Landeshauptstadt
Mainz

Antwort zur Anfrage Nr. 1644/2021 der Stadtratsfraktion PIRATEN & VOLT betreffend **IT-Sicherheit der städtischen Verwaltung / Schutz vor Ransom-Ware-Attacken (Piraten & Volt)**

Die Anfrage wird wie folgt beantwortet:

1. **Wie bewertet die Verwaltung insgesamt das aktuelle Schutzniveau der IT-Systeme der Stadt Mainz vor technischen Angriffen zur Sabotage, Informationsgewinnung oder Erpressung?**

Die Stadtverwaltung Mainz erachtet sich aus technischer Sicht gut aufgestellt, um den Risiken von Ransom-Ware-Attacken begegnen zu können. So sind durch den städtischen IT-Dienstleister und Eigenbetrieb KDZ Mainz, der für den Hostingbetrieb auch durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) zertifiziert ist, verschiedene Sicherheitsmaßnahmen in der Infrastruktur getroffen worden, die bislang erfolgreich die Stadt Mainz vor Angriffen schützen konnten. Auf organisatorischer Ebene wird versucht, durch Maßnahmen wie Phishingtests, Awareness-Kampagnen, Fortbildungen und Newsletter die Mitarbeiterschaft für die Gefahren der heutigen Informationsgesellschaft zu sensibilisieren. Das aktuelle Schutzniveau der IT-Systeme wird seitens der Verwaltung als gut bewertet.

2. **Welche Konzepte, Maßnahmen und Prozesse existieren zum Schutz der IT-Infrastrukturen der Stadt? Entsprechen diese Konzepte aktuellen ISO-Normen und können öffentlich einsehbar gemacht werden?**

Spätestens durch die BSI-Zertifizierung der KDZ wurden notwendige Konzepte für den Betrieb als IT-Dienstleister realisiert. Die Verwaltung orientiert sich stark am BSI IT-Grundschutz, strebt aber keine eigene BSI-Zertifizierung an. 2018 wurde auf Basis des BSI Grundschutzkompendiums das Grundschutzprofil Kommunal veröffentlicht. Dieses Profil enthält die Mindestanforderungen an die Informationssicherheit in Kommunen. Die Verwaltung hat entschieden, dass diese Anforderungen umgesetzt werden und lässt dies durch eine externe Beratung prüfen. Zum Schutz der Informationssicherheit und um potenziellen Angreifern keine Ansatzpunkte für Angriffe bieten zu können, werden Konzepte natürlich nicht öffentlich gemacht. Im Rahmen der BSI-Zertifizierung hat die KDZ Mainz entsprechende Konzepte, Richtlinien und Dienstanweisungen verabschiedet, an denen sich die Stadt Mainz orientiert. Ebenfalls wurden die technischen und organisatorischen Maßnahmen nach Art. 32 der Datenschutz-Grundverordnung (DSGVO) gemeinsam von Verwaltung und KDZ Mainz dokumentiert. Die Verwaltung und die KDZ Mainz stehen im engen Austausch und sicherheitsrelevante Themen werden im städtischen Arbeitskreis für Informationssicherheit (AKIS) gemeinsam besprochen. Weiterhin ist die KDZ Mainz Mitglied im CERT Kommunal (Computer Emergency Response Team) und erhält regelmäßig Warnungen und Informationen zu sicherheitsrelevanten Themen.

3. **Welche Notfallpläne existieren für den Fall eines größeren Angriffs auf die IT-Systeme der Stadt?**

Für den Fall eines größeren Angriffs existieren die im Rahmen der o. g. BSI-Zertifizierung notwendigen Vorgaben. Die KDZ Mainz hat ein Notfallmanagement mit entsprechenden Konzepten, welches auch auf die Stadt Mainz angewandt wird. Es existiert ein Alarmierungskonzept für die Stadt Mainz und im KDZ-eigenen internen Wissensmanagement sind Handlungsanweisungen für den Notfall dokumentiert (beispielsweise für einen Rechenzentrums-Shutdown). Diese Konzepte können aus Sicherheitsgründen nicht öffentlich gemacht werden.

4. **Existieren definierte Prozesse dafür, welche Ämter und Behörden im Notfall eingebunden werden?**

Ja, es gibt definierte Prozesse, wie im Falle eines Sicherheitsvorfalles von der ersten Meldung bis hin zur abschließenden Bewältigung des Vorfalles umgegangen wird und welche Stellen wann eingeschaltet werden (Alarmierungskonzept/Notfallkonzept).

5. **Nimmt die Stadt Beratung zum Thema IT-Sicherheit in Anspruch z.B. durch das Bundesamt für Sicherheit in der Informationstechnik (BSI), andere Behörden oder Privatfirmen? Wenn ja durch wen und was sind die Resultate dieser Beratung?**

Die Stadt Mainz nimmt zu Beratungszwecken, zur BSI-Zertifizierung, aber auch für Penetrationstests Leistungen von qualifizierten Dienstleistern in Anspruch. Im Rahmen der o. g. BSI-Zertifizierung und der damit verbundenen Auditierung nimmt die KDZ Mainz ebenfalls Leistungen von Externen in Anspruch. Zudem werden in der KDZ Mainz regelmäßig interne Audits zu den verschiedensten Themen durchgeführt. Zur Beratung beim Sicherheitsprozess der KDZ Mainz ist eine externe Fachfirma beauftragt. Die Resultate der Beratung sind sehr zufriedenstellend. Natürlich versucht sich die KDZ Mainz durch die Ergebnisse der Beratung stetig zu verbessern und den Prozess der IT-Sicherheit zu überprüfen und zu optimieren. Einzelergebnisse können aus Gründen der IT-Sicherheit nicht bekannt gegeben werden.

6. **Welcher Anteil der von der Stadt Mainz genutzten Softwaresysteme wird selbst gehostet oder extern betrieben (im Sinne von Sicherstellung der Anwendungssicherheit durch Externe)?**

Annähernd 100 % der von der Stadt Mainz genutzten Softwaresysteme werden selbst gehostet. Eine Ausnahme bietet beispielsweise das kommunale Waffenwesen, welches durch die Stadt Kaiserslautern gehostet wird.

7. **Finden regelmäßige Penetrationstests gegen die Systeme der Stadt statt, um Sicherheitslücken frühzeitig selbst - und vor der Entdeckung durch Kriminelle - zu erkennen? Wenn ja, welche Erkenntnisse zieht die Verwaltung aus den Resultaten dieser Tests?**

Ja, es werden immer wieder Penetrationstest gegen städtische Systeme durchgeführt und mögliche aufgezeigte Schwachstellen bewertet und behoben. Bei jeder Anwendung, die aus dem Internet erreichbar ist, wird vor Inbetriebnahme ein Penetrationstest durchgeführt. Jährlich finden allgemeine Tests und Überprüfungen durch das städtische Revisionsamt im Rahmen der IT-Revision statt. Sollten Penetrationstests nicht erfolgreich sein, wird die Anwendung so lange nicht produktiv eingesetzt, bis die negativen Ergebnisse behoben werden.

8. **Wie ist die Stadt Mainz vorbereitet auf Angriffe durch sog. Ransom-Ware-Attacken? Welche Handlungsoptionen zieht die Verwaltung für den Fall einer erfolgreichen Ransom-Ware-Attacke in Betracht?**
9. **Inwiefern berücksichtigt die städtische Backup-Strategie die größer werdenden Gefahren durch Ransomware-Attacken?**

Die Verwaltung ergreift selbstverständlich allgemeine Schutzmechanismen gegen Viren und sonstige Angriffe - nähere Informationen zu unserer Schutzstrategie können aus Sicherheitsgründen nicht offengelegt werden. Vor allem werden die angegriffenen und beeinträchtigten Bereiche isoliert, die Hardware wird bereinigt und Daten aus der Datensicherung werden wiederhergestellt.

10. **Verwendet die Stadt Mainz ausschließlich Software und Hardware, die noch mit Sicherheitsupdates versorgt wird und bei der so gewährleistet ist, dass entdeckte Sicherheitslücken unverzüglich geschlossen werden? Falls nein: Was sind die Gründe dafür und gibt es in jedem Fall zumindest Pläne, um möglichst bald Abhilfe zu schaffen?**

Es wird möglichst nur Soft- und Hardware eingesetzt, die regelmäßig mit Sicherheitsupdates versorgt wird.
Sollte dies vom Hersteller nicht mehr gewährleistet werden können, sind die zuständigen Fachbereiche aufgefordert, im Rahmen einer Risikoabwägung den weiteren Umgang mit dem entsprechenden System festzulegen.
In der Regel erfolgt dann ein Systemaustausch. In allen sicherheitsrelevante Bereichen werden nur Produkte verwendet, die mit entsprechenden Sicherheitsupdates versorgt werden. Sollte es keine aktuellen Sicherheitsupdates geben und kein Systemaustausch möglich sein, werden entsprechende Sonderverträge mit dem Hersteller abgeschlossen.

Mainz, 19. November 2021

gez.
Michael Ebling
Oberbürgermeister