CSBW

Den IT-Notfall praktisch üben

[10.11.2026] Die Cybersicherheitsagentur Baden-Württemberg hat mit der Stadt Eppingen ihre erste eigen, umfassende IT-Notfallübung durchgeführt. Dabei ging es nicht nur um Technik, sondern auch um Kommunikation. Das Angebot steht weiteren Kommunen und öfentlichen Stellen offen.

Wenn Hacker angreifen, zählt jede Minute. Die Cybersicherheitsagentur Baden-Württemberg (CSBW) bietet eine realitätsnahe Notfallübung, mit deren Hilfe sich Kommunen auf den Ernstfall vorbereiten können. Damit bleiben sie handlungsfähig. Denn auch wenn die Angreifer nicht weit in IT-Systeme vordringen, wenn keine Daten entwendet werden – in solchen Fällen sind Kommunen oft von einem Moment zum nächsten von der digitalen Außenwelt abgeschnitten. Was passiert, wenn keine E-Mails mehr versendet werden können, Fachverfahren ausfallen und Mitarbeitende keinen Zugriff mehr auf ihre Systeme haben, wurde nun erstmals erfolgreich mit der Stadt Eppingen simuliert: Dort hat die CSBW die erste eigene IT-Notfallübung durchgeführt.

Üben schafft Sicherheit

Wie die CSBW betont, habe die IT-Notfallübung in Eppingen gezeigt, dass Cyber-Sicherheit weit mehr sei als eine technische Aufgabe der IT-Abteilung. Vielmehr handele es sich um eine Führungsaufgabe, die aber die gesamte Verwaltung betrifft. Mit der Unterstützung der CSBW können Kommunen, Landkreise und öffentliche Stellen lernen, organisatorische und technische Vorsorgemaßnahmen kritisch zu überprüfen und gezielt weiter zu entwickeln. Die aus der Übung gewonnenen Erkenntnisse stärken dabei nicht nur die eigene Resilienz, sondern liefern auch wertvolle Impulse für andere öffentliche Stellen. An der ganztägigen Übung für die Kommunal- und Landesverwaltung Baden-Württemberg können Vertreterinnen und Vertreter aus der Verwaltungsführung, der IT, der Personalverwaltung, der Öffentlichkeitsarbeit sowie weitere Mitglieder des vorgesehenen Krisenstabs teilnehmen.

Von der Cyber-Krise zur Kommunikations-Krise

Bei einem echten Cyber-Notfall und auch in der Übung verdichten sich nach ersten Auffälligkeiten oft die Hinweise auf eine Kompromittierung zentraler Systeme. Im Verlauf der Übung werden die Teilnehmenden dann vor typischen Fragestellungen eines Cyber-Notfalls gestellt: Wer muss zuerst informiert werden? Wann wird der Krisenstab einberufen? An welche externen Stellen muss Meldung gemacht werden? Welche Informationen werden an Mitarbeitende, Bürgerinnen und Bürger sowie die Presse weitergegeben? Und schließlich: Wie kann die Organisation handlungsfähig bleiben?

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

Vom ersten Alarm zum Krisenstab

In diesem Teilbereich der Übung steht die Zusammenarbeit innerhalb des Krisenstabs im Fokus. Die Teilnehmenden lernen wie sie Informationen bewerten, Entscheidungen vorbereiten und gegenüber unterschiedlichen Zielgruppen kommunizieren. Gerade in einer Krisensituation zeigt sich, wie wichtig klare Zuständigkeiten, kurze Entscheidungswege und eine offene Diskussionskultur sind. Ein weiterer Baustein der IT-Notfallübung ist die Krisenstabsarbeit. Dabei werden grundlegende Methoden der Krisenorganisation vermittelt und anhand des Szenarios praktisch angewendet.

Maßnahmen für mehr Resilienz

Aktiv geht es bei der Übung auch um den Ausbau der Resilienz in der Behörde, Kommunen oder öffentlichen Stelle. Aus den IT-Notfallübungen der CSBW entsteht für Kommunen, die an der Übung teilnehmen, ein individueller Maßnahmenkatalog. Sie erhalten Empfehlungen aus den verschiedenen Bereichen des Krisenmanagements. Dazu gehören nach Angaben der CSBW unter anderem die Erstellung eines IT-Notfallhandbuchs, die Definition von Meldeketten und Erstmaßnahmen, die Einrichtung alternativer Kommunikationswege und die Vorbereitung analoger Arbeitsabläufe für kritische Verwaltungsleistungen. „Cyberangriffe machen nicht an Stadt- oder Gemeindegrenzen halt. Umso wichtiger ist es, dass Kommunen, Land und spezialisierte Institutionen wie die CSBW eng zusammenarbeiten. Die Übung hat uns gezeigt, dass wir auf einem guten Weg sind, aber auch, wo wir noch nachschärfen müssen“, sagt Sönke Brenner, Leiter der Abteilungen IT, Personal und Organisation sowie der Stabsstelle des Oberbürgermeisters und Digitalisierung bei der Stadt Eppingen.

(sib)

Stichwörter: Allgemein, CSBW, Eppingen