Der Oberbürgermeister

Dezernat, Dienststelle
I/12

22.09.2014

Vorlagen-Nummer
2755/2014

Beantwortung einer Anfrage nach § 4 der Geschäftsordnung

öffentlicher Teil

Gremium	Datum
Ausschuss Allgemeine Verwaltung und Rechtsfragen / Vergabe / Internationales	22.09.2014

Offensichtlicher Online-Einbruch von Geheimdiensten in Kölner Unternehmen und städtische Kommunikation: Was tut die Stadtverwaltung?; Beantwortung der Anfrage der Gruppe der Piraten (AN1157/2014) gem. § 4 der Geschäftsordnung des Rates

Die Verwaltung nimmt zu der Anfrage der Gruppe der Piraten wie folgt Stellung:

Frage 1:
Welche Erkenntnisse hat die Stadt zu den aktuellen Vorgängen?

Antwort der Verwaltung:
Die NetCologne GmbH ist als Telekommunikations- und Internetdienstleister Vertragspartner der Stadt Köln. Aufgrund der aktuellen Presseberichterstattung vom 15.09.2014 wurde die NetCologne um Stellungnahme gebeten.
Die NetCologne bestätigte am 18.09.2014, dass die Analyse des Verdachts auf Zugriffe durch ausländische Nachrichtendienste in enger Abstimmung mit den Sicherheitsexperten der Telekom und externen Experten durchgeführt wurde. Sowohl das Bundesamt für Sicherheit in der Informationstechnik (BSI) als auch der Bundesdatenschutzbeauftragte waren eingebunden. Es hat umfassende Überprüfungen gegeben, die ohne Befund geblieben sind. Die im Spiegel angesprochenen Dokumente seien auch mindestens 2 Jahre alt.
Die NetCologne beabsichtigt einen externen Gutachter zu beauftragen, der die intern durchgeführten Maßnahmen, die im Zusammenhang mit den Behauptungen des Magazins Der Spiegel veranlasst wurden, umfassend zu überprüfen. Dieser Ergebnisbericht wird selbstverständlich den Kontrollgremien vorgelegt.

Frage 2:
Welche Unternehmen mit städtischer Beteiligung oder kommunale Einrichtungen des öffentlichen Rechts nutzen Dienstleistungen von NetCologne?

Antwort der Verwaltung:
NetCologne kann grundsätzlich ohne Vorliegen einer entsprechenden Rechtsgrundlage keine Informationen darüber erteilen, welche städtischen Einrichtungen oder Unternehmen unter städtischer Beteiligung bzw. welche kommunalen Einrichtungen des öffentlichen Rechts Dienstleistungen der NetCologne nutzen, da dies eine Weitergabe von grundsätzlich streng geschützten Kundendaten darstellen würde.
Es ist jedoch allgemein bekannt, dass der SWK Konzern mit Rheinenergie, KVB und AWB sowie die Köln Messe zu den Kunden der NetCologne gehören.

Frage 3:
Welche Konsequenzen ziehen diese und die Stadtverwaltung aus den aktuellen Erkenntnissen, und welche Maßnahmen werden geplant, um die Sicherheit der Kommunikations-Infrastruktur und das Vertrauen von Bürgerinnen und Bürgern, Unternehmen usw. in den Datenverkehr mit der Kölner Verwaltung, der Polizeibehörde, dem Jobcenter u.a. wiederherzustellen?

Antwort der Verwaltung:
Die Stadt Köln unterhält ein eigenständiges Netzwerk mit eigenen Datenleitungen und mit eigener TK- und IT- Infrastruktur. Die Telekommunikation und Daten-Kommunikation im städtischen Netz (CAN / Cologne Area Network) läuft somit autonom ausschließlich über eigene IT-Systeme und TK-Anlagen. Dabei wird das städtische Datennetz (CAN / Cologne Area Network) permanent und kontinuierlich durch das Amt für Informationsverarbeitung betreut, aktualisiert und bedarfsorientiert weiter ausgebaut. Hierbei wird ein besonderer Stellenwert auf die IT-Sicherheit gelegt und die Verwaltung verfolgt für ihre Infrastruktur hohe Sicherheitsstandards.

Für Mail- und Datenkommunikation mit Bund, Ländern oder anderen Kommunen wird bereits seit Jahren das sichere Behörden-Netzwerk DOI (Deutschland Online Infrastruktur) verwendet. Das DOI-Netz ist ein vom Bund zur Verfügung gestelltes, geschlossenes Netzwerk, an dem ausschließlich Behörden und Einrichtungen mit entsprechender Sicherheitsüberprüfung teilnehmen dürfen, die vor dem Anschluss vom Bund geprüft werden.

Mail- und Datenkommunikation mit externen Partnern über das Internet durchläuft immer die mehrstufige IT-Sicherheitsinfrastruktur der Stadt Köln, welche aus Content-Filtern, Spam-Filtern, Schadcode-Filtern, Proxy-Systemen, Intrusion Detection Systemen (IDS) und Intrusion Prevention Systemen (IPS) sowie Firewallsystemen besteht. Hierbei sind die Produkte nach dem Multi-Vendor-Prinzip ausgewählt. Dies bedeutet zum Beispiel beim städtischen Virenschutz, dass der Virenscanner eines Herstellers an der Netzwerkgrenze durch einen weiteren Virenscanner eines anderen Herstellers ergänzt und zusätzlich abgesichert wird. Mit dem Multi-Vendor-Prinzip können sowohl Schwachstellen der Hersteller als auch Aktualisierungszeiten (z.B. bei Zero-Day-Attacken) deutlich reduziert werden.

Zudem sind alle Netzzugangspunkte zum stadteigenen Netzwerk konzentriert und werden mit der o.a. IT-Sicherheitsinfrastruktur über 2-Standorte ausfallsicher geschützt. Dabei führt ein Ausfall der IT-Sicherheitsfunktionen zu einem Verbindungsabbruch und nicht zu einem ungeschützten Netzwerkverkehr.

Für Bürgerinnen und Bürger wird zum 01.10.2014 die Stadt Köln ihren Zugang für die De-Mail-Kommunikation eröffnen. Mit De-Mail-Diensten wird der verbindliche und vertrauliche Versand elektronischer Dokumente und Nachrichten für die Bürgerinnen und Bürger deutlich einfacher sein als bisher.

Da die IT-Sicherheit für die Stadt Köln einen sehr hohen Stellenwert hat, wird die Infrastruktur regelmäßig externen Qualitätssicherungen wie z.B. einer Zertifizierung durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) nach ISO 27001 oder Penetrationstests unterzogen.

Frage 4:
Welche weiteren Stellen und Behörden werden nun eingeschaltet, wenn z. B. das zentrale städtische Verwaltungsnetz/CAN gegen unberechtigte externe Zugriffe nicht geschützt ist, da es mutmaßliche Schnittstellen bei NetCologne gibt?

Antwort der Verwaltung:
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 Frage-

stellungen 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 Informationen.

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 der 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.

Die Stadt Köln und der IT-Sicherheitsverantwortliche stehen mit dem BSI, dem Landeskriminalamt und den IT-Sicherheitsverantwortlichen im KDN – Dachverband der kommunalen IT-Dienstleister in NRW im engen Kontakt. Der Arbeitskreis der IT-Sicherheitsbeauftragten im KDN hat einstimmig den Aufbau eines gemeinsamen Computer Emergency Response Teams (CERT) beschlossen. Ein CERT ist die zentrale Anlaufstelle für präventive und reaktive Maßnahmen bei sicherheitsrelevanten Vorfällen in Computer-Systemen. Das Computer-Notfallteam des KDN-CERT besteht aus IT-Sicherheitsspezialisten, die täglich aktuelle Meldungen und Informationen zu Schwachstellen und Bedrohungen auswerten und proaktive sowie reaktive Maßnahmen zur Schadensbegrenzung oder –beseitigung entwickeln und empfehlen.

Daneben wurde im Rahmen der Einsatzplanungen für Großschadensereignisse bei der Stadt Köln mit dem Aufbau einer Projektgruppe Cybercrime und damit verbunden mit dem Aufbau und der Etablierung eines Kölner CERT begonnen. Zukünftige Teilnehmer dieses CERT sollen neben dem Amt für Informationsverarbeitung, der Berufsfeuerwehr der Stadt Köln und dem Amt für Straßen und Verkehrstechnik auch Vertreter aus den Kölner Stadtwerkekonzernen, Energieversorgern und der in Köln ansässigen chemischen Industrie sein.

Frage 5:
Wird die Stadtverwaltung Köln rechtliche Schritte gegen den Angriff auf die Kommunikationsstrukturen einleiten? Dazu gehören mögliche Anzeigen wegen Verstoßes gegen § 202a, 202b, 202c StGB (Vorbereitung, Ausspähen und Abfangen von Daten) oder weiterer relevanter Rechtsnormen.

Antwort der Verwaltung:
Aufgrund der aktuellen Sachlage (vgl. Antwort 1) stellt sich die Frage zurzeit nicht.
Die NetCologne bestätigt, dass sie im Falle eines nachweisbaren Verstoßes gegen die angesprochenen Rechtsnormen rechtliche Schritte einleiten und Strafanzeige erstatten wird.
Dies gilt auch für die Stadt Köln.

Des weiteren wird darauf hingewiesen, dass mit heutiger Ausgabe der Spiegel berichtet, dass die Staatsanwaltschaft Köln im Zusammenhang mit dem Verdacht der Datenausspähung beim Unternehmen Stellar aus Hürth ein Ermittlungsverfahren gegen Unbekannt eingeleitet hat; bzgl. NetCologne und der Deutschen Telekom wurde von der Einleitung eines Ermittlungsverfahrens mangels Anfangsverdacht abgesehen. (s. Anlage)

gez. Kahlen