkungen. Ziel war es, die Öffentlichkeit und die Medien jeweils über den aktuellen Stand und die Erreichbarkeit der Stadtverwaltung zu informieren. Dies gelang zeitnah und dem Informationsbedürfnis der Bürgerinnen und Bürger entsprechend. Als Kommunikationskanäle wurden die Homepage, die Social-Media-Kanäle und das Intranet der Stadt Mössingen sowie Aushänge am Rathaus und Pressemitteilungen genutzt. So konnten viele Fragen der Bürgerinnen und Bürger durch FAQ-Seiten geklärt werden.

„Der Austausch in der Kommunikationsrunde war uns vom ersten Tag des Cyberangriffs eine große Hilfe bei der Bewältigung. Wir haben immer schnelle, kompetente und hilfreiche Tipps für die interne und externe Kommunikation erhalten“, sagt Nicole Siller, Pressesprecherin der Stadt Mössingen.

„Wir haben gute Erfahrung damit gemacht, die Kommunikation nach innen und außen von Anfang an zu steuern und proaktiv zu gestalten. Wichtig ist, dass zu allen Zielgruppen korrekt, klar, konkret und konsistent kommuniziert wird. Gute Kommunikation in Krisensituationen kann das Vertrauen in die Gemeinde stärken und nimmt viel Druck aus der Situation“, ergänzt Susanne Eva Krieg, Pressesprecherin der CSBW.

Sicherer und sorgfältiger Wiederaufbau

Parallel wurde der Wiederaufbau der IT-Infrastruktur vorangetrieben. Sofortige Unterstützung nach der Alarmierung erhielt Mössingen dabei von der Komm.ONE. Die IT-Dienstleisterin setzte neue IT-Sicherheitsmaßnahmen sofort um. Ebenso stellte sie kurzfristig neue Arbeitsplatzausstattungen, wie beispielsweise Notebooks, zur Verfügung. Neben der Hardware wurde auch die Software der IT-Infrastruktur umgehend erneuert, um die Arbeitsfähigkeit der Mitarbeitenden schnellstmöglich wiederherzustellen und den Service für die Mössinger Bürgerinnen und Bürger zeitnah in vielen Bereichen wieder anbieten zu können. So wurde beispielsweise der Zugriff auf die wichtigsten Fachverfahren und das E-Mail-Programm realisiert. Die Anstrengungen zeigten schnell Wirkung: Sicherungsarbeiten am Wochenende ermöglichten es, dass bereits nach zwei Werktagen einzelne Abteilungen den Notbetrieb aufnehmen konnten. „Sicher, schnell und effektiv hat unser Cyber Security Incident Response Team im 24/7-Einsatz in Zusammenarbeit mit allen Fachabteilungen den Wiederaufbau der Mössinger Verwaltung unterstützt,“ erklärt Mark Schimmer, CSIRT-Leiter der Komm.ONE.

Optimiert in die Zukunft dank kritischem Rückblick

Zur erfolgreichen Bewältigung eines Sicherheitsvorfalls gehört auch ein genauer Review der Ereignisse. Darum haben sich alle Beteiligten nach der Bewältigung der akuten Gefahrensituation zu einer kritischen Analyse zusammengefunden. Durch die detaillierte Berichterstattung konnten alle relevanten Aspekte – Ursachen, Auswirkungen, Maßnahmen – einer Bewertung unterzogen werden. Das aufgezeigte Verbesserungspotenzial führte zu einer weiteren Optimierung der Notfall- und Ablaufpläne. Auch die Schulung der Mitarbeitenden wurde noch einmal angepasst, die Aufmerksamkeit beim Thema Cybersicherheit weiter erhöht.

Das Fazit: Der Cyberangriff hat zwar zu einem kurzfristigen Ausfall der Verwaltungsdienste geführt, der Notbetrieb konnte jedoch innerhalb kurzer Zeit aufgenommen und ein größerer Schaden abgewendet werden. Erfreulicher Nebeneffekt: Die erfolgreiche Präventionsarbeit und die sofortige Reaktion Mössingens bereits bei den ersten Auffälligkeiten sowie der mit dem Angriff einhergehende Lernprozess haben die Resilienz der Mössinger Verwaltung und die Sicherheit ihrer IT-Systeme letztendlich sogar weiter gestärkt.

„In einem solchen Krisenfall ist es von zentraler Bedeutung, gut zusammenzuarbeiten und gemeinsam nach vorn zu blicken. Denn mehr denn je werden wir an den Entscheidungen gemessen, die wir in einem solchen Fall treffen. Mössingen hat das exzellent gemacht“, attestiert das Beratungsteam aus CSBW, LKA und Komm.ONE.