



Antwort zur Anfrage Nr. 1044/2022 der ÖDP-Stadtratsfraktion betreffend **Hackerangriff auf die Unternehmensgruppe der Stadtwerke Mainz (ÖDP)**

Die Anfrage wird wie folgt beantwortet:

1. Welche Konsequenzen ziehen die Stadtwerke Mainz aus der Cyberattacke? Welche Maßnahmen werden nun ergriffen, damit sich dies möglichst nicht wiederholt?

Es werden sowohl technische als auch organisatorische Maßnahmen bei den Mainzer Stadtwerken und dem IT-Dienstleister COUNT+CARE getroffen. Dazu gehören zum Beispiel zusätzliche Absicherungen des Netzwerkes bei Zugriffen von außen durch die COUNT+CARE aber auch die Aufarbeitung der Erkenntnisse bei den Mainzer Stadtwerken. Eine Wiederholung kann durch die Natur eines Hacker-Angriffs nie gänzlich ausgeschlossen werden.

2. Wie hoch ist der finanzielle Schaden?

Dies ist aktuell in der Analyse und in der Abstimmung mit der Cyberversicherung.

3. Waren Teile der „kritischen Infrastruktur“ betroffen, wie z.B. die Wasser- oder Stromversorgung?

Nein

4. Konnten inzwischen alle Systeme wieder aktiviert werden? Welche Systeme und Webseiten mussten neu erstellt werden?

Es sind über 90 Prozent der Systeme wiederhergestellt. Die Wiederherstellung aller Systeme wurde dabei priorisiert und strukturiert abgearbeitet. Kein System musste neu erstellt werden, da alle aus dem Backup wiederhergestellt werden konnten. Gleiches gilt für die Webseiten der Unternehmensgruppe. Da die Original-Webseiten jedoch für etwas mehr als zwei Wochen nicht erreichbar waren, wurden in dieser Zeit Ersatz-Webseiten und Ersatz-E-Mail-Postfächer in Betrieb genommen.

5. Waren sensible Daten betroffen?

Nach dem kriminellen Hackerangriff auf den Darmstädter IT-Dienstleister Count + Care am 12. Juni 2022 wurden von den Tätern einige Zeit später Daten im so genannten Darknet verbreitet. Hiervon waren unter anderem auch personenbezogene Daten von Kundinnen und Kunden verschiedener Tochter- und Beteiligungsgesellschaften der Mainzer Stadtwerke AG betroffen. Darunter fallen Kontakt-, Vertrags- und in einem Teil der Fälle auch Zahlungsdaten. Die betroffenen Kundinnen und Kunden wurden umgehend von der jeweiligen Tochter- und Beteiligungsgesellschaft der Mainzer Stadtwerke AG über Einzelheiten informiert.

6. Derzeit werden wieder Busausfälle bei der Mainzer Mobilität beobachtet. Ist dies eine Folge des Hackerangriffes und wenn ja, warum?

Vor allem am Johannismachtwochenende gab es gehäuft Ausfälle von Fahrten im Bereich der Mainzer Mobilität. Gründe dafür waren ein hoher Krankenstand aufgrund der sich bundesweit verschärfenden Corona-Situation sowie die IT-Probleme durch den Hackerangriff. In der ersten Zeit nach dem 12. Juni konnten für den Fahrplanbetrieb notwendige Systeme nicht oder nur eingeschränkt eingesetzt werden. Dies wirkte sich unter anderem auf die Einsatzdisposition der Fahrerinnen und Fahrer aus, die nicht wie gewohnt funktionierte. Durch den Hackerangriff arbeiteten in der ersten Zeit zudem auch die rechnergesteuerten Auskunftssysteme nicht so zuverlässig wie gewohnt. Nach und nach wurden einzelne IT-Systeme wieder in Betrieb genommen – die Situation besserte sich daher von Tag zu Tag.

7. Gibt es in der Zwischenzeit veröffentlichte Erkenntnisse der staatsanwaltlichen Ermittlungen?

Nein, hierzu liegt uns nichts vor.

8. Welche Erkenntnisse zieht die Stadtverwaltung Mainz für sich und ihre Netzwerke aus diesem Cyberangriff?

Die Kommunale Datenzentrale entwickelt den vorhandenen und vielfach gestaffelten technischen Schutz des städtischen Netzes von innen und außen kontinuierlich weiter und prüft diesen auf jeweils aktuelle Bedrohungslagen. Darüber hinaus hat die Stadtverwaltung bereits in der Vergangenheit die Mitarbeitenden der Verwaltung regelmäßig zum Thema Informationssicherheit sensibilisiert.

Mainz, 05.09.2022

gez.

Günter Beck
Bürgermeister