Landeshauptstadt
Mainz

Antwort zur Anfrage Nr. 1247/2015 der Stadtratsfraktion BÜNDNIS 90/DIE GRÜNEN betreffend
IT-Sicherheit bei der Stadt Mainz (GRÜNE)

Die Anfrage wird wie folgt beantwortet:

1. Gibt es ein definiertes IT Sicherheitskonzept?
Bereits von Anfang an existiert in der Verwaltung ein elaboriertes Sicherheitskonzept, das kontinuierlich weiterentwickelt wird. Dazu gehören eine technische IT-Sicherheitsinfrastruktur mit zahlreichen Einzelmaßnahmen und anwenderorientierte Vorkehrungen.
Die große Bandbreite der kommunalen Produkte und Leistungen erfordert gleichfalls 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.

2. Wie sieht dieses Konzept aus?
Über die Konzeption wurde der Haupt- und Personalausschuss zuletzt unter dem Tagesordnungspunkt „Neukonzeption der IT-Sicherheit bei der Stadtverwaltung Mainz“ in der Sitzung am 26.11.2014 informiert. Auf die Vorlage Nr. 1368/2014 wird verwiesen.

3. Wird dieses Konzept allen MitarbeiterInnen kommuniziert und werden diese regelmäßig darüber unterrichtet?
Mitarbeiterinnen und Mitarbeiter werden seit mehreren Jahren immer wieder mittels Newsletter, Artikeln in der Mitarbeiterzeitung sowie durch die zuständigen EVPs (EDV-Verbindungspersonen in den Fachämtern) über den richtigen und sicheren Umgang mit IT-Technik informiert. EVPs erhalten die dafür notwendigen Informationen durch die KDZ per Mail oder erweitern ihr Wissen auf regelmäßig stattfindenden Workshops. Dadurch können sie dann als Multiplikatoren gegenüber den Mitarbeiterinnen und Mitarbeitern auftreten.

4. Wie wird die Einhaltung der Sicherheitsrichtlinien kontrolliert?
Die Stadtverwaltung lässt regelmäßig, ohne Wissen der KDZ, so genannte Penetrationstest 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.
Weiterhin finden, in Abstimmung mit dem städtischen Personalrat, organisatorische Maßnahmen wie z.B. Regelmäßige Kontrollgänge oder Auswertung von Protokolldaten (Internetnutzung) statt, die durch technische Maßnahmen wie Monitoring oder Protokollierung unterstützt werden.

5. Liegen bereits Erkenntnisse vor, ob durch den Hackerangriff auf die Zulassungstellensoftware möglicherweise auch andere von der Stadt Mainz betriebene Systeme betroffen waren?
Durch den Hackerangriff waren keine von der Stadt Mainz betriebenen IT-Systeme betroffen. Der Angriff zielte auf ein Modul der Zulassungsstellensoftware (Wunschkennzeichen), welches nicht in der Stadt Mainz, sondern gemeinsam durch den LDI (Rheinland-Pfalz) und eKomm21 (Hessen) 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 sofort vom Netz genommen und Tests auf Schadsoftware durchgeführt. Es wurde keine lokale Infektion mit Schadsoftware auf Systemen der Stadt Mainz gefunden.

Mainz, 13. Juli 2015

gez.
Michael Ebling