Stadt
Heidelberg

Heidelberg, den 19.07.2021

Anfrage Nr.: 0073/2021/FZ
Anfrage von: Stadtrat Geschinski
Anfragedatum: 13.07.2021

Betreff:

Cyberattacken auf die Stadtverwaltung

Schriftliche Frage:

1. Betreibt die Stadt eigene Server oder bedient sie sich Drittanbietern? Werden Daten der Stadt in der Cloud gelagert?

2. Welche Anstrengungen werden seitens der Stadt unternommen, um Angriffe aus dem Internet auf die Server, auf denen die Daten der Stadt lagern, zu verhindern?

3. Wie wird die Abwehr von Hackerangriffen sichergestellt (eigenes Personal, Outsourcing)?

4. Wie schätzt die Stadt den Schutz eigener Computersysteme vor Cyberattacken ein? Wäre die Stadt in der Lage, auch bei einem Cyberangriff, zum Beispiel mit Ransom-Software wie im Landkreis Anhalt-Bitterfeld, den Dienst aufrechtzuerhalten?

Antwort:

1. Die Stadt Heidelberg nutzt sowohl eigene Server als auch Dienste des kommunalen Datenverarbeitungsverbandes, welches insbesondere die landeseinheitlichen Verfahren bereitstellt. Daten von Bürgerinnen und Bürgern werden auf eigenen Servern und beim kommunalen Datenverarbeitungsverband verarbeitet und gespeichert. Für die Verarbeitung von Bürgerdaten werden Clouddienste nicht eingesetzt.

2. Um die Vertraulichkeit, Verfügbarkeit und Integrität sicherzustellen, setzen wir zahlreiche technische und organisatorische Maßnahmen um.

Technisch setzen wir auf ein mehrschichtiges Sicherheitskonzept, das wir aus Sicherheitsgründen nur grob skizzieren können. Hier kommen Komponenten wie Firewall-Systeme, Schutz gegen Schadsoftware et cetera zum Einsatz. Organisatorische Maßnahmen wie Dienstanweisungen und Awareness-Maßnahmen ergänzen das Sicherheitskonzept.

3. Die Verhinderung von Hackerangriffen wird durch eigenes Personal sichergestellt, das in einzelnen Aspekten durch externe Dienstleister unterstützt wird.

4. Eine derzeit besonders erfolgreiche Angriffsmethode ist es, Benutzerinnen und Benutzer mittels E-Mails zur Eingabe der Benutzerdaten/Passwort zu bewegen oder Links zum Herunterladen von Schadsoftware zu verbreiten. Ziel dieser Angriffe sind vorranging Menschen, um auch in *technisch* gut geschützte Systeme einzudringen. Die städtischen Awareness-Maßnahmen gehören damit zu den wichtigsten Informationssicherheitsmaßnahmen.

Allgemein ist die Sicherheitslage weiterhin als sehr angespannt zu beurteilen. Ein einhundertprozentiger Schutz gegen Cyberangriffe ist aber nicht machbar. Im Rahmen unserer Möglichkeiten haben wir technische und organisatorische Maßnahmen ergriffen, um die Informationssicherheit bestmöglich umzusetzen.

Ein großflächiger Ransomware-Vorfall wie beim Kammergericht Berlin, beim Kreis Anhalt-Bitterfeld, bei den Städten Angermünde oder Potsdam kann auch bei der Stadt Heidelberg nicht vollständig ausgeschlossen werden. In solchen massiven Fällen ist davon auszugehen, dass eine Unterstützung durch externe Dienstleister, dem BSI und der Polizei erforderlich werden. Einen Teil des finanziellen Risikos sichern wir mit einer Versicherung ab. Die Ausfallzeiten und der Schadensumfang können pauschal nicht abgeschätzt werden. Je nach Angriffsszenario kann ein möglicher Ausfall wenige Stunden bis mehrere Wochen betragen und sich auf einen Teilbereich oder die gesamte Stadtverwaltung auswirken.

Grundsätzlich ist die Informationssicherheit bei der Stadt Heidelberg gewährleistet, aber auch potenziell gefährdet. Um der wachsenden Gefährdungslage adäquat zu begegnen, ist es erforderlich, Maßnahmen permanent anzupassen, weiter zu entwickeln und gegebenenfalls weitere finanzielle und personelle Ressourcen zur Verfügung zu stellen.