

Digitalisierungsausschuss, 04.05.2021, öffentlich

Anfrage der CDU „Kommunale IT-Sicherheit“

Die Anfrage lautet:

„Mittlerweile gibt es kaum einen Bereich, auf den der digitale Wandel keine direkten oder indirekten Auswirkungen hat. Datensicherheit und Datenschutz nehmen angesichts wachsender Cyberkriminalität eine wichtige Rolle ein. Daher stellen wir zur Sitzung des Digitalisierungsausschusses am 04.05.2021 folgende Anfragen zur kommunalen IT-Sicherheit von hochsensiblen und personenbezogenen Daten:“

Frage:

„Welche präventiven und reaktiven Maßnahmen ergreift die Stadt Bielefeld in Bezug auf sicherheitsrelevante Vorfälle beim Schutz der kommunalen IT-Sicherheit?“

Antwort der Verwaltung:

Die notwendige Infrastruktur zum Schutz hochsensibler und personenbezogenen Daten wird im Rechenzentrum der Stadtwerke Bielefeld GmbH zur Verfügung gestellt und von den dort zuständigen Personen mit hohem Verantwortungsbewusstsein sehr professionell betrieben.

Die Fachleute setzen sich täglich intensiv mit aktuellen „Bedrohungs-Szenarien“ auseinander, damit die Datensicherheit technisch gewährleistet ist.

Dieses geschieht in enger Abstimmung mit dem Informationssicherheitsbeauftragten (ISiBe) der Stadt Bielefeld sowohl proaktiv als auch reaktiv unter ggf. Einbindung des Datenschutzbeauftragten.

Für fremdgehostete Fachverfahren werden Verträge zur Auftragsverarbeitung mit den jeweiligen Vertragspartnern geschlossen, damit auch hier durch geeignete technische und organisatorische Maßnahmen der Anbieter Datenschutz und Datensicherheit gewährleistet sind.

Über das Intranet (Bielefeld intern) wird in regelmäßigen Abständen und anlassbezogen auf den „sicheren“ Umgang mit IT in der täglichen Arbeit hingewiesen. Über diesen Weg werden die Mitarbeiterinnen und Mitarbeiter kontinuierlich informiert und gleichzeitig für möglichen „Gefahren aus dem Internet“ sensibilisiert.

Zusätzlich sind auf den Seiten des Datenschutzbeauftragten, des Informationssicherheitsbeauftragten und der IT die geltenden Dienstanweisungen Datenschutz und IT sowie verschiedene Servicedokumente zu den Themen Datenschutz, Datensicherheit, Internetnutzung oder Nutzung sozialer Netzwerke hinterlegt.

Für den Fall, dass Systeme evtl. kompromittiert wurden, werden umfangreiche Prüfungen und Maßnahmen zur System(ab)sicherung und Datensicherung eingeleitet. Notwendige Meldungen und Informationen werden an die hierfür vorgesehenen

Stellen (z.B. CERT*-Bund) weitergegeben. Unter Umständen werden die betroffenen Systeme zeitweise deaktiviert.

Zusatzfrage:

„Werden die ergriffenen Vorgaben des Bundes bzw. des Landes durch ein kommunales Sicherheitskonzept ergänzt und welche Elemente umfasst diese Konzept?“

Antwort der Verwaltung:

Die Stadt Bielefeld hat nicht ein zentrales Sicherheitskonzept, sondern anlassbezogen mehrere; zum Beispiel beim Verfahren iKfz (Anbindung an das Kraftfahrtbundesamt) oder für die Nutzung des Bundesnetzes (NdB, früher DOI).

Der städtische Informationssicherheitsbeauftragte erarbeitet die geforderten Konzepte gemeinsam mit der IT, den zuständigen Fachbereichen, den Stadtwerken und externer Unterstützung. Alle Aktivitäten und Regelungen fließen in ein Informationssicherheitsmanagementsystem (ISMS) ein, welches sukzessive aufgebaut wird und als Nachweis für die Vorkehrungen dient, die die Stadt zum Schutz ihrer IT trifft.

Neben einem hohen Sicherheitsniveau steht dabei die kontinuierliche Verbesserung des sicheren Umgangs mit Informationen und Informationstechnik in den jeweiligen Verantwortungsbereichen im Vordergrund.