Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Weg in die Basis-Absicherung (WiBA): Management Summary

Aufgaben der Leitungsebene

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
E-Mail: wiba@bsi.bund.de
Internet: https://www.bsi.bund.de

Inhalt

1 Einleitung

Die Abhängigkeit der Verwaltungen von IT-gestützten Verfahren ist groß, der Grad an digitaler Vernetzung in Städten und Gemeinden wächst stetig. Gleichzeitig verschärfen sich Bedrohungslagen. Cyber-Angriffe nehmen zu und treffen regelmäßig 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 durch Sicherheitsvorfälle so massiv bedroht, dass das Gemeinwesen dadurch stark eingeschränkt werden kann.

2 Zielsetzung

Um Kommunen bei der systematischen Umsetzung von Informationssicherheitsmaßnahmen zu unterstützen und die Risiken von Cybervorfällen zu minimieren, hat das BSI das Konzept der Einstiegsstufe „Weg in die Basis-Absicherung“ (WiBA) entwickelt.

Das vorliegende Dokument richtet sich an die Leitungsebene von Behörden und öffentlichen Institutionen. Ziel ist es, die Wichtigkeit des Informationssicherheitsprozesses auf oberster Ebene zu unterstreichen und ihr den Einstieg in den IT-Grundschutz zu vereinfachen.

WiBA führt noch nicht zur Etablierung eines Managementsystems für Informationssicherheit (ISMS). Vielmehr bietet WiBA einen Einstieg in das Thema und gibt konkrete Maßnahmenempfehlungen. Damit werden Gefährdungen für Kommunen effizient und effektiv minimiert und der Weg für eine Umsetzung des IT-Grundschutz-Profils „Basis-Absicherung Kommunalverwaltung“ [1] vorbereitet.

3 Funktion der Institutionsleitung

Als Voraussetzung für effektive Informationssicherheit ist es unabdingbar, dass die Leitung einer Institution sich ihren Aufgaben und Pflichten bewusst ist. Nachfolgend werden die grundlegenden Aufgaben für die Führungsspitze aufgezeigt, damit der Einstieg in die Informationssicherheit gelingen kann.

3.1 Übernahme der Gesamtverantwortung

Die Leitung einer Institution trägt stets die Gesamtverantwortung für die Informationssicherheit (IS). Entsprechend wichtig ist es, dass diese sich dessen bewusst ist, zu ihren Pflichten steht und positiv zur Informationssicherheit beiträgt. Gängige ISMS-Standards wie der BSI-Standard 200-2 (Kapitel 3.1) [2] und die DIN EN ISO/IEC 27001:2017 (Kapitel 5) [4] setzen eine aktive Rolle der Leitung daher fest voraus. Dafür muss sich die Institutionsleitung regelmäßig über den Status der Informationssicherheit informieren lassen und die möglichen Risiken kennen, die insbesondere aufgrund fehlender Maßnahmen drohen [3]. Die Kontrolle und Steuerung des Sicherheitsprozesses obliegt ebenfalls der Institutionsleitung.

Darüber hinaus hat die Leitung eine Vorbildfunktion gegenüber ihren Mitarbeitenden. Wird sie dieser nicht gerecht, sinkt in der Folge das allgemeine Bewusstsein für Informationssicherheit in der Institution. Sie wird damit z. B. anfälliger für Social Engineering und andere Angriffe, die den Faktor Mensch ausnutzen.

Zusammengefasst zeigt sich: **Informationssicherheit ist Chefinnen- und Chefsache!** Ein deutliches Engagement der Leitung hat in der Praxis einen erheblichen Effekt auf die positive Entwicklung der Informationssicherheit.

3.2 Festlegung der Informationssicherheitsstrategie und –ziele

Die oberste Leitungsebene muss den Sicherheitsprozess initiieren, steuern und überwachen. Die Aufgabe der Institutionsleitung umfasst zudem die Festlegung der Strategie zur Informationssicherheit und der Sicherheitsziele. Diese könnten beispielweise eine kurzfristige Umsetzung der vorliegenden Einstiegsstufe, mittelfristig die Anwendung des IT-Grundschutz-Profils „Basis-Absicherung Kommunalverwaltung“ und langfristig die vollständige IT-Grundschutz-Methodik mit einer optionalen Zertifizierung vorsehen. Dabei muss immer der Bezug zu den Zielen und Aufgaben der Institution berücksichtigt werden.

3.3 Aufgaben verteilen und Ressourcen bereitstellen

Die Leitung einer Institution ist für die Aufgabenverteilung innerhalb des Sicherheitsprozesses verantwortlich. Insbesondere muss sie festlegen, wer dabei die Koordination dieses Prozesses übernimmt. Die Aufgaben in der Informationssicherheit erfordern eine Kommunikation über verschiedene Fachabteilungen und Hierarchiestufen hinweg.

Informationssicherheit betrifft ohne Ausnahme alle Mitarbeitenden. Um Sicherheitsmaßnahmen wie geplant umsetzen zu können, müssen bei den Mitarbeitenden die erforderlichen Grundlagen vorhanden sein. Dazu gehört neben den Kenntnissen, wie Sicherheitsmechanismen bedient werden müssen, auch das Wissen über den Sinn und Zweck von Sicherheitsmaßnahmen und wie mögliche Risiken verringert werden können, wenn Sicherheitsmaßnahmen eingehalten werden (Sensibilisierung). Auch das Arbeitsklima, gemeinsame Wertvorstellungen und das Engagement der Mitarbeitenden beeinflussen die Informationssicherheit entscheidend.

Zudem sollten von der Leitung geeignete organisatorische Rahmenbedingungen geschaffen werden. Alle Personen mit Aufgaben im Kontext der Informationssicherheit müssen entsprechend qualifiziert sein. Diesen Personen müssen die notwendigen Ressourcen (zeitlich und finanziell) zur Verfügung stehen. Hierzu zählen neben dem Personalbedarf beispielsweise auch Investitionen in erforderliche Software, Hardware und Infrastruktur. Auch die Teilnahme an Schulungen, um das Wissen der Fachkräfte (z. B. Administratoren und Administratorinnen) zu erhalten und auszubauen, muss ermöglicht werden.

3.4 Vorgehensweise

Informationssicherheit ist kein Projekt, sondern sollte von der Institutionsleitung als ein dauerhafter Prozess verstanden werden. Um wesentliche Sicherheitsmaßnahmen bereits zu Beginn umzusetzen, ist die vorliegende Vorgehensweise die geeignete Wahl. Mit der Einstiegsstufe können Institutionen ohne tiefergehende methodische Kenntnisse einen Sachstand anhand einfacher Checklisten erheben und wesentliche, effektive Sicherheitsmaßnahmen umsetzen. So kann durch den effizienten Einsatz von Ressourcen ein gesteigertes Sicherheitsniveau erreicht werden. Aufbauend auf diesem Sicherheitsniveau kann dann nahtlos das IT-Grundschutz-Profil „Basis-Absicherung Kommunalverwaltung“ sowie die gesamte Basis-Absicherung umgesetzt werden [1].

Der erste Schritt ist der wichtigste, fangen Sie an.

Viel Erfolg!

Literaturverzeichnis

[1] Arbeitsgruppe Kommunales Basis-Profil der Kommunalen Spitzenverbände und Bundesamt für Sicherheit in der Informationstechnik, „IT-Grundschutz-Profil: Basis-Absicherung Kommunalverwaltung," https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Profile/Basis_Absicherung_Kommunalverwaltung.html.

[2] Bundesamt für Sicherheit in der Informationstechnik, „BSI-Standard 200-2: IT-Grundschutz-Methodik", 2017. https://www.bsi.bund.de/dok/10027846.

[3] Deutscher Landkreistag und Bundesamt für Sicherheit in der Informationstechnik, „Informationssicherheit für Landrätinnen und Landräte" https://landkreistag.de/images/stories/themen/ITSicherheit/211217_Handlungsleitfaden_IT-Grundschutz.pdf.

[4] Deutsches Institut für Normung, DIN EN ISO/IEC 27001, Informationstechnik - Sicherheitsverfahren - Informationssicherheitsmanagementsysteme - Anforderungen, Berlin: Beuth-Verlag, 2017.