Informationssicherheit für die Verwaltungsspitzen von Städten und Gemeinden

In diesem Papier werden Bedeutung und Herausforderung von Informationssicherheit in Städten und Gemeinden und die Rolle der Verwaltungsspitze beschrieben (I.). Darüber hinaus werden die notwendigen Schritte der Verwaltungsspitze zur Steigerung der Informationssicherheit in Städten und Gemeinden, für das IT-Notfallmanagement und das betriebliche Kontinuitätsmanagement (BCM) dargestellt (II.).

I. Informationssicherheit als Grundvoraussetzung kommunalen Handelns

Die Bedeutung von Informationssicherheit in den Städten und Gemeinden wächst rasant: Die Informationstechnik wird immer komplexer. Der Grad an Vernetzung ist hoch, die Abhängigkeit der Verwaltungen von IT-gestützten Verfahren groß. Gleichzeitig verschärfen sich Bedrohungslagen. Cyber-Angriffe nehmen zu und treffen auch die kommunale Ebene.

Umso wichtiger ist die Informationssicherheit für die Kommunen. Informationssicherheit zielt darauf ab, Daten, Informationen und Infrastrukturen angemessen vor allen denkbaren Gefahren zu schützen. Ohne Informationssicherheit gibt es kein verlässliches und nachvollziehbares Verwaltungshandeln in Städten und Gemeinden, keine erfolgreiche Digitalisierung und letztendlich keine kommunale Daseinsvorsorge.

Denn die Folgen von Angriffen auf die Informationssicherheit der Städte und Gemeinden können immens sein: Handlungsunfähige Behörden, enorme wirtschaftliche Schäden, veröffentlichte sensible Datensätze, Desinformation etc. Die Angebote der kommunalen Daseinsvorsorge und die gesamte Arbeitsfähigkeit der Kommunen werden so massiv bedroht, das Gemeinwesen insgesamt stark eingeschränkt.

Rolle der Verwaltungsspitze

Die Verwaltungsspitze trägt die Verantwortung für die Funktionsfähigkeit der Kommunalverwaltung, die stark von der Informationssicherheit abhängt. Informationssicherheit ist daher Sache der Verwaltungsspitze – „Chefinnen- und Chefsache“. Die Verwaltungsspitze übernimmt die Gesamtverantwortung für den Sicherheitsprozess. Sie steuert, kommuniziert und begleitet ihn aktiv im Zeitverlauf. Insbesondere die Vorbildfunktion der Verwaltungsspitze ist ein maßgeblicher Beitrag zur gelungenen Umsetzung von Informationssicherheit in der Verwaltung.

Zur Initiierung und kontinuierlichen Steuerung des Sicherheitsprozesses gehören strategische Leitaussagen der Verwaltungsspitze zur Informationssicherheit. Ebenso gehören konzeptionelle Vorgaben, die Schaffung organisatorischer Rahmenbedingungen sowie ausreichende Ressourcen

dazu. Die Verwaltungsspitze benennt Stellen, die sie bei der Wahrnehmung dieser Aufgaben unterstützen. Sowohl Technik und Organisation als auch die Beschäftigten aller Organisationseinheiten in den Städten und Gemeinden müssen aktiv einbezogen werden.

Die Erfolgsfaktoren sind Zusammenarbeit und Austausch: Innerhalb der Kommune und mit anderen Kommunen ebenso wie der Ebenen übergreifende Austausch mit Landesverwaltungen und ihren Institutionen und Einrichtungen sowie dem Bund. Es braucht ein gemeinsames Verständnis von Informationssicherheit und eine ausgezeichnete fachliche Expertise.

Die nachfolgende Liste soll dabei unterstützen, den aktuellen Stand der Informationssicherheit, des IT-Notfallmanagements und des betrieblichen Kontinuitätsmanagements sowie weiterer, damit verbundener Erfordernisse einzuschätzen, und auf dieser Grundlage Handlungsbedarf zu begründen und notwendige Maßnahmen zu identifizieren. Weitere Unterstützung können die Veröffentlichungen der zuständigen Stellen in den Ländern, der kommunalen Spitzenverbände und des Bundesamts für Sicherheit in der Informationstechnik (BSI) bieten.

II. Prüfliste für die Leitungsebene zu Informationssicherheit, IT-Notfallmanagement und betrieblichem Kontinuitätsmanagement

Hinweis: Die Fußnoten beziehen sich auf Standards, Bausteine oder Veröffentlichungen des IT-Grundschutzes des Bundesamtes für Sicherheit in der Informationstechnik (BSI).

a) Informationssicherheit

Die Verwaltungsspitze

- ☐ übernimmt erkennbar die Gesamtverantwortung für Informationssicherheit. Sie kommuniziert dies aktiv in die Institution und Gemeinde und legt Sicherheitsziele sowie eine Strategie fest.[1]

- ☐ benennt eine/n Informationssicherheitsbeauftragte/n (ISB), der/die im Auftrag der Verwaltungsspitze die Aufgabe Informationssicherheit koordiniert und vorantreibt. Insbesondere berät er/sie die Verwaltungsspitze zur Informationssicherheit. Der/die ISB wird mit den erforderlichen Kompetenzen und Ressourcen ausgestattet. Er/sie agiert für seine Aufgabenerfüllung unabhängig und weisungsfrei.[2]

- ☐ zeichnet die Leitlinie zur Informationssicherheit, die als Grundsatzdokument den Stellenwert der Informationssicherheit, die verbindlichen Prinzipien und das anzustrebende Niveau der Informationssicherheit beschreibt. Hierzu gehören die Sicherheitsziele, die wichtigsten Aspekte der Sicherheitsstrategie, die Verantwortlichkeiten sowie die Organisationsstruktur für Informationssicherheit.[3] Die Erstellung wird von der Verwaltungsspitze angestoßen und sollte unter Federführung des/der ISB erarbeitet und kontinuierlich aktualisiert werden.

[1] ISMS.1.A1 Übernahme der Gesamtverantwortung für Informationssicherheit durch die Leitung + ISMS.1.A2 Festlegung der Sicherheitsziele und -strategie
[2] ISMS.1.A4 Benennung eines Informationssicherheitsbeauftragten
[3] ISMS.1.A3 Erstellung einer Leitlinie zur Informationssicherheit + Handreichung zur Ausgestaltung der Informationssicherheitsleitlinie in Kommunalverwaltungen der Kommunalen Spitzenverbände

- ☐ verfügt über eine der Leitlinie entsprechende, geeignete Organisationsstruktur für Informationssicherheit, in der Aufgaben, Rollen, Verantwortungen und Kompetenzen nachvollziehbar definiert und zugewiesen sind.[4]

- ☐ initiiert die Umsetzung des IT-Grundschutz-Profils „Basis-Absicherung Kommunalverwaltung“.[5]

- ☐ lässt sich regelmäßig über den Status der Informationssicherheit sowie über mögliche Risiken und Konsequenzen aufgrund fehlender Sicherheitsmaßnahmen durch Management-Berichte informieren.[6]

- ☐ lebt Informationssicherheit aktiv vor und agiert als Vorbild für die Mitarbeitenden.

b) IT-Notfallmanagement als Kern eines betrieblichen Kontinuitätsmanagements

Das IT-Notfallmanagement ist eine Säule der Informationssicherheit und gleichzeitig ein Kernelement eines betrieblichen Kontinuitätsmanagements, das eine ganzheitliche Aufrechterhaltung des Geschäftsbetriebs zum Ziel hat. Es fokussiert auf den Ausfall der Ressource Informationstechnik (IT). Es betrachtet nicht den Ausfall von Personal, Infrastruktur (z. B. Gebäude und Anlagen) und Dienstleistungen in anderen Bereichen. Diese werden im ganzheitlichen Betriebskontinuitätsmanagement (BCM) betrachtet.

Die Verwaltungsspitze

- ☐ verfügt über ein IT-Notfallkonzept, in dem alle zeitkritischen Geschäftsprozesse und Ressourcen identifiziert und in dem die Geschäftsprozesse für einen Notbetrieb sowie eine Priorisierung für einen Wiederanlauf festgelegt wurden.[7]

Die IT-Leitung

- ☐ verfügt über ein IT-Notfallhandbuch ggf. als Teil eines übergeordneten Notfallhandbuchs, in dem die wichtigsten Informationen zu Rollen, Sofortmaßnahmen, Alarmierung und Eskalation sowie Kommunikations-, grundsätzlichen Geschäftsfortführungs-, Wiederanlauf- und Wiederherstellungsplänen enthalten sind.[8]

- ☐ testet und übt alle wesentlichen Sofortmaßnahmen und Notfallpläne regelmäßig und anlassbezogen.[9]

- ☐ hat mit der im Land zuständigen Stelle (z. B. Landes-CERT) geklärt, wie und für welche IT-Vorfälle Unterstützung gewährt werden kann.

[4] ISMS.1.A6 Aufbau einer geeigneten Organisationsstruktur für Informationssicherheit
[5] Vom BSI veröffentlichtes IT-Grundschutz-Profil: Basis-Absicherung Kommunalverwaltung. IT-Grundschutz-Profile sind Schablonen für bestimmte Anwendungsfälle aus der Praxis, mit der eine Umsetzung von Maßnahmen ressourcenschonend vorangetrieben werden kann.
[6] ISMS.1.A12 Management-Berichte zur Informationssicherheit
[7] DER.4.A7 Erstellung eines Notfallkonzepts
[8] DER.4.A1 Erstellung eines Notfallhandbuchs
[9] DER.4.A10 Tests und Notfallübungen

- ☐ hat IT-Dienstleister identifiziert, die bei IT-Notfällen geeignet unterstützen können und mit diesen Vorabsprachen zu Erreichbarkeit, Verfügbarkeit sowie ggf. Service-Level-Agreements getroffen.

- ☐ führt Schulungen für diejenigen durch, die mit der Bewältigung von IT-Notfällen betraut sind.[10]

- ☐ trägt die Verantwortung dafür, dass regelmäßig ausreichend aktuelle Sicherheitskopien (Offline-Backups) der Daten erstellt werden, um vor Verlust geschützt zu sein. Deren Wiederherstellung muss regelmäßig getestet werden.[11]

c) Business Continuity Management (BCM) als ganzheitlich betriebliches Kontinuitätsmanagement[12]

Ein ganzheitlich betriebliches Kontinuitätsmanagement - Business Continuity Management (BCM) – hat zum Ziel, durch geeignete Maßnahmen relevante Geschäftsunterbrechungen gar nicht erst eintreten zu lassen oder sicherzustellen, dass der Geschäftsbetrieb nach einem Ausfall in angemessener Zeit auf einem definierten Mindestniveau fortgeführt werden kann. Es ermöglicht so die Aufrechterhaltung des wesentlichen Geschäftsbetriebs. Ein BCM ist keine Alternative zu einem IT-Notfallmanagement, sondern schließt es mit ein und ermittelt Vorgaben für das IT-Notfallmanagement.

Die Verwaltungsspitze

- ☐ übernimmt für alle erkennbar die Gesamtverantwortung für ein betriebliches Kontinuitätsmanagement (Business Continuity Management (BCM)), legt hierfür Ziele fest.

- ☐ hat eine/n Business-Continuity-Beauftragte/n (BCB) benannt und mit den erforderlichen Kompetenzen und Ressourcen ausgestattet.

- ☐ verfügt eine Leitlinie zum BCM, in der der Stellenwert des betrieblichen Kontinuitätsmanagements, der abzusichernde Zeitraum, die Rahmenbedingungen, die Vorgehensweise sowie die Organisationsstruktur für ein BCM-System beschrieben werden.

- ☐ verfügt über eine geeignete Organisationsstruktur für ein BCM-System, in der Aufgaben, Rollen, Verantwortungen und Kompetenzen nachvollziehbar definiert und zugewiesen sind.

- ☐ hat eine Business Impact Analyse (BIA) initiiert, mit der zeitkritische Geschäftsprozesse und Ressourcen, sowie die potenziellen Auswirkungen bei deren Ausfall ermittelt werden.

- ☐ lässt sich regelmäßig über den Status des BCM sowie über mögliche Risiken und Konsequenzen aufgrund fehlender Sicherheitsmaßnahmen informieren.

[10] DER.4.A8 Integration der Mitarbeiter in den Notfallmanagement-Prozess
[11] CON.3 Datensicherungskonzept
[12] BSI-Standard 200-4 Business Continuity Management