Landeshauptstadt
Mainz

Antwort zur Anfrage Nr. 1341/2015 der FDP-Stadtratsfraktion betreffend **Datensicherheit in Mainz (FDP)**

Die Anfrage wird wie folgt beantwortet:

1. Wie werden sensible Daten durch die Verwaltung geschützt?
In der Verwaltung existiert eine weitreichende technische IT-Sicherheitsinfrastruktur, die einem stetigen Weiterentwicklungs- und Verbesserungsprozess unterliegt.
Die große Bandbreite der kommunalen Produkte und Leistungen erfordert gleichfalls auch eine Vielzahl von individuellen organisatorischen Regelungen, welche die vorhandenen technischen Sicherheitsmaßnahmen der KDZ unterstützen. Diese manifestieren sich in Dienstanweisungen, Dienstvereinbarungen und Richtlinien für die Verwaltung sowie die KDZ, die für eine hohe IT-Sicherheit in der Nutzung der eingesetzten Computer und Kommunikationssysteme der Stadtverwaltung Mainz sorgen.

2. Welche zusätzlichen Sicherheitsmaßnahmen unternimmt die Verwaltung, um Hackerangriffe zu blockieren?
Siehe Antwort zu Frage 1.

3. Wie werden das Intranet und das WLAN im Rathaus bzw. Stadthaus geschützt?
Die Schutzmaßnahmen entsprechen dem Stand der Technik.
So werden städtischen Netze u. a. durch mehrstufige Firewalls gegen Angriffe von Außen geschützt.

4. Welche Lehren und Erkenntnisse zieht die Verwaltung aus den Hackerangriffen auf die Zulassungsstellen?
Durch den Hackerangriff waren keine von der Stadt Mainz betriebene IT-Systeme betroffen.
Der Angriff zielte auf ein Modul der Zulassungsstellensoftware (Wunschkennzeichen), welches nicht in der Stadt Mainz, sondern gemeinsam durch den Landesbetrieb Daten und Information (LDI) und den hessischen kommunalen IT-Dienstleister eKomm21 betrieben wird. Die städtische Zulassungsstelle greift auf diese Anwendung über gesicherte Verbindungen zu.
Dennoch hat die KDZ nach Bekanntwerden des Vorfalls die betroffenen IT-Systeme (PCs, die auf die Software zugreifen) sofort vom Netz genommen und sehr intensive Tests auf Schadsoftware durchgeführt. Es fand durch den Angriff keine lokale Infektion mit Schadsoftware auf Systemen in der Stadt Mainz statt.
Die Kommunikation zwischen Land und Kommunen (auch den Kommunen untereinander) bei Hackerangriffen oder ähnlichen Vorfällen muss optimiert werden. Hierzu hat die Stadt Mainz eine Initiative gestartet.

5. Wie werden die Räumlichkeiten der Verwaltung z. B. Lauschangriffe geschützt?
Da EDV- und TK-Systeme durch die KDZ selbst betrieben werden und hierfür eine weitreichende IT-Sicherheitsinfrastruktur besteht, wird hier kein größeres Gefahrenpotenzial gesehen.
Ergänzend existieren Vorgaben der entsprechenden Hausverwaltungen, dass beim Verlassen von Räumlichkeiten, diese zu verschließen sind. Einen Lauschangriff über private Endgeräte, z. B. Smartphones, die von Mitarbeitern, Bürgern und sonstigen Personen mit in die dienstlichen

Räumlichkeiten gebracht werden, sieht die Verwaltung als höheres Risiko, steht diesem aber ohne Handhabe gegenüber.

6. Bestehen Erkenntnisse, ob sensible Daten durch den Hackerangriff geklaut wurden?
In der Stadtverwaltung Mainz wurden durch diesen Hackerangriff keine sensiblen Daten gestohlen.

7. Wie werden Mitarbeiter, Stadtvorstand und Ratsmitglieder für dieses Thema sensibilisiert und welche Fortbildungen werden diesen angeboten?
Mitarbeiterinnen und Mitarbeiter werden seit mehreren Jahren immer wieder mittels Newsletter, Artikeln in der Mitarbeiterzeitung sowie durch die zuständigen EVPs (EVP -› EDV-Verbindungsperson in den Fachämtern) über den richtigen und sicheren Umgang mit IT-Technik informiert und unterrichtet. EVPs erhalten hierbei ihre notwendigen Informationen durch die KDZ per Mail oder erweitern ihr Wissen auf regelmäßig stattfindenden Workshops. Hierbei treten diese dann als Multiplikatoren zu den Mitarbeiterinnen und Mitarbeitern auf. Künftig werden diese Sensibilisierungsmaßnahmen durch verschiedene weitere Maßnahmen (z. B. Plakataktionen, Awareness-Kampagnen, gruppenspezifische Schulungen etc.) noch verstärkt.
Ratsmitgliedern wurde eine Schulung zum sicheren Umgang mit den zur Verfügung gestellten mobilen Endgeräten (iPads) angeboten.

8. Sind der Verwaltung Angriffspunkte bekannt, mit denen Räumlichkeiten abgehört werden können, z. B. Lautsprecher?
Der Verwaltung sind derzeit keine kritischen Angriffspunkte bekannt, mit denen Räumlichkeiten abgehört werden können.
Es besteht zwar die theoretische Möglichkeit, dass die in städtischen Dienstgebäuden betriebenen Mikrofon- und Lautsprechersysteme missbräuchlich genutzt werden könnten, jedoch sind diese Systeme vom städtischen Datennetz getrennt und es gibt bislang keine Anhaltspunkte dafür, dass die Stadtverwaltung Mainz ein Ziel für derartige Angriffe sein könnte.

9. Sind in den letzten 12 Monaten - und wenn ja, was für welche - illegale Hackerangriffe durchgeführt worden?
Es finden täglich Angriffe auf die IT-Infrastruktur der Stadtverwaltung Mainz statt. Das ist nicht ungewöhnlich und betrifft gleichfalls auch Privatpersonen, wenn man alleine das Thema Schadsoftware und Phishing-Mails betrachtet.
In den letzten 12 Monaten sind keine gezielten Hackerangriffe durchgeführt worden. Aber die IT-Sicherheitsinfrastruktur der Stadtverwaltung Mainz nimmt täglich standardisierte sowie automatisierte Angriffe wahr und blockiert diese.

10. Plant die Verwaltung einen Belastungstest (beauftragter Hack) in Auftrag zu geben, um Lücken zu erkennen und zu schließen?
Die Stadtverwaltung lässt seit 2008 regelmäßig, ohne Wissen der KDZ, so genannte Penetrationstests durch externe IT-Spezialisten durchführen, um die eingesetzten Sicherheitsmaßnahmen auf ihre Wirkung überprüfen zu lassen. Aus den Ergebnissen dieser Tests werden wertvolle Erkenntnisse gewonnen, die unmittelbaren Einfluss auf die Sicherheitsmaßnahmen haben und somit die IT-Sicherheit weiter erhöhen.

Mainz, 13.Juli 2015

gez.
Michael Ebling