Überörtliche Prüfung von Kommunen des Landes Sachsen-Anhalt

Querschnittsprüfung der Sicherheit der IT in den Kommunen

Stellungnahme der Stadt Aschersleben zu den Feststellungen und Schlussfolgerungen des Landesrechnungshofs

Auf die vom Landesrechnungshof geprüften Bereiche und die daraus resultierenden Feststellungen und Schlussfolgerungen nehmen wir als Stadt Aschersleben wie folgt Stellung:

1. Zertifizierung und Testierung

Stand heute ist der Informationsverbund der Stadt Aschersleben weder nach ISO-Standard 27001 zertifiziert, noch hat diese eine Testierung nach IT-Grundschutz bzw. von einer Basis-Absicherung gebraucht gemacht.

Die Stadt Aschersleben strebt allerdings ein Testat durch das BSI nach der Basisabsicherung gemäß dem IT-Grundschutz an. Um eine solche Testierung erfolgreich zu gestalten, sind verschiedenste Voraussetzungen zu erfüllen und etliche Maßnahmen innerhalb des Informationsverbundes zu realisieren. Die Stadt Aschersleben arbeitet bereits an den Voraussetzungen und an der Umsetzung der ersten Maßnahmen.

2. Leitlinie zur Informationssicherheit

Nachdem die Leitlinie zur Informationssicherheit durch alle relevanten Ämter innerhalb der Organisation der Stadt Aschersleben durchlaufen hat, wurde diese durch den HVB am 07.09.2023 freigegeben.

Informationssicherheitsziele und Grundsätze zur Informationssicherheit sind innerhalb der Leitlinie definiert worden. Eine regelmäßige Aktualisierung der Leitlinie zur Informationssicherheit ist vorgesehen und innerhalb der Leitlinie festgelegt (jährlich).

Die Leitlinie zur Informationssicherheit wird allen Beschäftigten innerhalb des Informationsverbundes bekannt gegeben (voraussichtlich in 10/2023). Die Bekanntmachung wird in Form einer E-Mail an alle Beschäftigten erfolgen. Die Bereitstellung der Leitlinie zur Informationssicherheit soll dabei zentral über das Intranet der Stadt Aschersleben erfolgen.

Aufgrund des Berichts des LRH wird in der ersten Überarbeitung der Leitlinie zur Informationssicherheit der noch nicht betrachtete Punkt der „politischen Gremien“ aufgenommen und betrachtet.

3. IT-Sicherheitskonzept

Das IT-Sicherheitskonzept für den Informationsverbund der Stadt Aschersleben ist grundsätzlich erstellt. Eine regelmäßige Aktualisierung des IT-Sicherheitskonzeptes ist vorgesehen (jährlich). Der Schutzbedarf wurde identifiziert und eine Risikoanalyse durchgeführt. Zudem wurden Sicherheitsmaßnahmen aus der Risikoanalyse abgeleitet.

Aufgrund des Berichts des LRH werden in den zukünftigen Aktualisierungen des IT-Sicherheitskonzeptes die folgenden Punkte neu betrachtet:

- Festlegung verbindlicher Fristen zur Umsetzung
- Politische Gremien

Weiterhin wird das Thema der Geschäftsprozesse aufgegriffen und dargestellt. Für das IT-Sicherheitskonzept wird dafür eine Prozesslandkarte erstellt. Der dafür notwendige Aufgabengliederungsplan ist aktualisiert worden und dient als Grundlage der Ermittlung und Darstellung der Kern- und Randprozesse innerhalb des Informationsverbundes der Stadt Aschersleben.

4. Dienstanweisungen, Informationsrichtlinien oder andere verbindliche Regelungen, Sicherheitsmechanismen

Verbindliche Regelungen zum Thema IT-Sicherheit werden bei der Stadt Aschersleben durch Dienstanweisungen und Richt- oder Leitlinien abgebildet.

Stand heute ist eine neue Dienstanweisung „Software“ in der Erstellungsphase, welche sich bereits am IT-Grundschutzkompendium des BSI orientiert und Bezug darauf genommen wird. Innerhalb dieser Dienstanweisung soll es in erster Linie um den Prozess der Softwarebeschaffung gehen, welcher Teil des System-Bausteins APP.6 des genannten IT-Grundschutz-Kompendiums ist.

Aufgrund des Berichts des LRH werden Regelungen zur elektronischen Post geprüft und ggf. neu betrachtet.

5. Informationssicherheitsbeauftragter (ISB)

Die Stadt Aschersleben hat einen Informationssicherheitsbeauftragten ernannt, welcher einen prozentualen Anteil seiner VzÄ von 30 Prozent hat. Zudem wurde ein Stellvertreter benannt. Der Informationssicherheitsbeauftragte ist dem HVB direkt unterstellt und kann ihm direkt berichten. Zudem wird der ISB bei allen größeren Projekten und bei der Einführung neuer Anwendungen und IT-Systeme frühzeitig beteiligt.

Die Bekanntgabe des ISB und seines Stellvertreters erfolgte über den Informationsbereich und der Auskunft im Intranet der Stadt Aschersleben. Weiterhin wird die Bekanntmachung innerhalb des Informationsverbundes der Stadt Aschersleben durch Informationsmails zu verschiedenen Themen und Maßnahmen verstärkt.

6. IT-Notfallkonzept

Das IT-Notfallkonzept für den Informationsverbund der Stadt Aschersleben ist grundsätzlich erstellt. Eine regelmäßige Aktualisierung des IT-Notfallkonzeptes ist vorgesehen (jährlich).

Im IT-Notfallkonzept sind Rollen und Sofortmaßnahmen beschrieben. Weiterhin sind die Kommunikationswege definiert und die kritischen Ressourcen identifiziert.

Das IT-Notfallkonzept sieht die Schaffung eines IT-Notfall-Teams vor, welches im Ernstfall dafür zuständig ist, den Überblick zu wahren und durch Handlungsanweisungen und beschriebenen Maßnahmen das weitere Vorgehen für alle Beteiligten aufzeigen soll.

Bereits seit einiger Zeit wird innerhalb des Informationsverbundes der Ernstfall einer Phishing-E-Mail geplant und durchgeführt. Dieses Szenario wird ausgewertet und Beschäftigte bereits gezielt geschult und auf das Bewusstsein solcher Szenarien sensibilisiert.

Aufgrund des Berichts des LRH werden in den zukünftigen Aktualisierungen des IT-Notfallkonzeptes die folgenden Punkte neu betrachtet oder erweitert und folgende Maßnahmen umgesetzt:

- Informationen zu Geschäftsfortführungsplänen
- Zugänglichkeit im Notfall
- Bekanntgabe des Konzeptes

- Testung der Notfallpläne
- Reaktions-/Abschaltpläne
- Geschäftsfortführungs-/Wiederanlaufpläne (BSI-Standard 100-4)

7. Identitäts- und Berechtigungsmanagement

Im Informationsverbund der Stadt Aschersleben sind Zugriffsberechtigungen vergeben. Zudem existieren Regelungen für den Entzug von Zugriffsrechten.

Im Rahmen des Identitäts- und Berechtigungsmanagement ist die Erstellung eines Berechtigungskonzeptes für den Informationsverbund Stadt Aschersleben vorgesehen. Dieses Konzept wird sich analog an das IT-Grundschutz-Kompendium, dem Baustein ORP.4 (Identitäts- und Berechtigungsmanagement) orientieren.

Aufgrund des Berichts des LRH werden in zukünftigen Aktualisierungen des Identitäts- und Berechtigungsmanagement die folgenden Punkte zusätzlich betrachtet:

- Schriftliche Regelung der Zugriffserforderlichkeit
- Dokumentation der Zugriffsrechte
- Kritische Überprüfung Super-User

8. Schutz vor Schadprogrammen

Der Einsatz von Schutzprogrammen innerhalb des Informationsverbundes der Stadt Aschersleben ist flächendeckend und im IT-Sicherheitskonzept schriftlich dokumentiert. Eine Aufklärung aller Beschäftigten über mögliche Bedrohungen findet statt.

Weiterhin sind die Mitarbeiter des EDV-Teams und der Informationssicherheitsbeauftragte als Ansprechpartner für den Fall eines Verdachts auf Infektion mit Schadprogrammen im Informationsverbund bekannt gegeben.

In der zukünftigen Betrachtung des Themas Schadprogramme ist die Dokumentation der Aufklärung der Benutzer über Schadprogramme vorgesehen.

9. Deaktivierung und Deinstallation

Im Informationsverbund der Stadt Aschersleben werden nicht benötigte Programme deaktiviert und/oder deinstalliert. Dies gilt auch für nicht mehr benötigte Funktionen und/oder Module einer Software.

10. Wartung von IT-Systemen – Umgang mit Updates

Das regelmäßige Kontrollieren auf Updates für die im Informationsverbund eingesetzten Programme sowie das zeitnahe sowie regelmäßige Aktualisieren dieser ist bei der Stadt Aschersleben gegeben. Weiterhin ist die Verantwortlichkeit für die regelmäßige Information über relevante Updates geregelt. Dies erfolgt Gruppenweise via E-Mail bei den Fachapplikationen.

Aufgrund des Berichts des LRH wird in der zukünftigen Betrachtung des Änderungsmanagements und Updates der folgende Punkt zusätzlich betrachtet:

- Dokumentation der Updates

11. Datensicherung – Backup

Bei der Stadt Aschersleben gibt es niedergeschriebene Festlegungen zur Verfahrensweise für die Datensicherung, wenn es sich um zeitliche und mediale Rahmenbedingungen handelt. Diese sind Teil des IT-Sicherheitskonzeptes.

Regelmäßige Datensicherungen werden durchgeführt, dazu gehören auch Offline-Backups. Die Offline-Backups werden dabei in unterschiedlichen Brandabschnitten gelagert.

Aufgrund des Berichts des LRH wird in der zukünftigen Betrachtung des Themas Datensicherung - Backup der folgende Punkt zusätzlich betrachtet:

- Erstellung Minimaldatensicherungskonzept

12. Infrastruktursicherheit – Serverräume

Die Serverräume im Informationsverbund der Stadt Aschersleben sind vor unberechtigten Zutritt gesichert. Die Dokumentation der Berechtigung des Zutritts (Schlüsselvergabe) ist Teil des IT-Sicherheitskonzeptes.

13. Personal

13.1 Personalausstattung im IT-Bereich

Die Personalausstattung im IT-Bereich der Stadt Aschersleben beträgt Stand heute 4,25 VzÄ.

Regelmäßige Organisationsuntersuchungen zum Personalschlüssel in der EDV gibt es nicht. Die Personal-Thematik im IT-Bereich wird aber in zeitlichen Abständen mit den Führungsebenen diskutiert.

13.2 Vertretungsregelungen im IT-Bereich

Vertretungsregelungen im IT-Bereich der Stadt Aschersleben sind festgelegt und definiert. Die Regelungen sind schriftlich dokumentiert. Zudem gibt es einzelne Vertretungen für verschiedene Tätigkeiten.

Aufgrund des Berichts des LRH wird in der zukünftigen Betrachtung des Themas Vertretungsregelungen im IT-Bereich folgender Punkt zusätzlich betrachtet:

- Ausschluss von Generalvertretungen aller IT-Mitarbeiter

13.3 Fortbildung/Schulung und Sensibilisierung zur IT-Sicherheit

Für die IT-Mitarbeiter der Stadt Aschersleben gibt es grundsätzlich Fortbildungen und Schulungen. Dazu gehört auch das Thema der IT-Sicherheit. Stand heute gibt es zur IT-Sicherheit gezielte Fortbildungen (Firewall, Hacking etc.) für die IT-Mitarbeiter, welche aber nicht verpflichtend sind. Dennoch ist es das Ziel, das jeder IT-Mitarbeiter mindestens einmal im Jahr eine Fortbildung im IT-Bereich absolviert.

Für die Beschäftigten innerhalb des Informationsverbundes werden grundsätzlich keine Schulungen oder Fortbildungen zum Thema IT-Sicherheit angeboten. Schulungen, Belehrungen sowie Informationen über das genannte Thema werden durch die IT-Mitarbeiter im Verbund vorgenommen. Dazu gehört auch die ständige Sensibilisierung aller Mitarbeiter im Einzelnen oder in Gruppen.

Aufgrund des Berichts des LRH werden in der zukünftigen Betrachtung des Themas Schulung und Belehrung der Mitarbeiter zur IT-Sicherheit folgende Punkte zusätzlich betrachtet:

- Regelmäßige Schulung sonstiger Mitarbeiter
- Verpflichtende Schulung IT-Mitarbeiter

14. IT-Prüfung durch das Rechnungsprüfungsamt (RPA)

Das RPA der Stadt Aschersleben führt Stand heute keine Prüfungen der IT bzw. EDV durch.

Der LRH empfiehlt den Kommunen, eine regelmäßige Prüfung der IT-Sicherheit durch das zuständige RPA zu veranlassen.

An dieser Stelle bitten wir den LRH um Unterstützung bei den folgenden Themen:

- Bereitstellung eines Leitfadens für die Prüfung durch das RPA vom LRH
- Bereitstellung einer Vorlage für einen Prüfbericht

15. Interkommunale Zusammenarbeit

Die Stadt Aschersleben arbeitet bereits seit einigen Jahren mit anderen Kommunen, der KITU und externen Dienstleistern auch im Bereich der IT-Sicherheit zusammen.

Abschlusshinweis:

Bitte um Rückmeldung, welche Dokumente erneut und/oder zur erstmaligen Prüfung durch den LRH durch die Stadt Aschersleben vorgelegt werden sollen.