Stadt Köln

Die Oberbürgermeisterin

Dezernat, Dienststelle
I/12

Vorlagen-Nummer 04.06.2019
1617/2019

Beantwortung einer Anfrage nach § 4 der Geschäftsordnung

öffentlicher Teil

Gremium	Datum
Unterausschuss Digitale Kommunikation und Organisation	17.06.2019

Beantwortung der Anfrage der Ratsgruppe BUNT AN/0289/2019
Datensicherheit und Datenschutz der Stadt Köln - Sachstand 2019

Anfragetext:

1. Wurden die IT-Systeme in der kommunalen Verwaltung, den kommunalen Unternehmen und den kommunalen Einrichtungen (Bibliotheken, Schulen, Jobcenter usw.) mithilfe von IT-Penetrationstests und Webchecks auch nach dem Test im Dezember 2015 überprüft? (Wenn nicht, begründen Sie bitte, warum nicht.)

2. In welchen kommunalen Einrichtungen, Behörden usw. wurden die IT-Systeme in den letzten vier Jahren IT-Penetrationstests und Webchecks unterzogen? (Bitte unter Angabe des Test-Datums.) Welche Ergebnisse haben diese Tests ergeben? (Bitte nennen Sie die gefundene Schwachstelle, wenn möglich.)

3. Plant die Verwaltung, zusätzliche Verfahren zur Überprüfung der IT-Sicherheit einzuführen, die auch die „Schwachstelle Mensch“ berücksichtigen?

4. Welche städtischen Einrichtungen sind vom Bundesamt für Sicherheit in der Informationstechnik (BSI) nach ISO 27001 auf der Basis von IT-Grundschutz zertifiziert?

5. Welche der in der Mitteilung 2648/2016 angekündigten Maßnahmen wurden umgesetzt?

Die Verwaltung nimmt wie folgt Stellung:

Zu 1. und 2.:

Das Dokument „IT-Sicherheitspolitik für die Stadt Köln” stellt eine grundlegende, allgemeingültige Richtlinie zur Aufrechterhaltung der IT-Sicherheit innerhalb der Stadt Köln dar und legt die Zuständigkeit für die Stadtverwaltung und zugeordneter Eigenbetriebe und eigenbetriebsähnlicher Einrichtungen fest.
Die organisatorisch selbstständigen Stadtwerkekonzerne planen ihre Penetrationstests in eigener Verantwortung. Auch die pädagogischen Netze der Schulen und das Netz des Jobcenter sind in dieser Hinsicht organisatorisch eigenständig. Ergebnisse aus Penetrationstests werden auch hier grundsätzlich durch die Verantwortlichen nicht veröffentlicht. Im Rahmen der Zusammenarbeit in der „Arbeitsgruppe Cybercrime/Cyberwar für kritische Infrastrukturen im Kölner Raum“ erfolgt ein regelmäßiger Informationsaustausch. Daneben wurde eine Plattform zur gegenseitigen Beratung und Unterstützung bei Sicherheitsvorfällen etabliert.
Seit 2015 werden die technischen und organisatorischen Maßnahmen zur Informationssicherheit bei der Stadt Köln im Rahmen eines kontinuierlichen Verbesserungsprozesses regelmäßig überprüft. Die Erfahrungen, welche dabei gewonnen werden, fließen in den beim Amt für Informationsverarbeitung etablierten „IT Security Management Prozess nach ITIL“ ein. Im Security Review

wird überprüft, ob die Sicherheitsmaßnahmen und –prozeduren immer noch im Einklang mit den in den Sicherheitskonzepten bestimmten Risikoeinschätzungen stehen. Die bereits getroffenen und umgesetzten Sicherheitsmaßnahmen werden dann aufgrund der gewonnenen Erkenntnisse gegebenenfalls erweitert oder angepasst. Zu den Prüfungen gehören Penetrationstests der öffentlichen Webzugänge und in Einzelfällen auch die entsprechende Prüfung besonders sensibler Systeme.

Im Bereich des CAN wurden 2017 Penetrationstests für die in diesem Jahr stattgefundenen Wahlen durchgeführt (Bundestagswahl, Landtag NRW). Im Jahr 2018 wurden aufgrund der hohen personellen Aufwände für die BSI-Zertifizierung keine Tests gemacht. Im Fokus des Penetrationstest zur Europawahl-Infrastruktur standen die drei Webanwendungen Wahlen, Wahlhelfer und Briefwahlantrag. Die Anwendungen wurden durch den TÜV IT aus dem Internet heraus auf Schwachstellen untersucht. Insgesamt wurden sieben Auffälligkeiten identifiziert, wobei keine Schwachstelle mit einem kritischen oder hohen Sicherheitsrisiko bewertet wurde. Zwei Empfehlungen wurden durch das Amt für Informationsverarbeitung noch vor der Wahl umgesetzt, alle übrigen wurden an die Hersteller übermittelt, da die Beseitigung der Schwachstellen nur dort realisiert werden kann. Der TÜV IT testiert: „Zusammenfassend weisen die Webanwendungen zum Zeitpunkt der Testdurchführung ein hohes Maß an wirksamen sicherheitstechnischen Schutzmaßnahmen auf."

Der Penetrationstest für das MESO-Inforegister ist für das 4. Quartal 2019 geplant, hier starten die Vorbereitungen nach den Sommerferien.

Im Bereich der Stadtentwässerung/StEB wurden 2016 die Systeme des StEB-WEB und die für Wartungszecke erreichbaren Zugänge der Abflusssteuerzentrale mittels eines Penetrationstests durch die Firma TÜV-Trust geprüft. Es gab bei diesen Tests keine Beanstandungen. Die grundsätzlich geplante zweijährige Wiederholung musste im Jahr 2018 auf 2019 verschoben werden. Grund waren die umfangreichen Arbeiten zur Auditierung nach dem Sicherheitsgesetz für „Kritische Infrastrukturen", welche im Jahr 2018 erfolgreich abgeschlossen wurden.

Im Bereich des internen Kundennetzes der Stadtbibliothek ist für das Jahr 2019 ein Penetrationstest der Kundenzugänge geplant.

Zu 3.:

Zur Intensivierung der Sensibilisierung von Mitarbeitern und Mitarbeiterinnen, ist der Ausbau von aktuellen eLearning-Möglichkeiten zur Informationssicherheit und Datenschutz geplant. Bei der Einstellung neuer Mitarbeiter/innen werden entsprechende polizeiliche Führungszeugnisse angefordert. Sicherheitsüberprüfungen nach dem Sicherheitsüberprüfungsgesetz Nordrhein-Westfalen (SÜG NW) sind für Mitarbeiter/innen bzw. auch bei Neueinstellungen nicht möglich. Das Gesetz hat diese Prüfung nur für bestimmte sicherheitsempfindliche Tätigkeiten und Personen vorgesehen, somit entfällt für die Stadt Köln die gesetzliche Legitimierung für entsprechende Überprüfungen.

Zu 4.:

<u>Cologne Area Network (CAN)</u>
Das Verfahren zur Erteilung eines Dachzertifikats nach ISO27001 auf Basis IT-Grundschutz durch das BSI wurde im Dezember 2018 erfolgreich durchgeführt. Das Zertifikat umfasst Dienstleistungen und den grundlegenden Betrieb der städtischen Rechenzentren bis auf die Ebene der Betriebssysteme und somit jeglicher IT-Komponenten, welche für die Datenverarbeitung und die Unterstützung von Verfahren der kommunalen Verwaltung eingesetzt werden.

<u>Stadtentwässerungsbetriebe Köln/StEB</u>
Die StEB gilt, als Entsorger von Wasser für mehr als 500.000 Einwohnern, nach dem Sicherheitsgesetz und der Spezifizierung in der BSI-KritisV (Verordnung zur Bestimmung Kritischer Infrastrukturen). Die Betreiber kritischer Infrastrukturen sind gemäß § 8a (3) BSIG zur Erbringung entsprechende Nachweise in Form eines durch das BSI zu bestätigenden Auditberichts verpflich-

tet. Das notwendige Audit wurde im Mai 2018 erfolgreich durchgeführt und wird 2020 erneuert werden.

Amt für Verkehrsmanagement

Der Verkehrsrechner und das zugehörige IT-Netzwerk sowie Außenanlagen und Feldgeräte des Amtes für Verkehrsmanagement gehört gem. BSIKritisV zu den kritischen Infrastrukturen. Bezüglich der sich daraus ergebenden Verpflichtung zur Auditierung im Zuständigkeitsbereich des Amtes für Verkehrsmanagement kann folgender Sachstand gemeldet werden:

- Aktuell laufen die Vorbereitungen für das gesetzlich vorgeschriebene Audit. Für die Unterstützung bei der Dokumentation und der Vorbereitung der Unterlagen hat das Amt ein hierauf spezialisierte Firma beauftragt. Es sind jedoch im erheblichen Umfang Eigenleistungen zu erbringen, die sich aus den Dokumentationspflichten und Darlegung der Prozesse ergeben.
- Das eigentliche Audit entsprechend der Fristsetzung durch das BSI in der letzten Juni Woche 2019 vorgesehen. Das geplante Audit befindet sich damit in dem durch die Verordnung vorgegebenen Zeitrahmen. Der entsprechende Auftrag wurde bereits vergeben.
- Aufgrund des geplanten Umzugs der Verkehrsleitzentrale und der noch nicht abgeschlossenen Erneuerung zentraler Komponenten des Systems können die Prüfungen nicht abschließend durchgeführt werden. Der TÜV-Süd wird, wie im Vorfeld mit dem BSI abgestimmt, bis Ende des Jahres 2020 ggf. noch vorhandene Risiken identifizieren und Vorgaben zur deren Beseitigung oder Reduzierung in einem entsprechenden Risikobehandlungsplan vorlegen.

Zu 5.:

Der nächste Termin für den jährlichen Sicherheitsbericht für den Unterausschuss Digitale Kommunikation und Organisation/DIKO ist im Herbst 2019 geplant. Aus den Anfragen 3850/2014, 2151/2015, 1771/2016, 2648/2016, 3667/2017, 4230/2018 gibt es keine offenen Aufträge.

Gez. Dr. Keller