Leitlinie zur Informationssicherheit

Gliederung

1 Zielsetzung

In der Stadtverwaltung Hamm wird flächendeckend Informationstechnik eingesetzt, um der großen Aufgabenvielfalt mit sich ständig ändernden Anforderungen effizient begegnen zu können. Durch die Digitalisierung steigt der Bedarf an IT-Unterstützung immer mehr an. Mit dieser zunehmenden Abhängigkeit von der IT-Infrastruktur steigt auch das Risiko eines Ausfalls bzw. einer Beeinträchtigung der IT und damit der städtischen Geschäftsprozesse durch technisches Versagen oder durch Cyber-Angriffe weiter an.

Für die Bewertung und Verbesserung der Informationssicherheit zum Schutz vor solchen Risiken ist es notwendig, das Zusammenspiel der Informationen, IT-Verfahren, Aufgaben und Prozesse sowie der Infrastruktur der Informationstechnik und Kommunikationskanäle ganzheitlich zu betrachten. Informationssicherheit umfasst die Summe aller organisatorischen, personellen und technischen Maßnahmen, um die Schutzziele Vertraulichkeit, Verfügbarkeit und Integrität zu erreichen und damit die regelkonforme und störungsfreie Arbeit der Stadtverwaltung Hamm zu unterstützen.

Eine Informationssicherheitsleitlinie und das damit verbundene Informationssicherheits-managementsystem (im Folgenden: ISMS) ermöglichen den Mitarbeitenden, ein Grundverständnis zur Informationssicherheit zu entwickeln und somit aktiv das Informationssicherheitsniveau mitzugestalten.

Diese Informationssicherheitsleitlinie gibt den Rahmen für das Management der Informationssicherheit bei der Stadtverwaltung Hamm vor.

Die Vorgehensweise orientiert sich am IT-Grundschutz des Bundesamts für Sicherheit in der Informationstechnik (BSI) und dem Grundschutz-Kompendium in der jeweils aktuellen Fassung. Zu berücksichtigen sind zudem die einschlägigen Gesetze und internen Regelungen (z.B. AGA und Besondere Dienstanweisungen) zur Informationssicherheit und zum Datenschutz sowie die vertraglichen Regelungen.

2 Geltungsbereich

Die Leitlinie für Informationssicherheit gilt für alle Organisationseinheiten und Beschäftigte der Stadtverwaltung Hamm. Die Leitlinie und die daraus resultierenden Vorschriften und Maßnahmen sind von allen Bediensteten der Stadtverwaltung Hamm zu beachten und einzuhalten. Ebenfalls ist sie für alle Geschäftspartner:innen der Stadtverwaltung Hamm in Bezug auf die Bereiche der Zusammenarbeit verpflichtend. Den Eigenbetrieben der Stadtverwaltung Hamm wird die Anwendung und Umsetzung dieser Leitlinie empfohlen.

3 Sicherheits- / Aufbauorganisation

3.1 Verwaltungsleitung

Die Gesamtverantwortung für die Sicherheit der gesamten Informationsverarbeitung trägt die/der Oberbürgermeister:in. Es obliegt ihr/ihm, für die Umsetzung der Maßnahmen zur Gewährleistung der Informationssicherheit zu sorgen und die dafür benötigten Ressourcen bereitzustellen.

3.2 Verwaltungsvorstand

Der Verwaltungsvorstand, der der Leitung und Steuerung der Verwaltung dient, unterstützt den Oberbürgermeister bei der grundsätzlichen Organisation der Verwaltung sowie bei der Planung bedeutsamer Vorhaben und der Aufstellung des Haushaltsplanes und folglich auch bei der Umsetzung der Maßnahmen zur Gewährleistung der Informationssicherheit. Die Dezernent:innen sind darüber hinaus auch für die Umsetzung und Koordination der Maßnahmen in ihren Dezernaten zuständig.

3.3 Stabsstelle IT-Sicherheit

Die Stabsstelle IT-Sicherheit ist der Leitung des Amtes für Organisationsentwicklung, IT und Digitalisierung zugeordnet. Die Stabsstelle koordiniert die Bereiche Informationsicherheit, Notfallmanagement/ Business-Continuity-Management (im Folgenden: BCM) und IT-Sicherheit für die gesamte Stadtverwaltung. Die Stabsstelle unterstützt bei strategischen Entscheidungen, bei der Bewältigung von Sicherheitsvorfällen sowie bei Einzelmaßnahmen mit Sicherheitsbezug (z.B. bei Projekten entsprechender Größenordnung).

3.4 Informationssicherheitsbeauftragte:r

Die Leitung der Stabsstelle IT-Sicherheit nimmt die Funktion des Informationssicherheitsbeauftragten (im Folgenden: ISB) für die Stadtverwaltung wahr und wird in dieser Rolle durch die/den Oberbürgermeister:in ernannt. Die/Der ISB arbeitet fachlich weisungsfrei und steht den Führungskräften der Stadtverwaltung mit ihrer/ seiner Beratungsfunktion zur Seite.

Die Hauptaufgabe des ISB besteht darin, die Behördenleitung bei deren Aufgabenwahrnehmung bezüglich der Informationssicherheit zu beraten und diese bei der Umsetzung zu unterstützen. Seine Aufgaben umfassen unter anderem:

- den Informationssicherheitsprozess zu steuern und an allen damit zusammenhängenden Aufgaben mitzuwirken,
- die Leitungsebene bei der Erstellung der Leitlinie zur Informationssicherheit zu unterstützen,
- die Erstellung des Sicherheitskonzepts, des Notfallvorsorgekonzepts und anderer Teilkonzepte und System-Sicherheitsrichtlinien zu koordinieren sowie weitere Richtlinien und Regelungen zur Informationssicherheit zu erlassen,
- die Realisierung von Sicherheitsmaßnahmen zu initiieren und zu überprüfen,
- der Leitungsebene über den Status quo der Informationssicherheit zu berichten,
- sicherheitsrelevante Projekte zu koordinieren,
- Sicherheitsvorfälle zu untersuchen und
- Sensibilisierungs- und Schulungsmaßnahmen zur Informationssicherheit zu initiieren und koordinieren.

Die/ der ISB ist außerdem bei allen größeren Projekten, die deutliche Auswirkungen auf die Informationsverarbeitung haben könnten, zu beteiligen, um die Beachtung von Sicherheitsaspekten in den verschiedenen Projektphasen zu gewährleisten. So sollte der ISB bei

der Planung und Einführung neuer Anwendungen und IT-Systeme ebenso beteiligt sein wie bei neuen Komponenten oder wesentlichen Änderungen der Infrastruktur.

Es ist ein betrieblicher Informationssicherheitsbeauftragter bestellt:

Maik Zimner
Stadtverwaltung Hamm
Amt für Organisationsentwicklung, IT und Digitalisierung
Leitung Stabsstelle IT-Sicherheit
Informationssicherheitsbeauftragter
Theodor-Heuss-Platz 16
59065 Hamm

Fon: 02381 173335
Mail: maik.zimner@stadt.hamm.de

3.5 BCM-Koordination

Der Aufgabenzweck der Stadtverwaltung Hamm richtet sich nach dem Öffentlichen Zweck, welcher sich grundlegend aus dem Recht auf Kommunale Selbstverwaltung (Artikel 28 GG) ableiten lässt. Danach ist die Stadtverwaltung Hamm rechtlich dazu verpflichtet, das Wohl ihrer Einwohner:innen im Rahmen der kommunalen Daseinsvorsorge zu fördern.

Ein Ausfall des Geschäftsbetriebs hätte direkten Einfluss auf die Erfüllung des öffentlichen Auftrags, das Vertrauen der Bürger:innen sowie die öffentliche Ordnung und Versorgungssicherheit.

Ein umfangreiches Business Continuity Management (im Folgenden: BCM) ermöglicht es der Stadtverwaltung Hamm in einer Notfall- oder Krisensituation, zumindest die zeitkritischen Geschäftsprozesse in einem vorab definierten Notbetrieb fortführen zu können und schnellstmöglich in den Normalbetrieb zurückzukehren.

Im Rahmen des BCM-Systems (BCMS) werden sowohl eine BCM-Organisation sowie BCM-Prozessschritte, Maßnahmen und Pläne zur Notfallvorsorge als auch zur Notfallbewältigung etabliert, gesteuert und überwacht.

Die Stadtverwaltung Hamm verfolgt damit die folgenden Ziele:

- Die Sicherstellung der Aufgabenerfüllung der Stadtverwaltung Hamm gegenüber ihrer Einwohner:innen
- Die Sicherstellung, dass relevante Gesetze, Vorschriften, Normen und Standards eingehalten werden und Regressforderungen, Bußgelder, Strafen und Schadenersatz durch Anforderungen an das BCM angemessen verhindert werden.
- Den Schutz der Reputation der Stadtverwaltung Hamm in der Öffentlichkeit insbesondere bei Unterbrechungen des Geschäftsbetriebs.

Das BCM der Stadtverwaltung Hamm orientiert sich methodisch am BSI-Standard 200-4 „Business Continuity Management“.

3.6 Datenschutzbeauftragte:r

Die Stadtverwaltung Hamm erkennt den Datenschutz als Teil der Informationssicherheit (Ziel „Vertraulichkeit“) und somit als wichtiges Institutionsziel an. Zur Sicherstellung der sich daraus ergebenden Anforderungen dienen die vorliegenden Richtlinien. Alle Beschäftigten, die personenbezogene Daten verarbeiten, sind auf das Datengeheimnis verpflichtet.

Bei Änderungen der bestehenden Prozesse oder Einführung neuer Prozesse/ Verfahren ist der/die betriebliche Datenschutzbeauftragte frühzeitig zu beteiligen. Änderungen bzw. Neueinführungen werden erst nach Freigabe durch den/die betriebliche:n Datenschutzbeauftragte:n umgesetzt.

Es ist ein betrieblicher Datenschutzbeauftragter bestellt:

Ulrich Reinken
Stadtverwaltung Hamm
Büro des Oberbürgermeisters
Datenschutzbeauftragter
Theodor-Heuss-Platz 16
59065 Hamm

Fon: 02381 173557
Mail: reinken@stadt.hamm.de

3.7 Fachämter

Alle Führungskräfte in den Fachämtern tragen die Verantwortung, dass die einschlägigen Gesetze und internen Regelungen (z.B. AGA und Besondere Dienstanweisungen) zur Informationssicherheit und zum Datenschutz sowie die vertraglichen Regelungen von allen Mitarbeitenden der entsprechenden Fachbereiche eingehalten werden.
Alle Führungskräfte sensibilisieren ihre Mitarbeitenden für die Gefahren im Umgang mit Informationen und IT-Systemen und tragen dafür Sorge, dass ihre Mitarbeitenden hinreichend geschult sind.

3.8 Mitarbeitende

Alle Mitarbeitenden sind für die Informationssicherheit mitverantwortlich. Um ein geeignetes Informationssicherheitsniveau zu erreichen, wird die Mitwirkung aller Beschäftigten vorausgesetzt. Alle Beschäftigten haben durch die Einhaltung der einschlägigen Gesetze und internen Regelungen (z.B. AGA und Besondere Dienstanweisungen) zur Informationssicherheit und zum Datenschutz sowie der vertraglichen Regelungen zur Gewährleistung des Sicherheitsniveaus beizutragen und dadurch negative materielle und immaterielle Folgen für die Stadtverwaltung Hamm zu vermeiden. Alle Mitarbeitenden sind sich ihrer Verantwortung beim Umgang mit Informationen und Informationstechnik bewusst und unterstützen die Sicherheitsstrategie nach besten Kräften.

4 Schutzziele in der Informationssicherheit

Zur Abbildung des hohen Stellenwertes der Informationssicherheit werden für die Stadtverwaltung die nachstehenden Sicherheitsziele festgelegt, für die geeignete Sicherheitsniveaus definiert werden:

- Vertraulichkeit: Informationen dürfen ausschließlich einem berechtigten Personenkreis zur Verfügung stehen.
- Integrität: Die physische und logische Unversehrtheit von Systemen, Anwendungen und Daten muss jederzeit gewahrt sein. Dieses umfasst auch die unberechtigte Erstellung oder Änderung von Informationen.
- Verfügbarkeit: Systeme, Anwendungen und Daten müssen den Berechtigten in jeder Situation wie vorgesehen zur Verfügung stehen.

5 Sicherheitsstrategie

Die Sicherheitsstrategie der Stadtverwaltung Hamm ist es, mit wirtschaftlichem Ressourceneinsatz ein risikoangemessenes Sicherheitsniveau zu erreichen und aufrechtzuerhalten.

Die Stadtverwaltung Hamm betreibt zur Wahrung ihrer Aufgaben ein ISMS. Dieses dient dazu, die Informationssicherheit zu definieren, zu steuern, zu kontrollieren, aufrechtzuerhalten und fortlaufend zu verbessern.

Die Umsetzungsstrategien sind in entsprechenden Richtlinien und Verfahrensanweisungen dokumentiert.

Im Rahmen der Strategie wird ein Informationssicherheitsmanagementprozess eingeführt, der sich an der IT-Grundschutzvorgehensweise des Bundesamtes für Sicherheit in der Informationstechnik (BSI) orientiert und als kontinuierlicher Prozess nach dem PDCA-Zyklus gestaltet wird:

- Plan: Festlegung der Vorgaben für den Sicherheitsprozess und das ISMS
- Do: Aufbau eines ISMS, Erstellung und Umsetzung eines Sicherheitskonzepts sowie Etablierung des Sicherheitsprozesses
- Check**:** Erfolgskontrolle zur Erreichung der Sicherheitsziele
- Act**:** Durchführung von Korrekturen zur Optimierung des Sicherheitsprozesses und der Sicherheitsorganisation

Die Sicherheitsstrategie umfasst die gesamte Informationsverarbeitung in der Stadtverwaltung. Das ISMS soll dem jeweiligen Schutzbedarf entsprechend angemessene Sicherheitsmaßnahmen definieren und für deren Umsetzung sorgen. Bei der Auswahl von Sicherheitsmaßnahmen ist darauf zu achten, dass das erforderliche Sicherheitsniveau erreicht wird, ohne den Ablauf von Geschäftsprozessen / Fachaufgaben unnötig zu beeinträchtigen.

Die Sicherheitsstrategie wird von den folgenden Grundsätzen geprägt:

- Zentrale Rolle der Informationssicherheit:
  Die Informationssicherheit und der Datenschutz werden bei Änderungen und Neuerungen von Beginn an mitberücksichtigt.

- Verhältnismäßigkeit der Sicherheitsmaßnahmen:
  Aufwand und Ergebnis der eingesetzten Sicherheitsmaßnahmen müssen in einem angemessenen Verhältnis zueinanderstehen.

- Sicherheit für nachhaltige Verfügbarkeit:
  Um eine langfristige Verfügbarkeit zu erreichen, sind kurzfristige oder geringfügige Einschränkungen bei Funktionalität und Komfort vertretbar.

- Prinzip des Schutzbedarfs:
  Zweck der Schutzbedarfsfeststellung ist es, zu ermitteln, welcher Schutz für die Geschäftsprozesse und Fachaufgaben ausreichend und angemessen ist. Zu berücksichtigen sind stets die dabei verarbeiteten Informationen sowie die eingesetzte Informationstechnik. Hierzu werden für jeden Vorgang, jede Anwendung und die dabei verarbeiteten Informationen die zu erwartenden Schäden betrachtet, die bei einer Beeinträchtigung der Sicherheitsziele entstehen können. Wichtig ist es dabei auch, die möglichen Folgeschäden sowie Risiken für die Rechte und Freiheiten natürlicher Personen realistisch einzuschätzen.

- Minimalprinzip des Zugriffs:
  Der Zugriff auf IT-Systeme und Daten wird auf die notwendigen Personen und Systeme beschränkt.

- Restriktives Nutzungsprinzip:
  Es werden nur Berechtigungen erteilt, die zur Erfüllung der jeweiligen Aufgabe tatsächlich benötigt werden.

- Bereitstellung von ausreichenden Ressourcen:
  Um ein angemessenen Sicherheitsniveaus zu erreichen und aufrecht zu erhalten, werden ausreichende finanzielle und personelle Ressourcen bereitgestellt.

- Einbindung aller Bediensteten:
  Alle Bediensteten werden in den Sicherheitsmanagementprozess zur Unterstützung der Sicherheitsstrategie eingebunden und hinsichtlich der Informationssicherheit sensibilisiert.

6 Umsetzung der Informationssicherheitsleitlinie

Die/der Oberbürgermeister:in stellt im erforderlichen Rahmen Personal- und Finanzmittel bereit, um ein angemessenes Informationssicherheitsniveau bei der Verarbeitung schützenswerter Informationen sicher zu stellen. Die Sicherheitsmaßnahmen müssen in einem wirtschaftlich vertretbaren Verhältnis zum Schaden stehen, der durch Sicherheitsvorfälle verursacht werden kann und zur dadurch erzielten Schutzwirkung.

Diese Maßnahmen und deren Auswirkungen ergeben sich aus dem etablierten Risikomanagement zur Informationssicherheit, welches in der Richtlinie zum Risikomanagement beschrieben ist.

Es werden regelmäßig und bedarfsgerecht Schulungs- und Sensibilisierungsmaßnahmen angeboten, die sich an alle Beschäftigten richten. Zusätzlich werden interne Medien, insbesondere die Mitarbeiterzeitschrift und das Intranet, für regelmäßige und anlassbezogene Informationsweitergabe verwendet.

7 Verpflichtung zur kontinuierlichen Verbesserung

Durch ständige Weiterentwicklungen von gesetzlichen, technischen und organisatorischen Gegebenheiten ist die Informationssicherheit kein unveränderlicher Zustand. Diesen Entwicklungen müssen sich die Ansätze zum Management der Informationssicherheit anpassen. Aus diesem Grund trägt die/der ISB dafür Sorge, dass die Sicherheitsstrategie kontinuierlich weiterentwickelt wird.