dsb
datenschutzbeauftragte
des kantons zürich

Leitfaden

Informationssicherheit in Gemeinden – Bevölkerungszahl > 6000

Inhalt

Datenschutzbeauftragte des Kantons Zürich
Postfach, 8090 Zürich, +41 43 259 39 99
datenschutz@dsb.zh.ch, datenschutz.ch, X: @dsb_zh

1 Einleitung

Die Digitalisierung durchdringt sämtliche Lebensbereiche. Eine Informationsbearbeitung ohne IKT-Unterstützung ist nicht mehr denkbar. Die Risiken nehmen zu und Angriffe auf Systeme häufen sich. Ein bewusster und strukturierter Umgang mit den Themen Informationssicherheit und Datenschutz ist notwendig. Ein Risikomanagement, klare Weisungen und gute Schutzmassnahmen, helfen die Risiken einzuschränken.

Dieser Leitfaden richtet sich an Gemeinden/Städte des Kantons Zürich mit mehr als 6000 Einwohnerinnen und Einwohnern und hilft bei der Einführung, Umsetzung und Pflege einer nachhaltigen Informationssicherheit. Er enthält eine Übersicht der vom Gesetz über die Information und den Datenschutz (IDG, LS 170.4) geforderten Massnahmen zur Informationssicherheit sowie eine Einführung, wie diese umgesetzt werden. Das Vorgehen, die Massnahmen und die Empfehlungen richten sich nach den Vorgaben der Allgemeinen und der Besonderen Informationssicherheitsrichtlinien des Kantons Zürich sowie dem international anerkannten Standard des deutschen Bundesamts für Sicherheit in der Informationstechnik (BSI). Weiter werden die von der Datenschutzbeauftragten (DSB) zur Verfügung gestellten Vorlagen erläutert.

2 Übersicht Dokumente

Für eine umfassende und integrale Informationssicherheit müssen die erforderlichen Informationssicherheitsdokumente auf der strategischen, taktischen und operativen Ebene erstellt werden. Die nachfolgende Pyramide zeigt die entsprechende Gliederung und Zuweisung der Dokumente in den verschiedenen Ebenen. Idealerweise werden die Dokumente im Top-Down-Ansatz (von oben nach unten) erstellt.

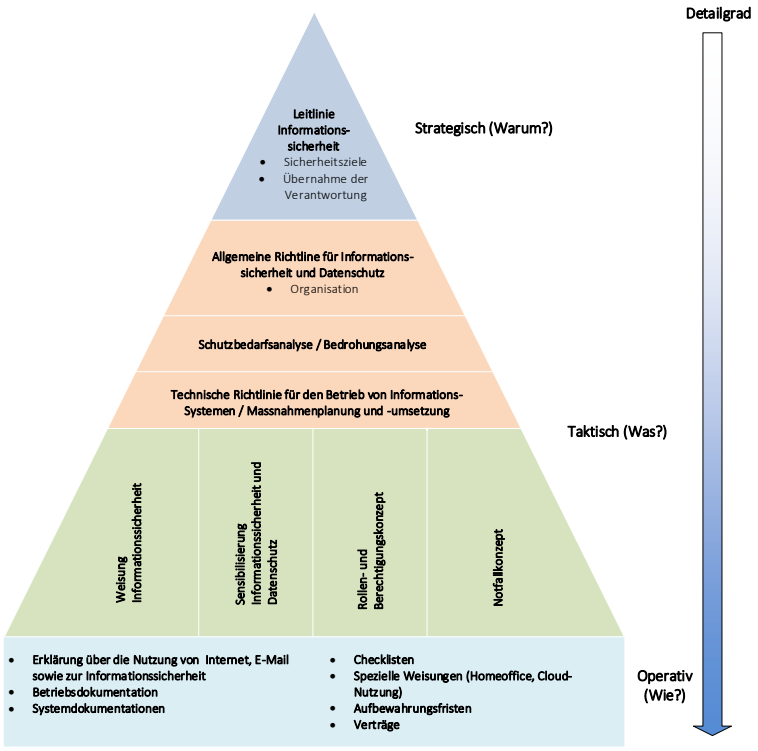

Abbildung 1: Sicherheitspyramide Übersicht Dokumente Informationssicherheit

Für die Erstellung und Einführung der nötigen Leitlinien, Weisungen und Konzepte stehen folgende Dokumente zur Verfügung.

Dokumente	Thema
Leitlinie	– Leitlinie zur Informationssicherheit in Gemeinden – Bevölkerungszahl > 6000 Einwohner
Vorlagen	– Allgemeine Richtlinie für Informationssicherheit und Datenschutz – Technische Richtlinie für den Betrieb von Informationssystemen – Schutzbedarfsanalyse – Weisung zur Informationssicherheit und zum Datenschutz – Erklärung über die Nutzung von Internet und E-Mail sowie zur Informationssicherheit – Sensibilisierung Informationssicherheit und Datenschutz – Rollen- und Berechtigungskonzept – Notfallkonzept – Bedrohungsanalyse – Betriebsdokumentation
Checklisten	– Massnahmenkatalog
Glossar / Abkürzungsverzeichnis	– Glossar und Abkürzungen Informationssicherheit

3 Umsetzung der Anforderungen an die Informationssicherheit

Informationssicherheit ist eine Aufgabe aller Mitarbeitenden von Verwaltungen und der Mitglieder von Behörden über alle Hierarchiestufen hinweg. Je nach interner Organisation können sich die Zuständigkeiten bei der Umsetzung der Informationssicherheit unterscheiden. Die oberste Leitung trägt die Verantwortung, legt entsprechende Abläufe fest und kann Verantwortliche für die Informationssicherheit bestimmen.

Die Umsetzung der Anforderungen an die Informationssicherheit in Gemeinden/Städten mit mehr als 6000 Einwohnerinnen und Einwohnern erfolgt in sieben Schritten:

1. Sicherheitsstrategie erstellen
2. Informationssicherheitsorganisation definieren
3. Allgemeine Richtlinie für Informationssicherheit und Datenschutz erstellen
4. Technische Richtlinie für den Betrieb von Informationssystemen erstellen
5. Schutzbedarfsanalyse durchführen
    a. Inventar der Anwendungen erstellen
    b. Anwendungsverantwortliche bestimmen
    c. Schutzstufe zuteilen
6. Massnahmenplanung und -umsetzung durchführen
    a. Verantwortliche zuweisen
    b. Basis-Sicherheitscheck durchführen
    c. Umsetzung planen
    d. Revision planen
7. Massnahmen umsetzen
    a. Weisung Informationssicherheit und Datenschutz erstellen
    b. Sensibilisierung Informationssicherheit und Datenschutz durchführen
    c. Rollen- und Berechtigungskonzept erstellen
    d. Bedrohungsanalyse erstellen
    e. Notfallkonzept erstellen

3.1 Schritt 1: Sicherheitsstrategie definieren

Die Sicherheitsstrategie, das angestrebte Sicherheitsniveau sowie die für die Gemeinde/Stadt gültigen Sicherheitsziele müssen definiert und festgehalten werden. Die DSB stellt eine Vorlage für die Erstellung zur Verfügung, die Leitlinie zur Informationssicherheit in Gemeinden – Bevölkerungszahl > 6000.

Was ist zu tun:

1. Layout der Vorlage Leitlinie zur Informationssicherheit in Gemeinden – Bevölkerungszahl > 6000 an das eigene Corporate Design anpassen
2. Inhalt überprüfen und ergänzen
3. Leitlinie durch einen Beschluss des Gemeinderats/Stadtrats in Kraft setzen
4. Leitlinie allen Mitarbeitenden kommunizieren und an einem intern zugänglichen Ort publizieren

3.2 Schritt 2: Informationssicherheitsorganisation definieren

Die Organisation, die zur Planung, Um- und Durchsetzung sowie Aufrechterhaltung des Informationssicherheitsprozesses erforderlich ist, wird als Informationssicherheitsorganisation bezeichnet.

Eine Informationssicherheitsorganisation muss aufgebaut werden. Diese definiert die Vorgaben und Anforderungen, um das definierte Sicherheitsniveau zu erreichen. Eine mögliche Regelung ist in der Vorlage Allgemeine Richtlinie für Informationssicherheit und Datenschutz dokumentiert.

Das von einer Gemeinde/Stadt angestrebte Informationssicherheitsniveau kann nur erreicht werden, wenn der Informationssicherheitsprozess gemeindeweit/stadtweit umgesetzt wird. Dieser übergreifende Charakter des Informationssicherheitsprozesses macht es notwendig, Rollen festzulegen und diesen die entsprechenden Aufgaben zuzuweisen. Die Informationssicherheitsorganisation ermöglicht diesen Prozess und erlaubt der Gemeinde/Stadt das angestrebte Informationssicherheitsniveau zu erreichen und aufrechtzuerhalten.

Im Rahmen der Informationssicherheitsorganisation sind die folgenden Rollen massgebend:

- die Gemeindeschreiberin/der Gemeindeschreiber / die Stadtschreiberin/der Stadtschreiber
- die Datenschutzberaterin/der Datenschutzberater
- die/der Informationssicherheitsverantwortliche
- die Daten- und Anwendungsverantwortlichen
- die Mitarbeitenden und die Lernenden

Was ist zu tun:

1. Rollenträgerinnen und -träger sowie Verantwortlichkeiten definieren und kommunizieren. Dabei ist zu beachten, dass nur qualifizierte Mitarbeitende eine optimale Aufgabenerfüllung gewährleisten.
2. Dokumentation der Rollenzuteilungen und Verantwortlichkeiten. Idealerweise werden die Aufgaben in den Stellenbeschreibungen festgehalten und die Rollenträger im Organigramm zugewiesen. Zudem ist den Mitarbeitenden ein Arbeitspensum zuzuweisen.
3. Die Mitarbeitenden benötigen für ihre Aufgaben entsprechendes Fachwissen und müssen ausgebildet werden, zum Beispiel durch den Besuch von Weiterbildungsveranstaltungen.

Die Struktur der Informationssicherheitsorganisation soll diejenige einer Stabsstelle sein, um den zentralen Rollenträgerinnen und Rollenträgern den direkten Zugang zu den Daten- und Anwendungsverantwortlichen zu gewährleisten.

Für die Datenschutzberatenden gelten folgende Anforderungen:

- Gesetz (IDG, LS 170.4) und Verordnung (IDV, LS 170.41) über die Information und den Datenschutz kennen
- Wichtigste Fachausdrücke der Informationssicherheit kennen

- Prozesse und Abläufe in der Gemeinde/Stadt kennen
- Fähigkeit haben, den Mitarbeitenden die datenschutzrechtlichen Voraussetzungen zu vermitteln
- Organisatorische Fähigkeiten haben, um datenschutzrelevante Massnahmen zu planen und umzusetzen
- Sollten nicht Gemeindeschreiberin/Gemeindeschreiber / Stadtschreiberin/Stadtschreiber sein
- Sollten nicht die informationssicherheitsverantwortliche Person sein

Für die Informationssicherheitsverantwortlichen gelten folgende Anforderungen:
- Überblick über die Aufgaben und Ziele der Gemeinde/Stadt haben
- Sich mit den Zielsetzungen der Informationssicherheit identifizieren
- Kooperations- und Teamfähigkeit
- Fähigkeit zum selbstständigen Arbeiten
- Durchsetzungsvermögen
- Erfahrungen im Projektmanagement
- Sollten nicht Gemeindeschreiberin/Gemeindeschreiber / Stadtschreiberin/Stadtschreiber sein
- Sollten nicht IKT-Verantwortliche/IKT-Verantwortlicher sein

Geeignete Personen für die Daten- und Anwendungsverantwortlichen der Fachanwendungen sind die Abteilungsleitungen. Für die übergreifenden Applikationen ist der oder die Informationssicherheits-verantwortliche die geeignete Person.

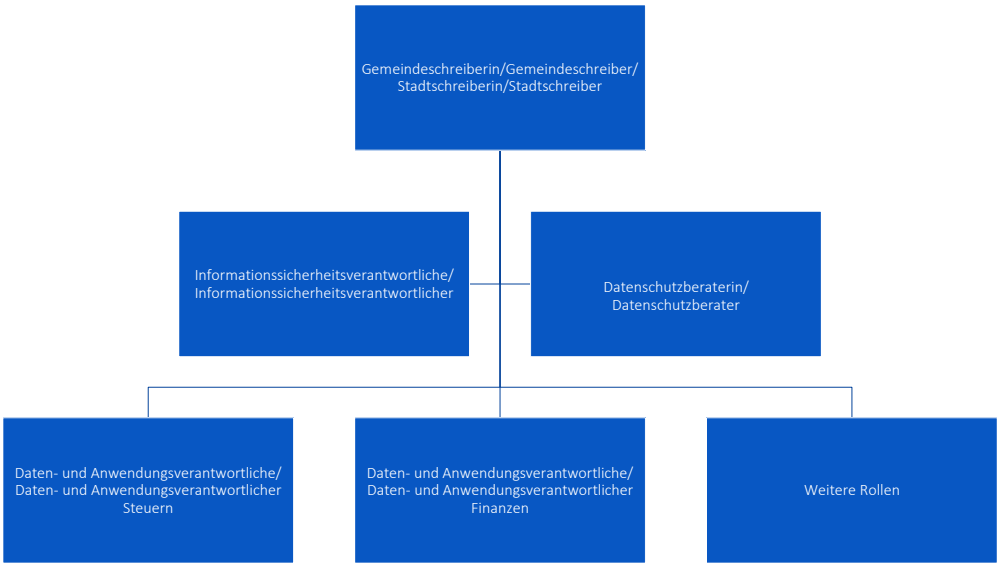

Abbildung 2: Beispiel Informationssicherheitsorganisation

3.3 Schritt 3: Allgemeine Richtlinie für Informationssicherheit und Datenschutz erstellen

Eine allgemeine Richtlinie für Informationssicherheit muss erstellt werden. Die DSB stellt hierzu die Vorlage Allgemeine Richtlinie für Informationssicherheit und Datenschutz zur Verfügung. Sie enthält die Organisation (Rollen und Verantwortlichkeiten) sowie allgemeine Regelungen der Informationssicherheit und des Datenschutzes.

Was ist zu tun:
1. Layout der Vorlage Allgemeine Richtlinie für Informationssicherheit und Datenschutz an das eigene Corporate Design anpassen.
2. Inhalte überprüfen und bei Bedarf anpassen.
3. Durch das oberste Organ der Gemeinde/Stadt genehmigen und in Kraft setzen lassen.

3.4 Schritt 4: Technische Richtlinie für den Betrieb von Informationssystemen ergänzen/erstellen

Die Vorlage Technische Richtlinie für den Betrieb von Informationssystemen enthält die technischen Vorgaben für den Betrieb der IKT-Umgebung. Diese können durch die Gemeinde/Stadt selbst umgesetzt werden oder in Zusammenarbeit mit externen Dienstleistern. Sie sind aus diesem Grund von der Allgemeinen Richtlinie losgelöst.

Was ist zu tun:
1. Layout der Vorlage Technische Richtlinie für den Betrieb von Informationssystemen an das eigene Corporate Design anpassen.
2. Inhalte überprüfen und bei Bedarf anpassen.

3.5 Schritt 5: Schutzbedarfsanalyse durchführen

Ziel der Schutzbedarfsanalyse ist es, die in Bezug auf das Risiko angemessenen Sicherheitsmassnahmen festzulegen. Eine Vorlage für die Durchführung der Schutzbedarfsanalyse stellt die DSB zur Verfügung. Für die Umsetzung sind die folgenden Schritte notwendig.

3.5.1 Inventar der Anwendungen erstellen

Für die Schutzbedarfsanalyse sind alle Anwendungen zu erheben, welche die Erfüllung oder Unterstützung bestimmter Aufgaben ermöglichen. Zusätzlich zu der Auflistung der Anwendungen sind die zugehörigen bearbeiteten Datenarten zu vermerken.

Nr	Funktion / Zweck	Anwendung	Bearbeitete Datenart
A.1	Baugesuchsverwaltung	CMI Bau	Nur Sachdaten
A.2	Scanning Steuererklärungen	ARTS	Personendaten
A.3	Office-Anwendungen	Office 2019	Besondere Personendaten

Abbildung 3: Beispiel Inventar Anwendungen

3.5.2 Anwendungsverantwortliche bestimmen

Für alle Anwendungen beziehungsweise Daten muss festgelegt werden, wer für ihre Sicherheit verantwortlich ist. Die Aufgaben der Anwendungsverantwortlichen sind in der Allgemeinen Richtlinie für Informationssicherheit und Datenschutz definiert. Die Anwendungsverantwortlichen sind im Register Anwendungen zu hinterlegen.

3.5.3 Schutzstufe zuteilen

Um den Schutzbedarf jeder Anwendung und der bearbeiteten Datenarten (Sachdaten, Personendaten, besondere Personendaten) zu beurteilen, sollte die Schutzstufe zugeteilt werden. Die Schutzstufe setzt sich aus den Schutzziele der Daten (Vertraulichkeit, Integrität, Verfügbarkeit) zusammen.

Schutzstufe		
Vertraulichkeit	Integrität	Verfügbarkeit
Hoch	Normal	Hoch
Normal	Normal	Normal
Sehr hoch	Normal	Sehr hoch

Abbildung 4: Schutzstufen

Im Register Schutzstufenzuteilung wird vorerst die Datenart sowie die Zuordnung (Normal, Hoch, Sehr hoch) überprüft und gegebenenfalls angepasst. Anschliessend wird pro Anwendung und je Schutzziel die Schutzstufe (Normal, Hoch, Sehr hoch) im Register Anwendungen zugeteilt.

Danach sind die restlichen Informationen (z.B. Hersteller, Betrieb durch und Datenstandort) zu ergänzen.

3.6 Schritt 6: Massnahmenplanung und -umsetzung durchführen

Zur Planung von Sicherheitsmassnahmen stellt die DSB einen Massnahmenkatalog. Dieser basiert auf dem IT-Grundschutzkatalog des deutschen Bundesamts für Sicherheit in der Informationstechnik (BSI). Der Massnahmenkatalog unterstützt das öffentliche Organ bei der Umsetzung und Kontrolle der Informationssicherheitsmassnahmen.

Jeder Massnahme ist eine eindeutige Nummer zugeordnet (z.B. ISMS.1.A1). Die vollständige Beschreibung der Massnahme kann über das BSI abgerufen werden.

3.6.1 Verantwortliche zuweisen

Die DSB empfiehlt Gemeinden/Städten mit > 6000 Einwohnerinnen und Einwohner die Massnahmen der Schutzstufe 2 umzusetzen. Diese sind im Massnahmenkatalog in der Spalte Niveau S2 mit einer 2 gekennzeichnet.

Sicherheitsmassnahmen werden nur plangemäss umgesetzt, wenn die Verantwortlichkeiten festgelegt sind. Diese können in der Spalte Verantwortung dokumentiert werden.

Was ist zu tun:

1. Massnahmenkatalog nach Niveau S2 filtern.
2. Für jede Sicherheitsmassnahme ist die oder der umsetzungsverantwortliche Mitarbeitende beziehungsweise Auftragnehmende einzutragen.

3.6.2 Basis-Sicherheitscheck durchführen

Beim Basis-Sicherheitscheck wird geprüft, ob die Massnahmen gemäss Niveau S2 bereits umgesetzt wurden oder ob Sicherheitsmassnahmen fehlen. Dieser Check wird anhand von Unterlagen, Gesprächen mit Verantwortlichen sowie stichprobenartigen Überprüfungen vor Ort ermittelt. Werden Dienstleistungen durch externe Auftragnehmende erbracht, ist die Gemeinde/Stadt dafür verantwortlich, dass die erforderlichen Sicherheitsmassnahmen umgesetzt sind.
Im Massnahmenkatalog stehen vier Möglichkeiten zur Verfügung, um den Umsetzungsgrad der Massnahmen in der Spalte Umsetzung zu dokumentieren:

- Ja – wenn alle in der Massnahme genannten Anforderungen vollständig umgesetzt sind.
- Teilweise – wenn einige, aber nicht alle Anforderungen umgesetzt sind.
- Nein – wenn keine oder nahezu keine der Anforderungen umgesetzt sind.
- Entbehrlich – wenn die Massnahme nicht benötigt wird, weil mindestens gleichwertige alternative Massnahmen umgesetzt wurden oder weil das zu schützende Objekt nicht vorhanden ist.

Was ist zu tun:

1. Status der Massnahmen bestimmen und in der Spalte Umsetzung dokumentieren. Wird bei einer Massnahme der Status Entbehrlich gewählt, so ist dies im Feld Bemerkung zu begründen.
2. Bei einer umgesetzten Massnahme ist die Spalte Nachweisdokument auszufüllen. Darin ist auf das Dokument zu verweisen, welches die umgesetzte Massnahme beschreibt.
3. In der Spalte Betroffene IKT-Systeme sind die Systeme zu dokumentieren, welche für die Massnahme anwendbar sind.
4. Bei Bedarf die restlichen Spalten nachführen
5. Massnahmenumsetzung bei den Verantwortlichen in Auftrag geben

3.6.3 Umsetzung planen

Die Umsetzung der noch nicht vorhandenen Massnahmen (Umsetzung: Teilweise/Nein) muss geplant werden. Dabei ist die Spalte Umsetzungstermin abzufüllen. Bei Bedarf sind zusätzlich die Priorität und Kosten einzutragen.

3.6.4 Revision planen

Bei der Durchführung von Revisionen kann der Massnahmenkatalog zur Unterstützung beigezogen werden. Bei jeder Massnahme kann der Termin der letzten und der nächsten Revision sowie die verantwortliche Revisorin beziehungsweise der verantwortliche Revisor dokumentiert werden. Der Status aller Massnahmen sollte mindestens alle drei Jahre überprüft werden.

Zudem ist die Umsetzung der Anforderung der Technische Richtlinie für den Betrieb von Informationssystemen zu überprüfen beziehungsweise einen Auftrag für die Umsetzung durch einen oder mehrere IKT-Dienstleister zu erteilen.

3.7 Schritt 7: Massnahmen umsetzen

Für Weisungen und Konzepte stellt die DSB Vorlagen zur Verfügung. Folgende Massnahmen sind bei der Umsetzung prioritär zu behandeln.

3.7.1 Weisung Informationssicherheit und Datenschutz erstellen

Die Vorlage Weisung zur Informationssicherheit und zum Datenschutz richtet sich an die Mitarbeitenden der Gemeinde/Stadt. Sie enthält die Regelungen, die bei der Arbeit zu beachten sind.

Was ist zu tun:

1. Layout der Vorlage Weisung Informationssicherheit und Datenschutz an das eigene Corporate Design anpassen
2. Durch das oberste Organ der Gemeinde/Stadt genehmigen und in Kraft setzen lassen
3. Weisung den Mitarbeitenden kommunizieren und mit Unterschrift bestätigen lassen (siehe Erklärung über die Nutzung von Internet und E-Mail sowie zur Informationssicherheit) sowie sicherstellen, dass dies bei neu eintretendem Personal ebenfalls erfolgt
4. Erklärungen in den Personaldossiers ablegen
5. Weisung und Erklärung zugänglich machen (z.B. auf dem Intranet)

3.7.2 Sensibilisierung für Informationssicherheit und Datenschutz durchführen

Die Vorlage Sensibilisierung für Informationssicherheit und Datenschutz enthält verschiedene Module zur Sensibilisierung und Schulung der Mitarbeitenden. Sie sind unterteilt in einen obligatorischen und einen optionalen Teil und setzt sich aus Inhalten für die erstmalige Grundausbildung sowie wiederkehrenden kurzen Ausbildungsblöcke zusammen.

Was ist zu tun:

1. Layout der Vorlage Sensibilisierung für Informationssicherheit und Datenschutz an das eigene Corporate Design anpassen
2. Zielgruppen und Kursleitende für Ausbildungsmodule bestimmen
3. Planung sowie Ausbildungskontrolle für obligatorische und optionale Ausbildungsmodule erstellen
4. Obligatorische Ausbildungsmodule durchführen
5. Eventuell optionale Ausbildungsmodule durchführen
6. Ausbildungskontrolle nachführen
7. Ausbildungsmodule periodisch prüfen und durchführen (z.B. für neu eintretende Mitarbeitende)

3.7.3 Rollen- und Berechtigungskonzept erstellen

Die Vorlage Rollen- und Berechtigungskonzept dient zur Beschreibung und Dokumentation der Berechtigungen von Mitarbeitenden der Gemeinde/Stadt auf die Dateiablage sowie die Anwendungen. Sie stellt sicher, dass die Berechtigungen nach klaren Vorgaben und beschränkt auf die notwendigen Rechte erfolgen.

Was ist zu tun:

1. Layout der Vorlage Rollen- und Berechtigungskonzept an das eigene Corporate Design anpassen
2. Funktionen und Verantwortlichkeiten gemäss Vorlage zuweisen
3. Zugriffsmatrix definieren (Rollen, Gruppen und Zuweisungen)
4. Prozesse für Beantragung, Prüfung, Zuweisung, Kontrolle und Löschung von Berechtigungen und Passwörtern festlegen

3.7.4 Bedrohungsanalyse erstellen

Die Vorlage Bedrohungsanalyse ist ein Hilfsdokument des Notfallkonzepts. Sie enthält einen vorgegebenen Katalog von Bedrohungen, die im Hinblick auf ihre Eintrittswahrscheinlichkeit sowie Auswirkungen auf die Gemeinde/Stadt beurteilt werden. Aufgrund der Analyse werden geeignete Massnahmen zu deren Verminderung oder Verhinderung definiert.

Was ist zu tun:

1. Überschriften und Titel der Vorlage Bedrohungsanalyse an die Gemeinde/Stadt anpassen
2. Bedrohungen gemäss Katalog auf Eintrittswahrscheinlichkeit und Auswirkung beurteilen und Risikostufe festlegen
3. Massnahmen definieren, mit jeweiligen Risiken verknüpfen und Risikostufe nach Massnahme bewerten.
4. Massnahmen zur Umsetzung planen und Fortschritt dokumentieren
5. Kommunikationsmatrix erstellen (als Ergänzung zum Notfallkonzept)

3.7.5 Notfallkonzept erstellen

Mit der Vorlage Notfallkonzept werden die Bedrohungen/Risiken, welche die Gemeinde/Stadt gefährden können, aufgenommen und bewertet sowie Schutzmassnahmen definiert. Sie enthält Vorgaben für das Vorgehen im Notfall sowie die dazu notwendige Organisation.

Was ist zu tun:

1. Layout der Vorlage Notfallkonzept an das eigene Corporate Design anpassen
2. Notfallorganisation, Funktionen und Kontaktinformationen aufnehmen
3. Notfallinfrastruktur definieren
4. Bedrohungen und Massnahmen aufnehmen (siehe auch Vorlage Bedrohungsanalyse)
5. Notfallprozesse definieren
6. Kommunikationsplan erstellen
7. Notfallkonzept den Mitarbeitenden vorstellen
8. Notfalltests und -übungen planen und durchführen
9. Notfallkonzept an verschiedenen Orten (auch physisch) aufbewahren, um es im Notfall zugänglich zu haben

4 Kontinuierliches Erhalten des Informationssicherheitsniveaus

Die Informationssicherheit ist ein fortlaufender Prozess. Um das Informationssicherheitsniveau erhalten zu können, sind die Massnahmen sowie deren Status regelmässig zu überprüfen und bei Bedarf anzupassen.

4.1 Regelmässige Überprüfung der Umsetzung der Massnahmen

Der Stand der Umsetzung muss regelmässig überprüft werden und die zuständige Stelle (z.B. die Gemeindeschreiberin/der Gemeindeschreiber / die Stadtschreiberin/der Stadtschreiber) ist über das Ergebnis zu informieren.

4.2 Regelmässige Überprüfung der Massnahmen

Die Erkenntnisse aus sicherheitsrelevanten Zwischenfällen, Veränderungen im technisch-organisatorischen Umfeld sowie Änderungen von Sicherheitsanforderungen erfordern eine Anpassung der bestehenden Sicherheitsmassnahmen. Dementsprechend sollten die Massnahmen mindestens jährlich respektive immer, wenn sich das Umfeld verändert, überprüft und angepasst werden, beispielsweise gemäss des BSI-Bausteins ISMS.1 Sicherheitsmanagement.

5 Links

Sicherheitsthemen benutzerfreundlich erklärt
Anleitung für das Erstellen eines IKT-Sicherheitskonzepts nach IT-Grundschutz
Diverse Dokumente zu den Themen Datenschutz und Informationssicherheit
Anwendung zur Überprüfung der Sicherheit von Passwörtern

V 3.5 / Oktober 2023