Serie Cyber-Sicherheit

Lohnenswerte Investition

[20.02.2023] Da die Bevölkerung auf arbeitsfähige Kommunen angewiesen ist, müssen sich diese nach einem Cyber-Angriff möglichst schnell erholen und mit der Wiederaufbauphase beginnen. Die Resilienz lässt sich durch ein Business Continuity Management stärken.

Mit der voranschreitenden Digitalisierung wächst die Erwartungshaltung der Bürgerinnen und Bürger: Dienstleistungen der Verwaltung sollen nutzerfreundlich, digital und möglichst ohne Wartezeiten erbracht werden. Nahezu jeder bürgernahe digitale Service erfordert ein komplexes Zusammenspiel zwischen unterschiedlichen Software-Schnittstellen, Datenbanken und Dienstleistern. Ein Cyber-Angriff auf eine solche gewachsene, komplexe Struktur hat oftmals ungeahnte Folgen. Die Realität zeigt auch, dass eine Rückkehr zum Zustand vor dem Cyber-Angriff fast unmöglich ist: Essenzielle Datenbanken müssen rekonstruiert werden, im Darknet veröffentlichte Daten sind nicht mehr zurückzuholen und Fristen etwa von Bußgeldverfahren können nicht eingehalten werden.
Doch Bürgerinnen und Bürger sowie lokale Unternehmen sind darauf angewiesen, dass die Kommune nach einem Cyber-Angriff schnell wieder arbeitsfähig ist. Die Frage ist daher nicht, ob bei einem Cyber-Angriff Schäden entstehen, sondern wie schnell sich eine Kommune erholt und die Wiederaufbauphase beginnen kann. Diese Fähigkeit, die organisatorische Resilienz, lässt sich mit einer der wichtigsten Maßnahmen des Cyber-Sicherheitsmanagements erhöhen. Diese erfordert die Mitarbeit und das Mitdenken unterschiedlicher Fachgruppen und Beschäftigter und liegt in der Verantwortung der Leitung: das Business Continuity Management (BCM).

Den Ernstfall immer wieder üben

Business Continuity Management bezeichnet die Entwicklung und das Einüben von Plänen und Abläufen, welche bei einer Störung des Normalbetriebs greifen. Ziel ist es, den normalen Betrieb nicht oder zumindest nicht für lange Zeit zu unterbrechen oder rasch einen Notbetrieb realisieren zu können. Das BCM muss sich mit den Kommunen und deren Infrastruktur, Personalstärke, Arbeitsweise, Fachverfahren und gebotenen bürgernahen Dienstleistungen entwickeln. Es ist daher immer wieder zu prüfen, zu üben und anzupassen.
Das Business Continuity Management ist in der Norm ISO 22301:2019 definiert. Zur Unterstützung bei der Erarbeitung eines BCM stellt das Bundesamt für Sicherheit in der Informationstechnik (BSI) den Standard 200-4 und Hilfsmittel wie beispielsweise Formatvorlagen zur Verfügung. Anders als sein Vorgänger ist der neue BSI-Standard 200-4 in Stufen aufgebaut. Selbstverständlich sollen BCM und Notfallplan nicht zum Selbstzweck werden, sondern im Notfall hilfreich sein. Eine umfassende Leitlinie, die nicht geübt und auf Tauglichkeit geprüft wurde, ist im schlimmsten Fall nur ein Haufen nutzloses Papier.
Gemeinsam mit IT-Dienstleister ekom21 bietet das Land Hessen seinen Kommunen im Hessischen Cyberabwehrausbildungszentrum Land/Kommunen (HECAAZ L/K) kostenlose Schulungen zum Thema BCM an. Fast alle hessischen Kommunen nehmen dieses Angebot des Innenministeriums wahr.

Kommune im Gesamtkontext bedenken

Ein grundlegender erster Schritt ist die Betrachtung der Kommune im Gesamtkontext: Von welchen Dienstleistern, Zulieferern, Ressourcen und Stellen ist sie abhängig? Was geschieht, wenn eine dieser

Ressourcen ausfällt? Cyber-Kriminelle greifen immer häufiger die Lieferkette an. Diese so genannten Supply-Chain-Angriffe können auch IT-Dienstleister treffen und sich von dort auf die Kommune und kommunalen Eigenbetriebe ausbreiten. Hat der IT-Dienstleister in einem solchen Fall ausreichend Ressourcen, um die Kommune und ihre Eigenbetriebe im Notfallbetrieb und bei der Wiederherstellung zu unterstützen oder ist die Kommune in diesem Fall auf sich alleine gestellt? Die Betrachtung im Gesamtkontext ermöglicht es, solche Fragen vor dem Eintritt eines Notfalls zu erörtern.
Zum Gesamtkontext gehört auch, zu bestimmen, wer von der Kommune abhängig ist. In den meisten Fällen sind hier kommunale Eigenbetriebe, lokale Unternehmen sowie Bürgerinnen und Bürger zu nennen. Eine feinere Betrachtung dieser Gruppen ermöglicht Rückschlüsse auf wichtige Fachverfahren, die in einer Krise zeitnah wiederhergestellt werden müssen, da sie für das Leben und Wohlergehen der Bevölkerung elementar sind. Verbunden mit einer Erfassung der Fachverfahren, der dazugehörigen Daten und ihrer Abhängigkeit von anderen Fachverfahren kann so eine Priorisierung vorgenommen werden. Diese dient als Grundlage für die Planung der technischen, finanziellen und personellen Ressourcen eines Notfallbetriebs.

Grundsteine für den Notfallplan

Die erarbeitete Übersicht der Fachverfahren dient zudem als Grundlage für das Management von Datensicherungen. Welchen Datenverlust kann die Kommune verschmerzen, welche Daten können wieder rekonstruiert werden und welche Daten müssen auch nach einem Cyber-Angriff rasch zur Verfügung stehen? Ein Beispiel für ein Fachverfahren, welches im Notbetrieb zeitnah wiederhergestellt werden muss, ist die Auszahlung von Sozialleistungen. Diese sind für die Empfängerinnen und Empfänger eine wesentliche Daseinsvorsorge. Die hierfür benötigten Daten haben daher eine besonders geringe Verlusttoleranz und müssen schnell wieder zur Verfügung stehen.
Diese Überlegungen bilden den Grundstein für den Notfallplan, der vor der Krise eingeübt, kritisch geprüft und angepasst werden muss. Viele Entscheidungen müssen die Handelnden nicht ad hoc in der Krise treffen, sondern können diese bereits vorab festlegen. Eine letzte Grundüberlegung ist, wer den Notfall ausrufen und den Notfallplan aktivieren kann. In größeren Kommunen bietet sich hier eine Besondere Aufbauorganisation (BAO) außerhalb der Linienorganisation an. Die BAO übernimmt Krisenkommunikation und Notfall-Management, während parallel die Wiederherstellung des Normalbetriebs anläuft. Ist die Normalität annähernd erreicht, wird die BAO wieder aufgelöst, und die Personen kehren in vollem Umfang in ihre normalen Rollen zurück.

Am reibungslosen Ablauf feilen

Durch Üben und Testen lässt sich ein reibungsloser Ablauf in der Krise fördern. Am Anfang steht eine moderierte Besprechung des Notfallplans – eine Planbesprechung. Eine Steigerung bietet die Stabsübung, bei der der Notfallstab gemeinsam die Bewältigung eines realitätsnahen Notfallszenarios simuliert. Dies kann durch zeitgleiche Simulationen anderer Organisationseinheiten, welche im Notfall zeitkritische Prozesse durchzuführen haben, ergänzt werden (Stabsrahmenübung). Aufwendigere Übungsszenarien sind die Alarmierungsübung und Funktionstests.
Ein BCM macht sich im Notfall bezahlt. Die eigene Kommune im Gesamtkontext zu betrachten, festzustellen, von welchen Dienstleistern und Ressourcen sie abhängig ist, und wer wiederum von ihr abhängig ist, erlaubt es rechtzeitig vor einer Krise, Lösungen zu finden. Wer Krisen dank vorausschauender Planung souverän meistern kann, braucht keinen Reputationsschaden zu fürchten.

()

Das Hessen CyberCompetenceCenter (Hessen 3C)

Dieser Beitrag ist in der Ausgabe Februar 2023 von Kommune21 erschienen. Hier können Sie ein Exemplar bestellen oder die Zeitschrift abonnieren.

Teil eins der Serie Cyber-Sicherheit

Stichwörter: IT-Sicherheit, Cyber-Sicherheit, Hessen CyberCompetenceCenter (Hessen3C) Serie Cyber-Sicherheit