

Wenn der Bildschirm schwarz bleibt



Wenn Hacker angreifen, zählt jede Minute. Mit IT-Notfallübungen der Cybersicherheitsagentur Baden-Württemberg können sich Kommunen auf den Ernstfall vorbereiten – und bleiben damit handlungsfähig, wenn er eintritt. Wie Eppingen eine solche Übung durchführte und welche Erkenntnisse die Stadt daraus zog, erklärt Sönke Brenner in seinem Gastbeitrag.

Was passiert, wenn plötzlich keine E-Mails mehr versendet werden können, Fachverfahren ausfallen und Mitarbeitende keinen Zugriff mehr auf ihre Systeme haben? Für Kommunen ist diese Frage längst keine theoretische mehr. Cyberangriffe auf öffentliche Verwaltungen haben in den vergangenen Jahren deutlich zugenommen.

Um auf einen solchen Ernstfall vorbereitet zu sein, führte die Stadt Eppingen Anfang Dezember 2024 gemeinsam mit der Cybersicherheitsagentur Baden-Württemberg (CSBW) eine umfassende IT-Notfallübung durch. Die Übung war Teil eines Pilotprojekts der CSBW, das Kommunen dabei unterstützt, ihre Reaktionsfähigkeit auf Cyberkrisen zu überprüfen und weiterzuentwickeln. Ziel war es, die Verantwortlichen für die besonderen Herausforderungen eines IT-Ausfalls zu sensibilisieren, die Zusammenarbeit im Krisenfall zu trainieren und konkrete Verbesserungsmöglichkeiten für die Notfallvorsorge zu identifizieren.

Cyberkrise realitätsnah simuliert

An der ganztägigen Übung nahmen Vertreter der Verwaltungsführung, der IT, der Personalverwaltung, der Öffentlichkeitsarbeit sowie weitere Mitglieder des vorgesehenen Krisenstabs teil. Begleitet wurde die Veranstaltung durch Fachleute der Cybersicherheitsagentur Baden-Württemberg. Besonderes Interesse zeigte auch der damalige Chief Digital Officer (CDO) des Landes Baden-Württemberg, Stefan Krebs, der sich vor Ort ein Bild von der Durchführung der Übung machte und den Austausch mit den Beteiligten suchte. Sein Besuch unterstrich die Bedeutung, die das Land der Stärkung der kommunalen Cyberresilienz beimisst.
Die Übung gliederte sich in mehrere Abschnitte. Im Mittelpunkt stand zunächst ein Cyber-Simulationsworkshop, bei dem die Teilnehmenden Schritt für Schritt mit einem sich zuspitzenden Angriffsszenario konfrontiert wurden. Ziel war es, ein möglichst realistisches Lagebild zu erzeugen und die Verantwortlichen unter Zeitdruck zu Entscheidungen zu zwingen – ähnlich wie in einem tatsächlichen Cybervorfall.

Vom ersten Alarm bis zum Krisenstab

Das eingespielte Szenario orientierte sich an einem schwerwiegenden Cyberangriff auf die städtische IT-Infrastruktur. Nach ersten Auffälligkeiten verdichteten sich die Hinweise auf eine Kompromittierung zentraler Systeme. Im weiteren Verlauf standen die Teilnehmenden vor typischen Fragestellungen eines Cybernotfalls:

Wer muss zuerst informiert werden?
Wann wird der Krisenstab einberufen?
Welche Stellen sind zu melden?
Wie kann die Verwaltung handlungsfähig bleiben?
Welche Informationen werden an Mitarbeitende, Bürgerinnen und Bürger sowie die Presse weitergegeben?

Dabei wurde deutlich, dass bei einem IT-Ausfall nicht nur technische Fragen zu lösen sind. Vielmehr rücken organisatorische und kommunikative Aspekte schnell in den Vordergrund. So mussten die Teilnehmenden entscheiden, welche Dienstleistungen weiterhin analog angeboten werden können, wie Zahlungen und Gehaltsabrechnungen sichergestellt werden und welche Prioritäten beim Wiederanlauf der Systeme gelten.

Im Anschluss an die Simulation folgte eine Kommunikationsübung. Hier stand die Zusammenarbeit innerhalb des Krisenstabs im Fokus. Die Teilnehmenden mussten Informationen bewerten, Entscheidungen vorbereiten und gegenüber unterschiedlichen Zielgruppen kommu-

Fotos – Adobe Stock, Stadt Eppingen



Die Verwaltung in Eppingen probt das Szenario eines Angriffs: Bei einem IT-Ausfall sind nicht nur technische, sondern auch organisatorische Fragen zu lösen.

nizieren. Gerade in einer Krisensituation zeigte sich, wie wichtig klare Zuständigkeiten, kurze Entscheidungswege und eine offene Diskussionskultur sind. Ein weiterer Baustein war die Krisenstabsarbeit. Dabei wurden grundlegende Methoden der Krisenorganisation vermittelt und anhand des Szenarios praktisch angewendet. Die Übungsleitung legte besonderen Wert darauf, dass sich alle Beteiligten unabhängig von Hierarchieebenen aktiv einbringen konnten.

Stärken erkannt – Handlungsbedarf identifiziert

Das Fazit der Cybersicherheitsagentur fiel insgesamt positiv aus. Besonders hervorgehoben wurden die hohe Beteiligung aller Akteure, die offene Diskussion im Krisenstab und die Bereitschaft, unterschiedliche Sichtweisen in die Entscheidungsfindung einzubeziehen. Gleichzeitig zeigte die Übung zahlreiche Ansatzpunkte für weitere Verbesserungen auf. So wurde deutlich, wie wichtig aktuelle und auch offline verfügbare Unterlagen sind. Netzwerkpläne, Rollen- und Rechtekonzepte, Notfallhandbücher, Passwortzugänge oder Kontaktlisten müssen im Ernstfall unabhängig von der eigenen IT-Infrastruktur verfügbar sein.

Auch die Alarmierungs- und Eskalationswege wurden intensiv betrachtet. Wer informiert wen? Welche Entscheidungen können auf welcher Ebene getroffen werden? Und wie werden Vertretungsregelungen organisiert? Die Übung machte deutlich, dass diese Fragen bereits vor einem Ereignis verbindlich geklärt werden müssen. Ein weiterer Schwerpunkt lag auf der Krisenkommunikation. Die Teilnehmenden diskutierten die Information des Gemeinderats, die Kommunikation mit den Mitarbeitenden sowie den Umgang mit Medienanfragen. Die Empfehlung der Expertinnen und Experten: Kommunen sollten frühzeitig Kommunikationsstrategien entwickeln und transparent mit Cybervorfällen umgehen, sobald belastbare Erkenntnisse vorliegen.

Konkrete Maßnahmen für mehr Resilienz

Aus der Übung entstand ein umfangreicher Maßnahmenkatalog. Dazu gehören unter anderem die Erstellung eines IT-Notfallhandbuchs, die Definition von Meldeketten und Erstmaßnahmen, die Einrichtung alternativer Kommunikationswege sowie die Vorbereitung analoger Arbeitsabläufe für kritische Verwaltungsleistungen. Darüber hinaus sollen wichtige Fachverfahren priorisiert, Notfallarbeitsplätze vorbereitet und die Zusammenarbeit mit externen Partnern weiter ausgebaut werden. Auch die gegenseitige Unterstützung innerhalb der Verwaltungsgemeinschaft und der Austausch mit bereits betroffenen Kommunen wurden als wichtige Bausteine identifiziert.

Die Erkenntnis aus der Übung ist eindeutig: Absolute Sicherheit gibt es nicht. Entscheidend ist vielmehr, wie gut eine Organisation auf einen Vorfall vorberei-

Mit der kostenfreien IT-Notfallübung unterstützt die Cybersicherheitsagentur Baden-Württemberg Kommunen dabei, sich praxisnah auf Cyberangriffe vorzubereiten. In einem simulierten IT-Sicherheitsvorfall trainieren Krisenstäbe ihre Abläufe und stärken ihre Handlungsfähigkeit im Ernstfall.

Interessierte Kommunen können sich für Informationen zu den kommenden Terminen per E-Mail an **beratung@cybersicherheit.bwl.de** wenden. Mehr zum Angebot der CSBW finden Sie zudem unter **www.cybersicherheit-bw.de/it-notfalluebung**







tet ist und wie schnell sie handlungsfähig bleibt. Gerade Kommunen müssen auch unter schwierigen Bedingungen ihre Kernaufgaben erfüllen können – von der Auszahlung von Gehältern über die Arbeit der Feuerwehr bis hin zu den Dienstleistungen für Bürgerinnen und Bürger.

Üben schafft Sicherheit

Die IT-Notfallübung in Eppingen hat eindrucksvoll gezeigt, dass Cybersicherheit weit mehr ist als eine technische Aufgabe der IT-Abteilung. Sie ist eine Führungsaufgabe und betrifft die gesamte Verwaltung. Mit der Unterstützung der Cybersicherheitsagentur Baden-Württemberg konnte die Stadt ihre organisatorischen und technischen Vorsorgemaßnahmen kritisch überprüfen und gezielt weiterentwickeln.

Das betont auch Eppingens Rathauschef Klaus Holaschke: „Die Digitalisierung eröffnet Kommunen enorme Chancen. Gleichzeitig wächst aber auch die Verantwortung, unsere Systeme und Daten bestmöglich zu schützen. Die IT-Notfallübung hat uns gezeigt, dass Cybersicherheit keine Aufgabe der IT allein ist, sondern die gesamte Verwaltung betrifft. Entscheidend ist, im Ernstfall schnell, strukturiert und handlungsfähig zu bleiben“, so der Oberbürgermeister. „Cyberangriffe machen nicht an Stadt- oder Gemeindegrenzen halt. Umso wichtiger ist es, dass Kommunen, Land und spezialisierte Institutionen wie die Cybersicherheitsagentur Baden-Württemberg eng zusammenarbeiten. Die Übung hat uns gezeigt, dass wir auf einem guten Weg sind, aber auch, wo wir noch nachschärfen müssen. Der Besuch des damaligen CDO Baden-Württemberg, Stefan Krebs, hat die Bedeutung des Themas zusätzlich unterstrichen.“

Die aus der Übung gewonnenen Erkenntnisse stärken nicht nur die eigene Resilienz, sondern liefern auch wertvolle Impulse für andere Kommunen. Denn eines wurde während der Übung besonders deutlich: Auf den Ernstfall vorbereitet zu sein, bedeutet nicht, einen Cyberangriff verhindern zu können. Es bedeutet, auch dann handlungsfähig zu bleiben, wenn er tatsächlich eintritt.





Sönke Brenner ist Leiter der Abteilungen IT, Personal und Organisation sowie der Stabsstelle des Oberbürgermeisters und Digitalisierung bei der Stadt Eppingen.

Fotos – Adobe Stock, Stadt Eppingen