zu TOP .....

Mainz, 13.11.2021

Anfrage 1644/2021 zur Sitzung am **24.11.2021**

IT-Sicherheit der städtischen Verwaltung / Schutz vor Ransom-Ware-Attacken (Piraten & Volt)

Immer öfter kommt es zu technischen Angriffen auch auf die Systeme von Kommunen. So ist aktuell z.B. die Stadt Witten von einer großen Attacke betroffen, die nahezu die komplette IT der Stadt lahmlegt.
Im Juli dieses Jahres wurde nahezu die gesamte IT des Landkreises Anhalt-Bitterfeld zerstört. Jeder einzelne PC der Kreisverwaltung musste gelöscht und neu eingerichtet werden. Es wurde der Katastrophenfall ausgerufen und die Bundeswehr zur Hilfe gerufen. Nachdem der Landkreis nicht auf die Erpressung der Täter*innen eingegangen ist, sind Behördendaten durch sie im Internet veröffentlicht worden. Der Landkreis befindet sich laut Medienberichten auch jetzt noch, nach über drei Monaten, im Katastrophenmodus und hofft aktuell bis Ende des Jahres die Folgen des Ransomware-Angriffs überwunden zu haben.
IT-Sicherheit spielt daher eine immer größer werdende Rolle zum Schutz der Infrastrukturen und der Arbeitsfähigkeit der Kommunen und der Daten von Bürgerinnen und Bürgern.

Wir fragen daher die Verwaltung:

1. Wie bewertet die Verwaltung insgesamt das aktuelle Schutzniveau der IT-Systeme der Stadt Mainz vor technischen Angriffen zur Sabotage, Informationsgewinnung oder Erpressung?
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?
3. Welche Notfallpläne existieren für den Fall eines größeren Angriffs auf die IT-Systeme der Stadt?
4. Existieren definierte Prozesse dafür, welche Ämter und Behörden im Notfall eingebunden werden?
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?

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

Conrad, Maurice