Landeshauptstadt Mainz

Antwort zur Anfrage Nr. 1842/2023 der SPD-Stadtratsfraktion betreffend **IT-Sicherheit der Landeshauptstadt Mainz (SPD)**

Die Anfrage wird wie folgt beantwortet:

Unlängst waren mehrere dutzend Kommunen in Nordrhein-Westfalen von einem Hacker-Angriff in Form einer Ransomware-Attacke betroffen. Auch in Rheinland-Pfalz war einige Kommunen in der Vergangenheit von ähnlichen Angriffen betroffen.

Vor diesem Hintergrund fragen wir die Verwaltung:

1. **Welche Sicherheitsmaßnahmen und -protokolle sind derzeit in der IT-Infrastruktur der Landeshauptstadt Mainz implementiert, um den Schutz vor Cyberangriffen zu gewährleisten?**

   Die Landeshauptstadt Mainz richtet ihre Sicherheitsmaßnahmen an den Vorgaben des Bundesamtes für Sicherheit in der Informationstechnik (BSI) aus. Diese Vorgaben halten ein Bündel von Maßnahmen bereit, die im sogenannten IT-Grundschutzkompendium beschrieben und deren Anwendung durch die BSI Standards 200-1 bis 200-3 geregelt sind. Insbesondere verweist die Verwaltung auf die erlassene Informationssicherheitsleitlinie (ISSL) der Landeshauptstadt Mainz. In dieser bekennt sich die Behördenleitung zur Einhaltung der Informationssicherheit und legt die Grundsätze, Sicherheitsziele und Maßnahmen fest.

2. **Gibt es regelmäßige externe Sicherheitsaudits und -überprüfungen, um die Wirksamkeit der aktuellen Sicherheitsmaßnahmen zu evaluieren? Wenn ja, in welchen zeitlichen Abständen finden diese statt?**

   Die Stadtverwaltung Mainz bezieht ihre IT-Dienstleistungen grundsätzlich von ihrem Eigenbetrieb Kommunalen Datenzentrale Mainz (KDZ Mainz). Die KDZ Mainz ist für den Betrieb zentraler Fachverfahren (z.B. Einwohnermeldewesen, Schulverwaltungsverwesen, Personenstandswesen) nach BSI-Grundschutz zertifiziert. Um die Zertifizierung aufrecht zu erhalten, finden wiederholt interne und externe Audits statt. Darüber hinaus werden regelmäßig Sicherheitsüberprüfungen (z.B. durch Penetrationstests) durchgeführt. Ferner wird das Informationssicherheitsmanagementsystem (ISMS) im Zuge der kontinuierlichen Verbesserung regelmäßig überprüft (vgl. Pkt. 8 der ISSL).

3. **Welche Maßnahmen sind vorhanden, um auf etwaige Sicherheitsvorfälle schnell und effizient zu reagieren? Gibt es einen Notfallplan für den Umgang mit Cyberangriffen?**

Die KDZ Mainz hat Richtlinien zur Behandlung von Sicherheitsvorfällen erlassen. Darüber hinaus bespricht der Arbeitskreis Informationssicherheit (AKIS) etwaige Sicherheitsvorfälle, um im Rahmen der kontinuierlichen Verbesserung, die getroffenen Maßnahmen ggf. zu erweitern. Die Verwaltung hat zudem reagiert und eine Stelle des Beauftragten für Krisenmanagement / Business Continuity Management beim Hauptamt geschaffen, der gemeinsam mit dem Informationssicherheitsbeauftragten (ISB) das Notfallmanagement sowie die Aufrechterhaltung der Daseinsfürsorge koordiniert.

4. **Welcher weiteren externen Beratungsleistungen und Expertisen bedient sich die Landeshauptstadt Mainz bei der ständigen Weiterentwicklung Ihrer Maßnahmen zur IT-Sicherheit?**

   Die Landeshauptstadt Mainz wird unterstützt durch das CERT-kommunal-rlp (Computer Emergency Response Team) bzgl. Sicherheitswarnungen und Schwachstellenmeldungen. Darüber hinaus nimmt der ISB regelmäßig an Netzwerktreffen der kommunalen Informationssicherheitsbeauftragten teil. Die Verwaltung wurde im Nachgang des Cyberangriffes auf die Stadtwerke Mainz durch eine externe Sicherheitsuntersuchung beraten, um ihre Sicherheitsmaßnahmen zu bewerten. Ferner hat die KDZ Mainz eine externe Beratung zur regelmäßigen Unterstützung beauftragt.

Mainz, 23.11.2023

gez.

Nino Haase
Oberbürgermeister