Kleine Anfrage der AfD-Ratsfraktion nach § 7 der Geschäftsordnung des Rates als Nr. K/17/1049-01 vom 30. 8. 2021 von W. Kempkes.

Betr.: Kommunale Infrastruktur als Objekt von Cyberkriminalität.

Antwort der Stadtverwaltung K/17/1114-01 vom 29. 9. 2021.

Hacker erpreßten den Landkreis Anhalt-Bitterfeld. Dabei legten sie das Computersystem der Verwaltung lahm. Der Landrat ließ daraufhin den Katastrophenfall ausrufen: https://www.spiegel.de/netzwelt/-netzpolitik/anhalt-bitterfeld-hacker-stellen-persoenliche-daten-von-abgeordneten-ins-darknet-a-b3655f6d-0002-0001-0000-000178686047

Daraus ergeben sich folgende Fragen:

Frage 1:

Wieviele Cybervorfälle aus Oberhausen wurden im vergangenen Jahr an das Bundesamt für Informationssicherheit durch wen gemeldet?

Antwort:

Durch die Sicherheitssysteme der Stadtverwaltung Oberhausen wurden im Zeitraum 01.01.2020 bis 31.12.2020 keine Ereignisse von Relevanz detektiert. Daher erfolgten keine Meldungen an das Bundesamt für Sicherheit in der Informationstechnik (BSI)

Frage 2:

Gibt es einen Notfallplan (Incident Response Plan), wie ihn auch Unternehmen nutzen, um Cyberangriffe koordiniert abzuwehren und um zwischen Dezernaten und Bürgern zu kommunizieren?

Antwort:

Zur Abwehr von Cyberangriffen wurden technisch organisatorische Maßnahmen hinsichtlich des Schutzes der wesentlichen IT-Sicherheitsziele Vertraulichkeit, Integrität und Verfügbarkeit durch die Oberhausener Gebäudemanagement GmbH (OGM) im Zusammenspiel mit der Stabstelle IT-Management der Stadt Oberhausen definiert. Diese waren ebenfalls Bestandteil der entsprechenden IT-Nutzungsverträge zwischen beiden Häusern. Mit der Zusammenführung der IT-Strukturen beider Häuser im Bereich 4-4 / IT der Stadt Oberhausen wurden diese technisch organisatorischen Maßnahmen überarbeitet und aktualisiert.

Darüber hinaus wurde zum 01.07.2021 die Stelle "IT-Sicherheit und Risikomanagement" im Bereich 4-4 / IT besetzt, welche federführend die Ausarbeitungen zum Thema IT-Sicherheit übernimmt. Das Ergebnis der Bestandsaufnahme des neuen IT-Sicherheits- und Risikomanagers zum Stand der IT-Sicherheit hat die Weiterentwicklung zu einem vollum-

fänglichen IT-Notfallkonzept als priorisierte Maßnahme festgestellt. Hierzu wird derzeit eine Erweiterung der technisch organisatorischen Maßnahmen zu einem vollständigen Notfallkonzept inkl. Notfallplan erarbeitet.

Frage 3:

Wer hat einen solchen Plan mit welcher fachlichen Expertise wann entwickelt?

Antwort:

Die IT-Experten der OGM GmbH sowie der Stadt Oberhausen haben die technisch organisatorischen Maßnahmen im Jahr 2016 mit der Unterzeichnung der IT-Leistungsverträge zwischen OGM GmbH und der Stadt Oberhausen erstellt, mitgewirkt haben hier auch die Datenschutzbeauftragten beider Häuser. Die Expertise der Ersteller*innen umfasst einschlägige Berufsausbildungen und Studiengänge sowie eine langjährige Erfahrung in der Erbringung von IT-Leistungen. In die letzte Überarbeitung konnten darüber hinaus auch Qualifikationen als ISO 20.000 Internal Auditor und Consultant sowie ITIL Expert durch internes Personal genutzt werden.

Frage 4:

Welche Fortschreibungen, Anpassungen, Weiterentwicklungen erfuhr dieser Notfallplan durch wen, wann und aus welchem Anlaß?

Antwort:

Die technisch organisatorischen Maßnahmen wurden im Jahr 2020 im Rahmen der Zusammenlegung der IT im Bereich 4-4 / IT überarbeitet und aktualisiert. An dieser Überarbeitung haben neben dem Bereich 4-4 / IT auch die Datenschutzbeauftragten der OGM GmbH sowie der Stadt Oberhausen mitgewirkt.

Frage 5:

Wird dieser Notfallplan regelmäßig geübt? Wenn ja, in welcher Form, mit welchen Beteiligten und mit welchen Ergebnissen bzw. Konsequenzen?

Antwort:

Im Rahmen der Weiterentwicklung der technisch organisatorischen Maßnahmen zu einem Notfallkonzept werden auch Übungen in Art und Umfang definiert. Die technisch organisatorischen Maßnahmen sehen bereits derzeit schon strukturierte Übungen im Bereich der IT vor. Auch die dienstleistenden Rechenzentren erproben regelmäßig Notfallmaßnahmen.