

An den Vorsitzenden des
Ausschusses für Digitalisierung,
Wirtschaftsförderung und Stadtmarketing
Herrn Bürgermeister N. Morkes
Stadt Gütersloh
Per Mail

16.09.2021

Sehr geehrter Herr Morkes,

die SPD-Fraktion stellt zu TOP 14 „Fragen der Ausschussmitglieder“ der Sitzung des ADWS am 27.09.2021 folgende

Anfrage zur IT-Sicherheit bei der Stadt Gütersloh

Sachverhalt:

Kürzlich hat das Bundesministerium des Inneren die Cyber-Sicherheitsstrategie des Bundes vorgestellt. Sie führt die Digitalisierung der Verwaltung als besonders gefährdeten Bereich auf: "Angesichts der zunehmenden Digitalisierung der öffentlichen Verwaltung stellen Cyberangriffe auf staatliche Institutionen – neben den Gefährdungen durch eine Ausspähung sensibler Daten – unter anderem eine elementare Gefahr für die Funktionsfähigkeit und Integrität der staatlichen Leistungserbringung dar." Auch vor dem Hintergrund der Corona-Pandemie sind die Anforderungen und Erwartungshaltungen an die Digitalisierung sprunghaft gestiegen, stellt das BMI weiter fest.

Dass diese Bedrohungslage akut und nicht abstrakt ist, zeigt der jüngste Cyberangriff auf den Landkreis Anhalt-Bitterfeld, der immense Einschränkungen für Bürgerinnen, Bürger und Verwaltung mit sich brachte. Wegen dieser Attacke konnten die Mitarbeiter und Mitarbeiterinnen des Kreises über Wochen nur noch per Telefon oder Fax kommunizieren. Der Zugriff auf ihre Rechner wurde verboten. Infolge dessen musste der Katastrophenfall ausgerufen, die Bundeswehr um Unterstützung gebeten und externe Dienstleister einbezogen werden, um die Folgen des Angriffs zu bewältigen und ein neues Netz aufzubauen. Aufgrund des Cyberangriffs konnten Gehälter, Sozialleistungen, Bafög kaum ausgezahlt und Kraftfahrzeuge wochenlang nicht angemeldet werden. (Quelle z.B.: <https://www.heise.de/news/Cyberangriff-auf-Anhalt-Bitterfeld-Landkreis-zeigt-sich-weiterhin-unerpressbar-6160917.html>)

Vor diesem Hintergrund bittet die SPD-Fraktion um die Beantwortung folgender

Fragen:

- 1. Hat die Verwaltung die Ereignisse im Kreis Anhalt-Bitterfeld zum Anlass genommen, ihre eigene IT-Sicherheit zu überprüfen? Wenn ja, mit welchem Ergebnis? Sind entsprechende Anfragen an die IT-Dienstleister gegangen und wie sind ggf. deren Ergebnisse?**
- 2. Welche Prozeduren, Kontrollmechanismen und organisatorische Vorkehrungen existieren, um Cyberangriffe zu verhindern? Wie werden die Mitarbeiterinnen und Mitarbeiter für diese Materie sensibilisiert und geschult?**

3. Finden regelmäßige Audits statt, bei denen externe Stellen die Sicherheit der IT-Systeme und der relevanten Organisationsabläufe der Stadt überprüfen und bewerten? Wenn ja, wie waren die Ergebnisse, welche Konsequenzen sind ggf. gezogen worden?
4. Finden regelmäßige Penetrationstests statt, bei denen externe Dienstleister entlang der Richtlinien des Bundesamtes für Sicherheit in der Informationstechnik (BSI) die Verwundbarkeit der IT-Infrastruktur bzgl. Cyberangriffen testen und bewerten? Wenn ja, welche Ergebnisse haben diese gebracht?
5. Wie sichert die Stadt ein hohes IT-Sicherheitsniveau ihrer externen Dienstleister? Werden IT-Security und -Compliance durch geeignete und angemessene Maßnahmen (Selbstauskunft, Zertifizierungen, Audits, Penetrationstests) festgestellt und regelmäßig überprüft? Ist IT-Sicherheit fester Bestandteil von Ausschreibungen in der Stadt-IT?
6. Wie sind die entsprechenden Verhältnisse bei den Beteiligungen der Stadt, insbesondere dem Klinikum und den Stadtwerken?

Mit freundlichen Grüßen

gez. Matthis Haverland
(SPD-Sprecher im ADWS)