Stadt Köln

Der Oberbürgermeister

Dezernat, Dienststelle
I/12

17.08.2015

Vorlagen-Nummer
2151/2015

Beantwortung einer Anfrage nach § 4 der Geschäftsordnung

öffentlicher Teil

Gremium	Datum
Unterausschuss Digitale Kommunikation und Organisation	17.08.2015
Ausschuss Allgemeine Verwaltung und Rechtsfragen / Vergabe / Internationales	31.08.2015
Rat	10.09.2015

Datensicherheit und Datenschutz der Stadt Köln; Beantwortung einer Anfrage der Gruppe der Piraten (AN/1031/2015)

Feststellung der Piratengruppe:
Die Bedeutung der Themen Datensicherheit und Datenschutz ist spätestens seit dem 6. Juni 2013 (erste Veröffentlichung von Dokumenten des Whistleblowers Edward Snowden im "Guardian") in aller Munde. Seither stellen öffentlichen Behörden mehr Ressourcen zur Verfügung um Daten zu schützen und die Sicherheit der IT-Infrastruktur zu erhöhen. Der Datenschutzbeauftragte des Landes NRW, Ulrich Lepper, hatte zuletzt Sonderprüfungen zur Datensicherheit in der öffentlichen Verwaltung bei den Kommunen veranlasst. Die Kontrollen ergaben, dass viele Kommunen kein eigenes Sicherheitskonzept haben. Lepper zog das Fazit, dass „bei der IT-Sicherheit noch eine Menge zu tun ist“.

Auch die GPA NRW (Gemeindeprüfungsanstalt Nordrhein-Westfalen) führte zuletzt eine Prüfung der IT der Städte durch. Die Ergebnisse der Prüfung finden sich hier, allerdings scheint keine Prüfung der Kölner IT stattgefunden zu haben:
http://gpanrw.de/de/prufung/prufberichte/5_53.html.

Der Deutsche Städtetag veröffentlichte vor kurzem eine Handreichung zur Ausgestaltung der Informationssicherheitsleitlinie in Kommunalverwaltungen und empfiehlt die Einrichtung eines Informationssicherheits-Managementsystem (ISMS). Die kommunalen Spitzenverbände raten zudem zu sogenannten IT-Penetrationstest und Webchecks. In der Antwort der Verwaltung auf die Piratengruppen-Anfrage „Schutz vor Angriffen auf kommunale IT-Systeme in Köln“ musste die Stadt einräumen, dass sie bisher keine Tests durchgeführt hat. Dies soll nun Ende 2015 nachgeholt werden. In Bonn werden diese Tests schon lange durchgeführt, und der Landkreis Wunsiedel hat ein unabhängiges Gutachterinstituts damit beauftragt, die IT-Sicherheit des Landratsamts zu checken.

In Köln ist der Datenschutzbeauftragte der Stadt zuständig für „alle Fragen, die den Schutz personenbezogener Daten einschließlich der Datensicherheit im Zusammenhang mit der Verwaltungstätigkeit der Stadt Köln betreffen“. Seine Aufgabe umfasst auch die Führung des Verzeichnisses automatisiert geführter Verfahren für die Gesamtverwaltung gemäß § 32 a Absatz 3 DSG NRW. Weitere Aufgaben des Datenschutzbeauftragten finden sich hier: http://www.stadt-koeln.de/service/adressen/datenschutzbeauftragter.

Stellungnahme der Verwaltung:
Im Rahmen strukturierter Prozesse im Amt für Informationsverarbeitung werden standardmäßig bei Inbetriebnahmen für alle neuen und sich aufgrund von Versions-Updates verändernden Produkte (Soft- und Hardware) Sicherheitsprüfungen durchgeführt und die entsprechend des Datenschutzgesetzes nach § 10 III DSG-NRW geforderten schriftlichen Dokumentationen für die Sicherheitskonzepte erstellt. Die Hard- und Softwareprodukte werden zusätzlich vor Produktivsetzung anhand der umfangreichen BSI-Grundschutzkataloge auf evtl. Implementierungsschwachstellen überprüft.

Die entsprechenden Nachweise über diesen Prozess wurden im Rahmen der im Jahr 2014 durchgeführten Zertifizierung durch das Bundesamt für Sicherheit in der Informationstechnik bestätigt.

Die oben genannte Anfrage des Datenschutzbeauftragten des Landes NRW wurde am 07.11.2014 entsprechend beantwortet.

Die GPA NRW hat eine Prüfung der Informationstechnik der Stadt Köln von Dezember 2012 bis Juli 2015 durchgeführt. Die Verwaltung wird zeitnah über die Ergebnisse informieren. Zu den im Amt für Informationsverarbeitung installierten Sicherheitsprozessen bescheinigt uns die GPA einen „hohen“ Standard (auch im interkommunalen Vergleich).

Zu den einzelnen Fragen nimmt die Verwaltung wie folgt Stellung:

Frage 1:
Wie viele Personen arbeiten für die Stadt Köln in den Bereichen der IT-Sicherheit und des Datenschutzes und mit welchen Aufgabengebieten sind sie befasst?

Stellungnahme der Verwaltung:

Die Verantwortlichkeiten für den Datenschutz bei der Stadt Köln sind in den §§ 6 und 7 der Dienstanweisung Datenschutz definiert. Die Stadt hat einen zentralen Datenschutzbeauftragten (§ 32a DSG NRW) und in den Ämtern und Dienststellen dezentrale Datenschutzbeauftragte bestellt. Diese stehen im regelmäßigen Kontakt zum Kompetenzcenter IT-Sicherheit beim Amt für Informationsverarbeitung und zum IT-Sicherheitsverantwortlichen der Stadt Köln.

Im Amt für Informationsverarbeitung ist in der Abteilung Infrastruktur ein eigenes Sachgebiet speziell für die IT-Sicherheit eingerichtet. Hier werden von insgesamt 8 Mitarbeiterinnen und Mitarbeitern u.a. folgende Schwerpunktthemen behandelt:

- Gateway-Security (Contentfilter, Web-Applikations-Firewalls),
- Network-Security (Firewalls, Intrusion Detection/Intrusion Prevention),
- Endpoint-Security (Virenschutz, Festplattenverschlüsselung, etc.),
- Mail-Security (Mail-Gateways, Mail-Routing, Mail-Verschlüsselung, DE-Mail),
- Daten-Sicherheit (Datenverschlüsselung, Zugriffskontrolle, Zugangskontrolle, etc.) und
- Authentifizierungssysteme (div. Authentifizierungstechnologien, Access-Gateway, etc.).

Ergänzend zur Technik werden Sicherheitskonzepte angelehnt an BSI-Grundschutz zur Qualitätssicherung erstellt und der Prozess IT-Sicherheit stetig weiterentwickelt.

Bereits im Jahr 2002 wurde nach den Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) bei der Stadt Köln ein Information Security Management (ISM) aufgebaut und der städtische Beirat für Sicherheit und Kommunikation mit Informationstechnik (SKIT) etabliert. Zu seinen Aufgaben gehören insbesondere die Koordination und Behandlung sicherheitsrelevanter Fragestellungen mit gesamtstädtischer Wirkung und die Erarbeitung von entsprechenden Regelungswerken. Der SKIT erarbeitete unter anderem die IT-Sicherheitspolitik der Stadt Köln, die Dienstanweisungen für den „Betrieb der IT-Infrastruktur“ und „Internet und E-Mail“, sowie das IT-Prüfhandbuch. Sie stellen die organisatorische Grundlage für eine sichere Verarbeitung der städtischen Informatio-

nen.

Im Jahr 2003 wurde zudem die Stelle eines zentralen IT-Sicherheitsverantwortlichen für die Stadt Köln eingerichtet. Dieser ist für alle Fragen der Sicherheit der Informationssysteme bei der Stadt Köln zuständig und fachlich an keine Weisungen gebunden. Die durch das Amt für Informationsverarbeitung und die Fachämter erarbeiteten Sicherheitsanalysen und Sicherheitsbewertungen werden durch den IT-Sicherheitsverantwortlichen qualitätsgesichert und freigegeben. Außerdem überwacht er nach der Inbetriebnahme von Softwareanwendungen die Umsetzung der geforderten Sicherheitsmaßnahmen.

Frage 2:
Sind schon einmal Fälle von Datenmissbrauch, Datenverlust und/oder Datendiebstahl in der Stadt aufgetreten? Wenn ja, wann war das, und welche Daten waren betroffen? Was genau ist danach unternommen worden? Falls nichts unternommen werden konnte, stellen Sie das auch gern kurz dar.

Stellungnahme der Verwaltung:
Die IT-Infrastruktur wird durch eingesetzte Intrusion Detection- und Intrusion Preventionsysteme automatisiert auf Auffälligkeiten überprüft. Dies schließt auch die Prüfung und Kontrolle der Sicherheits-Log-Dateien der eingesetzten Serversysteme, als auch die Prüfungen von beteiligten IT-Komponenten nach einem festgestellten Sicherheitsvorfall (z.B. Virenalarm) ein. Bei diesen Prüfungen gab es bisher keine Hinweise auf unberechtigte Zugriffe auf die städtische Infrastruktur.

Frage 3:
Werden bei der automatischen Datenverarbeitung erforderliche technische und organisatorische Maßnahmen gemäß § 9 BDSG (§ 8 i. V. mit § 32 a Absatz 3 DSG NRW) durchgeführt? Wenn ja, wie sieht das in der Praxis aus?

Stellungnahme der Verwaltung:
Im Rahmen der Betriebsprozesse im Amt für Informationsverarbeitung, die an dem internationalen Standard IT Infrastructure Library (ITIL) orientiert sind, werden standardmäßig im Inbetriebnahmeprozess für alle neuen und sich aufgrund von Versions-Updates verändernden Produkte (Soft- und Hardware) Sicherheitsprüfungen durchgeführt und die entsprechend nach § 10 III DSG-NRW geforderten schriftlichen Dokumentationen für die Sicherheitskonzepte erstellt. Die Hard- und Softwareprodukte werden zusätzlich vor Produktivsetzung anhand der umfangreichen BSI-Grundschutzkataloge auf evtl. Implementierungsschwachstellen überprüft.
Die entsprechenden Dokumente werden durch die Mitarbeiterinnen und Mitarbeiter des IT-Sicherheitsteams des Amtes für Informationssicherheit erstellt und durch den IT-Sicherheitsverantwortlichen der Stadt Köln qualitätsgesichert und freigegeben. Weiterhin wird in den Ablaufprozessen durch vorgeschriebene Mitzeichnungen sichergestellt, dass bei einer Inbetriebnahme oder Veränderungen der IT-Infrastruktur alle Prozessverantwortlichen beteiligt werden.
Bei Verfahren, in denen personenbezogene Daten verarbeitet werden, prüft der zentrale Datenschutzbeauftragte im Rahmen der sogenannten Vorabkontrolle, ob alle vorgeschriebenen technischen und organisatorischen Maßnahmen umgesetzt sind und mögliche Gefahren für das im § 1 DSG NRW geschützte Recht auf informationelle Selbstbestimmung ausgeschlossen bzw. minimiert worden sind.

Frage 4:
Werden den städtischen Mitarbeiterinnen und Mitarbeitern Weiterbildungen im Bereich "Sichere Kommunikation und Datenschutz" angeboten? Wenn ja, welche Inhalte stehen hierbei im Vordergrund? Bestehen vergleichbare Angebote auch für die Beteiligten im Ratszusammenhang?

Stellungnahme der Verwaltung:
Die Sensibilisierung der Mitarbeiterinnen und Mitarbeiter gehört zu den Vorgaben des BSI-Grundschutzes. Dementsprechend werden bei der Stadt Köln verschiedene Schulungen und Informationen zum Thema IT-Sicherheit angeboten. Für die Mitarbeiterinnen und Mitarbeiter ist der Besuch

der Veranstaltung „Sicherer Umgang mit Email und Internet“ Pflicht. Daneben stehen für die Themen Sicherheitsorganisation, IT-Sicherheit und Umgang mit vertraulichen Daten eLearning Programme im Intranet zur Verfügung. Diese Angebote stehen natürlich auch den Mandatsträgern zur Verfügung. Bei Interesse könnten für diese Beteiligten spezielle Informationsangebote entwickelt werden.

Durch den zentralen Datenschutzbeauftragten sind in den Jahren 2004-2008 alle städtischen Mitarbeiterinnen und Mitarbeiter zum Thema Datenschutz bedarfsgerecht geschult worden. Diese Pflichtschulung wird für alle neuen Mitarbeiterinnen und Mitarbeiter fortlaufend durchgeführt. Daneben wird im Rahmen des allgemeinen Fortbildungsangebotes der Stadt Köln für alle städtischen Mitarbeiterinnen und Mitarbeiter das Seminar „Die 20 häufigsten Datenschutzverstöße“ angeboten.

Frage 5:
Wie nimmt der Datenschutzbeauftragte der Stadt Köln http://www.stadt-koeln.de/service/adressen/datenschutzbeauftragter seine Aufgaben in der Praxis wahr?

Stellungnahme der Verwaltung:
Der städtische Datenschutzbeauftragte ist zuständig für alle Fragen, die den Schutz personenbezogener Daten einschließlich der Datensicherheit im Zusammenhang mit der Verwaltungstätigkeit der Stadt Köln betreffen.
Er hat gemäß § 32 a DSG NRW insbesondere folgende Aufgaben:

- Unmittelbarer Ansprechpartner aller Bürgerinnen und Bürger in Fragen zu Datenschutz und Datensicherheit in Zusammenhang mit der Verarbeitung ihrer personenbezogenen Daten bei der Stadt Köln, ferner aller Beschäftigten der Stadt Köln in Angelegenheiten des Arbeitnehmerdatenschutzes sowie der politischen Vertretung,
- Überwachung der städtischen Dienststellen auf die Einhaltung der datenschutzrechtlichen Vorschriften,
- Beratung und Unterstützung der Verwaltungsführung bei der Ausführung des Datenschutzgesetzes Nordrhein-Westfalen (DSG NRW) und anderer datenschutzrechtlicher Vorschriften,
- Beratung und Unterstützung der städtischen Dienststellen einschließlich der Personalvertretung in Angelegenheit des Datenschutzes und der Datensicherheit,
- Federführung in der Korrespondenz mit der Landesbeauftragten für den Datenschutz Nordrhein-Westfalen,
- Führung des Verzeichnisses automatisiert geführter Verfahren für die Gesamtverwaltung gemäß § 32 a Absatz 3 DSG NRW; Gewährung von Einsicht durch berechtigte Personen,
- Beteiligung bei der Planung und Entwicklung (so genannte Vorabkontrolle gemäß § 10 Absatz 3 DSG NRW), Einführung und dem Betrieb von IT-Verfahren zur Verarbeitung personenbezogener Daten,
- Durchführung von so genannten Datenschutzaudits gemäß § 10 a DSG NRW (Prüfung und Bewertung von Datenschutzkonzepten durch unabhängige Gutachten, Veröffentlichung),
- Mitwirkung in Projekten mit datenschutzrelevanten Komponenten, insbesondere bei der Erarbeitung von Satzungen, Dienstvereinbarungen, Geschäftsordnungen, Dienstanweisungen, Richtlinien und Rundschreiben,
- Mitwirkung bei der Entwicklung von Formularen und Makros, mit denen personenbezogene Daten verarbeitet werden, und bei der Formulierung von Verträgen, deren Gegenstand die Verarbeitung personenbezogener Daten ist (zum Beispiel Datenverarbeitung im Auftrag),
- Vertretung der Stadt in externen Arbeitskreisen und Gremien; Teilnahme an internen Arbeitskreisen,
- Entwicklung von Schulungskonzepten und Durchführung von Schulungen zu datenschutzrechtlichen Themen, gegebenenfalls in Zusammenarbeit mit anderen Stellen

gez. Jürgen Roters