Stadtrat der Stadt Frankenthal (Pfalz)

XVII. Wahlperiode 2019 – 2024

Drucksache Nr.

XVII/3128

Aktenzeichen: 10/B/Wa Datum: 17.03.2023 Hinweis:

Beratungsfolge: Stadtrat

IT-Sicherheit in der Verwaltung

Die Verwaltung bittet zu beschließen wie folgt:

1. Das vorgelegte Konzept zur IT-Sicherheit „Leitlinie zur Informationssicherheit in Frankenthal“ wird genehmigt.

2. Zur Durchführung eines Pen-Tests werden Mittel in Höhe von 10.000 € in den Haushalt eingestellt.

3. Zur Durchführung notwendiger weiterer Sicherheitsmaßnahmen werden jährliche Mittel in Höhe von 22.000 € in den Haushalt eingestellt.

4. Für die notwendigen Aufgaben der Informationssicherheit wird eine neue Stelle Informationssicherheitsbeauftragte/-r (E 11) in den Stellenplan aufgenommen.

Beratungsergebnis:

Gremium	Sitzung am	Top	Öffentlich:		Einstimmig:		Ja-Stimmen:	
					Mit		Nein-Stimmen:	
			Nichtöffentlich:		Stimmenmehrheit:		Enthaltungen:	

Laut Beschluss-vorschlag:	Protokollanmerkungen und Änderungen	Kenntnisnahme:	Stellungnahme der Ver-waltung ist beigefügt:	Unterschrift:
	siehe Rückseite:			

Begründung:

Die Informationstechnologie hat in den vergangenen Jahrzehnten eine zunehmende strategische Bedeutung für die Erfüllung aller anfallenden Aufgaben und Prozesse gewonnen.

Durch die intensive Durchdringung und die hierdurch erwachsende Abhängigkeit ist auch das Eintreten eines nennenswerten oder sogar großen Schadens im Falle eines Ausfalls, egal ob dieser technisch oder durch einen externen Angriff erfolgt ist, eine ständig wachsende Gefahr.

Neben dem fiskalischen Risiko birgt ein Ausfall der Datenverarbeitung, und somit eine Einschränkung des Dienstbetriebs, auch den nicht bezifferbaren Schaden des Vertrauensverlustes bei den Bürgerinnen und Bürgern.

Dies hat sich in den vergangenen Jahren in mehreren praktischen Beispielen (Bitterfeld, Rhein-Pfalz-Kreis, KSB, IHK) gezeigt, bei welchen den Kommunen und Firmen durch externe Angriffe nicht nur Schaden zugefügt wurde, sondern zum Teil auch Einwohnerdaten im sogenannten "Darknet" veröffentlicht wurden.

Die potentiellen Gefahrenquellen werden durch die aktuellen technischen Entwicklungen einer zunehmenden Zentralisierung, dem wachsenden Austausch von Daten durch das Onlinezugangsgesetz und dem rasant zunehmenden Kommunikationsmöglichkeiten über diverse Social-Media-Kanäle und Videoplattformen immer zahlreicher und schwerer abzusichern.

Aus diesem Grund gewinnt neben dem Themenbereich Datenschutz auch zunehmend der Komplex Informationssicherheit einen immer höheren Stellenwert in im Bereich der Datenverarbeitung.

Derzeit gibt es Bestrebungen der Gesetzgeber, auch die Kommunen zur kritischen Infrastruktur zu erklären, um damit einhergehend einen hohen Schutzbedarf zu fordern.

Kommunalverwaltungen sind auch bisher verpflichtet, ihre IT-Systeme und Verwaltungsvorgänge durch technische und organisatorische Maßnahmen ausreichend abzusichern, auch wenn keine unmittelbare Verpflichtung zur Umsetzung speziell des IT-Grundschutzes aus einer Rechtsnorm abgeleitet werden kann. Diese Verpflichtungen ergibt sich u.a. aus datenschutzrechtlichen Anforderungen (u. a. EU-Datenschutz-Grundverordnung; BDSG; LDSG rlp).

Zur Umsetzung der zwingend notwendigen Maßnahmen werden zusätzliche personelle Ressourcen (Benennung eines Informationssicherheitsbeauftragten) und finanzielle Mittel (Beschaffung einer Lernplattform, Durchführung von Penetrationstests in regelmäßigen Abständen, Zertifizierung / Rezertifizierungen) benötigt.

Nach einer ersten Schätzung für notwendige Einzelmaßnahmen wurde folgender vorläufiger Kostenrahmen ermittelt:

Durchführung eines Pen-Tests (Durchführung alle zwei Jahre)	zweijährlich ca. 10.000,00 €
Anmietung einer Lernplattform für die Verwaltung	jährlich ca. 12.000,00 €

Durchführung einer Zertifizierung sowie der notwendigen Rezertifizierungen	jährlich ca. 5.000,00 €
Bedarfsweise externe Beratung für die Härtung besonders sensibler Bereiche oder neuer Techniken	jährlich ca. 5.000,00 €

Im Weiteren ist die Schaffung einer Stelle „Informationssicherheitsbeauftragte/-r“ (vorbehaltlich einer Stellenbewertung mit einer Wertigkeit der tariflichen Eingruppierung in EG11) notwendig.

Der Kostenanforderung sowie dem Antrag auf Stellenmehrung liegen folgende Maßnahmen zu Grunde:

Derzeitiger Stand im Bereich Informationssicherheit / Datenschutz

Dem Datenschutz und der Informationssicherheit wird ein sehr hoher Stellenwert beigemessen. Da ein hoher Datenschutz ohne hohe Informationssicherheit nicht realisierbar ist, wird auf interne und externe Schutzmaßnahmen zur Absicherung der Datenverarbeitung Wert gelegt.

Nach IT-Grundschutz des Bundesamts für Sicherheit in der Informationstechnik (BSI) muss sowohl bei der Umsetzung der Informationssicherheit als auch bei der Steuerung des Notfallmanagements die Initiative von der Leitung einer Institution ausgehen.

Die Verwaltungsführung hat diese zuletzt mit der Leitlinie zur Informationssicherheit in Frankenthal **(Stand Januar 2021; siehe Anlage**) übernommen. Diese beginnt technisch mit Sicherheitsmaßnahmen im Bereich der Server- und Endgerätesicherheit und der internen und externen Absicherung des Netzwerks.

Sie greift aber auch organisatorisch, unter anderem auf der Ebene der Nutzerinnen und Nutzer durch Beschränkung der Rechte und Sensibilisierung für die Thematik.

Die Leitlinie zur Informationssicherheit in Frankenthal wird fortlaufend evaluiert und fortgeschrieben.

Ergänzende Maßnahmen sind in den technischen und organisatorischen Maßnahmen zur Umsetzung der Informationssicherheit gemäß Artikel 32 DSGVO ausgeführt.

Bereits seit einigen Jahren strebt die Verwaltung eine vollständige Dokumentation und Zertifizierung der Basisabsicherung nach BSI-Grundschutz an und hat in den vergangen zwei Jahren erhebliche Zeitanteile zur Umsetzung der dazu notwendigen BSI-Bausteine bereitgestellt.
Die Umsetzung und Dokumentation der Basisabsicherung wurde zum Stand März 2023 zu ca. 65% abgeschlossen.

Weiterhin befinden sich derzeit alle maßgeblichen Richtlinien und Konzepte in der Überprüfung und Überarbeitung. Bedingt durch personelle Engpässe und die pandemiebedingten Einschränkungen bei der Bearbeitung konnte eine weitergehende Vervollständigung bislang nicht erfolgen.

Die schriftliche Dokumentation aller getroffenen Maßnahmen, deren regelmäßige Evaluation und die Fortschreibung bei Änderungen ist die grundlegende Basis für die Etablierung eines Informations-Sicherheits-Management-Systems (ISMS) nach IT-Grundschutz des BSI.

Im Bereich der Überprüfung der bestehenden Absicherung wurde im November 2021 ein sogenannter Penetrationstest des Verwaltungsnetzwerks durch eine externe Sicherheitsfirma beauftragt. Dieser wurde sowohl als externer als auch als interner Test durchgeführt.

Dabei wurde der Verwaltung eine gute Absicherung der IT bescheinigt. Dies ist jedoch keine Garantie für einen vollständigen Schutz gegen potentielle Angriffe von innen oder außen.

Gewünschter Sollzustand im Bereich Informationssicherheit / Datenschutz;
Aktive Sicherheit

Die Stadtverwaltung Frankenthal hat sich zum Grundsatz gemacht, dass die Sicherheit und der Schutz von Daten und Informationen Vorrang vor der Bequemlichkeit der Nutzerinnen und Nutzer haben muss. Es ist der Verwaltung bewusst, dass hierdurch die Nutzung bestimmter Dienste, bzw. der Ablauf von Prozessen einen höheren personellen Aufwand mit sich bringen kann.

Um eine möglichst hohe und bedarfsgerechte Umsetzung des Schutzes für die zu verarbeitenden Daten zu gewährleisten, ist die Realisierung aller wirtschaftlich abbildbaren Sicherheitsmaßnahmen nach dem aktuellen Stand der Technik notwendig.

Diese Schutzmaßnahmen sind regelmäßig, auch durch unabhängige Prüfer, zu evaluieren um gegebenenfalls neue Angriffsszenarien zu erkennen und notwendige Verbesserungsmöglichkeiten umsetzen zu können.

Dazu gehört auch die regelmäßige Wiederholung von Penetrationstests durch spezialisierte externe Sicherheitsfirmen.

Zertifizierung auf der Basis des BSI - IT-Grundschutz

Es wird angestrebt bis zum Jahr 2025 eine offizielle Zertifizierung der Basisabsicherung nach BSI-Grundschutz zu erreichen. Sofern der Gesetzgeber die Kommunalverwaltungen zukünftig als kritische Infrastrukturen einstuft, ist der zu erreichende Mindeststandard entsprechend anzupassen.

Als ein Mittel zur Erreichung dieser Zielsetzung hat sich die Stadtverwaltung Frankenthal um die Teilnahme als Modellkommune für das Projekt "Neue Wege in dies Basis-Absicherung" des BSI unter Mitwirkung der kommunalen Spitzenverbände beworben.

Da eine solche Zertifizierung eine Gültigkeitsdauer von drei Jahren hat, sind regelmäßige Rezertifizierungen sowohl personell, als auch monetär einzuplanen. Der Aufwand reduziert sich nach der Erstzertifizierung, da die hierbei etablieren Prozesse

und Routinen des Informationssicherheitsmanagementsystems sicherstellen, dass die grundsätzliche Basis stets auf dem aktuellen Stand ist.

Sensibilisierung / Schulungsmaßnahmen für Mitarbeiterinnen und Mitarbeiter

Ein hoher Prozentsatz erfolgreicher Infiltrationen eines Netzwerks wird über unbedachtes oder versehentliches Auslösen einer Aktion durch eine Nutzerin / einen Nutzer verursacht.

Aus diesem Grund ist ein weiteres Standbein für die Verbesserung der IT-Sicherheit die Sensibilisierung und Schulung der Mitarbeiterinnen und Mitarbeiter zum verantwortungsvollen Umgang mit potentiell gefährlichen Nachrichten oder von extern überlassenen Daten.

Hierzu ist beispielsweise die Beschaffung eines Verfahrens zur Wissensvermittlung und Abfrage des Wissensstands eine mögliche Variante.

Benennung eines/einer Informationssicherheitsbeauftragten (ISB)
Nach IT-Grundschutz des BSI ist unter der Ebene der Unternehmensleitung ein/eine Informationssicherheitsbeauftragte/r zu benennen.

Dies wurde auch vom IT-Planungsrat in seiner "Handreichung zur Ausgestaltung der Informationssicherheitsrichtlinie in Kommunalverwaltungen" so formuliert. Zur Wahrung der Unabhängigkeit sollte der ISB direkt der Verwaltungsleitung zugeordnet sein.

Eine Integration in die IT-Abteilung soll nicht erfolgen, da es zu Rollenkonflikten führen kann. Der/die ISB kann die Verpflichtung zur Kontrolle der Sicherheitsmaßnahmen nicht frei von Beeinflussung wahrnehmen.

Eine Personalunion der Tätigkeiten Informationssicherheit und Datenschutz ist grundsätzlich aufgrund des notwendigen Fachwissens sowie der unterschiedlichen Handlungsfelder nicht zielführend, auch um Konflikte bei der Aufgabenwahrnehmung zu vermeiden.

Der/die ISB bildet gemeinsam mit dem/der Datenschutzbeauftragten und der IT-Abteilung das Informationssicherheits-Management-Team mit folgenden Aufgaben:

- Festlegung der Sicherheitsziele und -strategien sowie Weiterentwicklung der Leitlinie zur Informationssicherheit
- Überprüfung der Umsetzung der Sicherheitsleitlinie
- Initiierung, Steuerung und Kontrolle des Sicherheitsprozesses
- Mitwirkung bei der Entwicklung des Sicherheitskonzepts
- Überprüfung, ob die im Sicherheitskonzept geplanten Sicherheitsmaßnahmen geeignet und wie beabsichtigt wirksam sind.
- Konzeption von Schulungs- und Sensibilisierungsprogrammen für Informationssicherheit und Integration aller Mitarbeiter in den Sicherheitsprozess.
- Beratung der Fachverantwortlichen, der IT, sowie der Leitungsebene

Die Einrichtung einer eigenen Stelle für die Aufgaben der Informationstechnik ist erforderlich.

Notwendige Maßnahmen zur Zielerreichung

Ziel der weiteren Entwicklung ist das Erreichen des angestrebten Zielzustandes wird vor allem in den Standards BSI-200-1 (Managementsystem für Informationssicherheit ISMS) und BSI-200-2 (IT-Grundschutz-Methodik).

BSI-200-2 sieht mit der Umsetzung der Basis-Absicherung einen relativ kompakten Einstieg zur Initiierung eines Informations-Sicherheits-Management-Systems vor.

Zu dessen Umsetzung anhand des IT-Grundschutz-Profils „Basis-Absicherung Kommunalverwaltung“ sind bereits interne Maßnahmen angestoßen worden, die zu einem Umsetzungsgrad von 65% geführt haben.

Für einige weitere Schritte sind jedoch derzeit nicht vorhandene personelle und finanzielle Ressourcen notwendig.

Ergänzt werden die ersten beiden Standards durch BSI-200-3 (Risikomanagement), der bei der Etablierung der Standard-Absicherung nach BSI-200-2 relevant wird, sobald die Basis-Absicherung umgesetzt ist.

Bei BSI-200-1 handelt es sich um einen fortwährenden Prozess zur Erhaltung der Informationssicherheit, der stetig durchlaufen wird, mit dem Ziel der Aufrechterhaltung bzw. kontinuierlichen Verbesserung der Informationssicherheit.

Um Zustimmung zur Durchführung der konzeptionellen Maßnahmen, zur beantragten Mittelanmeldung sowie Schaffung einer Planstelle Informationssicherheit wird gebeten.

STADTVERWALTUNG FRANKENTHAL (PFALZ)

Martin Hebich
Oberbürgermeister

Anlage: Leitlinie zur Informationssicherheit in Frankenthal