Stadt Köln

Die Oberbürgermeisterin

Dezernat, Dienststelle
I/12

Vorlagen-Nummer 01.06.2016
1771/2016

Beantwortung einer Anfrage nach § 4 der Geschäftsordnung

öffentlicher Teil

Gremium	Datum
Unterausschuss Digitale Kommunikation und Organisation	06.06.2016

Sicherheit der IT-Systeme in Kölner Krankenhäusern und Co.; Beantwortung der Anfrage (AN/0299/2016) der Piratengruppe

Die Verwaltung nimmt wie folgt Stellung:

Frage 1: Hat die Stadt Köln den großen IT-Penetrationstest im 4. Quartal 2015 durchführen lassen, und was war das Ergebnis?

Antwort:
Ja, die Ergebnisse wurden dem Unterausschuss Digitale Kommunikation und Organisation in der Sitzung am 22.Februar 2016 durch den beauftragten Penetrationstester -das BSI-zertifizierte Unternehmen TÜV Trust IT der TÜV Austria Group- vorgestellt.

Der TÜV Trust IT bescheinigt der Verwaltung im Ergebnis eine sehr gute IT-Sicherheit. Es wurden keine unmittelbaren Angriffspunkte gegen die Systeme der Stadt Köln identifiziert.

Frage 2: Welche Konsequenzen hat die Stadt aus den Ergebnissen gezogen?

Antwort:
Eine Schwachstelle mit mittlerem Risiko und vier Schwachstellen mit geringem Risiko wurden untersucht und beseitigt.

Frage 3: Hat die Stadt Kenntnisse über Cyber-Angriffe gegen Krankenhäuser oder andere große städtische Einrichtungen in Köln?

Antwort:
Beim Amt für Informationsverarbeitung liegen keine über die in der Presse veröffentlichten Informationen und Erkenntnisse über Cyberangriffe vor.

Die Krankenanstalten Köln und die Universitätskliniken Köln, die der gemeinsamen Arbeitsgruppe „Cybercrime und Cyberwar - kritische Infrastrukturen Köln“ angehören, hatten nach eigener Aussage keine entsprechenden Sicherheitsvorkommnisse.

In der Presse wurde am 15.02.2016 folgende Erklärung des LKA und des BSI veröffentlicht:
Das Klinikum Arnsberg sei jetzt der dritte der Behörde bekannt gewordene Fall seit dem vergangenen Jahr, sagte ein Sprecher des Landeskriminalamtes. Die Attacke auf die Klinik in Neuss ist nach Einschätzung des Bundesamts für Sicherheit in der Informationstechnik kein gezielter Angriff gewesen. Das Lukaskrankenhaus sei Opfer einer breit gestreuten Cyber-Attacke geworden, sagte ein Sprecher der Bundesbehörde.

Ursächlich waren es wohl die gleichen Sicherheitsprobleme (Verschlüsselungstrojaner), die im ver-

gangenen Dezember bereits bei verschiedenen Kommunen, den Landschaftsverbänden und dem Innenministerium NRW zu Ausfällen geführt haben.

Frage 4: Welche Konsequenzen zieht die Stadt aus den Cyber-Angriffen auf Krankhäuser für die Kommune und das Gesundheitssystem?

Antwort:
Der Sicherheitsbeauftragte der Stadt Köln erfragt die konkrete Situation bei den städt. Kliniken und - sofern es erforderlich war- auch die getroffenen Maßnahmen. Die Auswertungen der Rückmeldungen und die gemeinsame Abstimmung der notwendigen Maßnahmen gehören zu den regelmäßigen Themen der gemeinsamen Arbeitsgruppe „Cybercrime und Cyberwar - kritischen Infrastrukturen Köln“.

Auf Anfrage des städtischen IT-Sicherheitsbeauftragten bestätigte die Datenschutzbeauftragte der Kölner Kliniken, Frau Birgit Terres, am 13.04.2016, dass die Sicherheitskonzepte der Kliniken und die daraus resultierenden und umgesetzten Sicherheitsmaßnahmen die Aktivierung der Ransomware verhindert haben. Aktuell werden die Sicherheitsvorkehrungen durch die Klinken als ausreichend angesehen.

Frage 5: Inwieweit sind Gefährdungsszenarien wie Angriffe auf IT-Infrastrukturen, insbesondere von Krankenhäusern, Wasser- und Elektrizitätswerken und Telekommunikationseinrichtungen, Gegenstand von Katastrophenschutzplänen der Stadt Köln?

Antwort:
Zur gemeinsamen Abwehr und Bekämpfung von Cybercrime und Cyberwar-Angriffen wurde am 07.01.2015 die Projektgruppe Cybercrime und Cyberwar (im Projekt Großschadensereignisse) eingerichtet und tagt seitdem quartalsweise. Zu den Teilnehmern gehören neben der Stadt Köln (Amt für Informationsverarbeitung, IT-Sicherheitsverantwortlicher, Dienststelle für E-Government und Online-Dienste, Berufsfeuerwehr und das Amt für Straßen- und Verkehrstechnik) noch folgende Partner aus der Region, die zur kritischen Infrastruktur im Kölner Raum gehören:

- Kliniken der Stadt Köln
- Rheinenergie
- NetCologne
- Universitätskliniken Köln
- Flughafen Köln-Bonn
- Bayerwerke
- Landeskriminalamt NRW.

Aktuelle Interessenten:

- KVB
- Deutsche Bahn
- Shell

Zu den Zielen der Arbeitsgruppe zählen:

- gemeinsamer Schutz der Infrastruktur vor Cybercrime- und Cyberwar- Angriffen
- gemeinsame Informationsbeschaffung und Bewertung
- Zentrale Meldestelle für Sicherheitsereignisse im Kölner Raum
- Workflow und Informationsfluss zwischen den Teilnehmern
- Abgestimmte Reaktionen und ggf. gemeinsame Maßnahmen
- Beschreibung von kritischen Szenarien und die Erstellung gemeinsamer Maßnahmenpläne

Wichtige Ergebnisse der Arbeitsgruppe „Cybercrime und Cyberwar“ werden in den Lenkungsgruppensitzungen Großschadensereignisse berichtet. Die Erkenntnisse und Empfehlungen der Arbeitsgruppe werden für Qualitätskontrollen, sowie eventuelle Optimierungen der bestehenden Sicherheitsorganisation und der umgesetzten Sicherheitsmaßnahmen der Stadt Köln genutzt.