Der Oberbürgermeister

Dezernat, Dienststelle
I/12

Freigabe am 27.11.2013

Vorlagen-Nummer
3031/2013

Beantwortung einer Anfrage nach § 4 der Geschäftsordnung

öffentlicher Teil

Gremium	Datum
Ausschuss Allgemeine Verwaltung und Rechtsfragen / Vergabe / Internationales	09.12.2013

Der Ausschuss Allgemeine Verwaltung und Rechtsfragen / Vergabe / Internationales hat in seiner Sitzung am 04. November 2013 die Beantwortung zur weiteren Bearbeitung in die Verwaltung verwiesen. Die Antwort der NetCologne liegt zwischenzeitlich vor und ist in die Vorlage eingearbeitet.

Der internationale Überwachungsskandal und die Datensicherheit bei der Stadt Köln Beantwortung der Anfrage der Fraktion DIE LINKE (AN/0990/2013) gem. § 4 der Geschäftsordnung des Rates

Die Verwaltung nimmt zu der Anfrage der Fraktion DIE LINKE. wie folgt Stellung:

Frage 1:

Beschäftigt sich die Verwaltung mit den Auswirkungen der Überwachungsskandale auf die Datensicherheit der Stadt Köln und auf das Recht auf informationelle Selbstbestimmung von Einwohnern und Mitarbeitern der Stadt Köln?

Was sind die bisherigen Aktivitäten und welche Dienststellen sind daran beteiligt?

Antwort:

Wegen der für Sicherheitsfragen erforderlichen, besonderen technischen Fachkenntnisse und der damit verbundenen, dauerhaften organisatorischen Aufgaben und Maßnahmen wurde 2002 der Fachbeirat für Sicherheit und Kommunikation mit Informationstechnik (SKIT) eingerichtet. Die Aufgabe des SKIT beinhaltet insbesondere die Koordination und Behandlung sicherheitsrelevanter Fragestellungen mit gesamtstädtischer Wirkung und die Erarbeitung von entsprechenden Entscheidungen. Damit soll für den Einsatz von Informations- und Kommunikationstechnik in der Stadt Köln ein Sicherheitsniveau gewährleistet werden, das den allgemein anerkannten und für die öffentliche Verwaltung geforderten Qualitätsansprüchen des Bundesamts für Sicherheit in der Informationstechnik (BSI) entspricht. Den externen Kommunikationspartnern soll damit genauso wie den Mitarbeiterinnen und Mitarbeitern der Verwaltung die verlässliche und vertrauenswürdige Nutzung der Informations- und Kommunikationstechnik zur verantwortlichen Erledigung ihrer Aufgaben ermöglicht werden.

Mitglieder des SKIT sind:
- 12 Amt für Informationsverarbeitung
- 12/1 IT-Sicherheitsverantwortliche/r der Stadt Köln
- OB/2 Datenschutzbeauftragte/r der Stadt Köln
- 11 Personal- und Organisationsamt
- 1300 E-Government und Online-Dienste
- 14 – Rechnungsprüfungsamt (in beratender Funktion)
- Vertreter des Gesamtpersonalrates

Um das zentrale städtische Verwaltungsnetz/CAN gegen unberechtigte externe Zugriffe zu schützen setzt die Stadt Köln nach den Empfehlungen des BSI ein Sicherheitsgateway ein, welches zur Absicherung der Netzübergängen in andere öffentliche und nichtöffentliche Netze verwendet wird. Hierbei handelt es sich um eine ganze Reihe von IT-Systemen, die unterschiedliche Aufgaben übernehmen, z. B. Firewall, Schutz vor Viren und die Überwachung des Netzverkehrs im Hinblick auf elektronische Angriffe ("Intrusion Detection"). Durch eine laufende Auswertung und Kontrolle dieser Systeme können Angriffe von außen frühzeitig erkannt und entsprechende Maßnahmen ergriffen werden.

Frage 2:

In welchen Hinsichten sieht die Verwaltung datenschutzrechtliche Belange und das Recht auf informationelle Selbstbestimmung im Verantwortungsbereich der Stadt Köln, bei Aktivitäten der städtischen Mitarbeiter im Internet, in der Kommunikation der Stadt zu anderen öffentlichen Stellen, in der Kommunikation zu Privatpersonen und bei der Nutzung städtischer Onlineangebote und der Köln-App durch Privatpersonen betroffen?

Antwort:

Die Aktivitäten der städtischen Mitarbeiter bei der Internetrecherche und der Nutzung der dienstlichen E-Mails werden in der „Dienstanweisung (DA) mit Umgangs- und Sicherheitsregeln für die Nutzung von Arbeitsplatzrechnern mit Zugang zum städtischen Netzwerk (CAN), E-Mail und Internetnutzung sowie Fax-Kommunikation“ geregelt. Die hier definierten Vorschriften zum sicheren Umgang bei der Internet- und Email-Nutzung werden seit 2004 in regelmäßigen Schulungen (an der alle Mitarbeiter/innen mit Internetrechten teilnehmen müssen) erklärt. Internetzugriffe erfolgen aus der Stadtverwaltung grundsätzlich über einen sogenannten Proxyserver. Aus Sicherheitsgründen ist ausschließlich dieser Proxyserver in der Firewall für die Kommunikation über unsichere Netze freigeschaltet. Im Internet kommuniziert die Stadtverwaltung über eine IP-Adresse. Zuordnungen zu einzelnen Mitarbeitern des Stadt Köln können von außen nicht hergestellt werden.

Bei den Pflichtschulungen zum Datenschutz werden die Mitarbeiter/innen durch den städtischen Datenschutzbeauftragten darauf hingewiesen, dass bei der Mailkommunikation mit Bürgerinnen und Bürgern keine personenbezogenen Daten versendet werden dürfen.

Die Kommunikation der Stadt zu anderen öffentlichen Stellen wird ausschließlich über die Deutschland-Online Infrastruktur (DOI) durchgeführt. Das DOI ist eine deutschlandweite Kommunikationsinfrastruktur für alle Behörden der Deutschen Verwaltung, die eine ebenen-übergreifende sichere Kommunikation zwischen Bundesnetzen, den Ländernetzen und Netzen der Kommunen ermöglicht. Zur Absicherung der Kommunikation realisiert das DOI neben der reinen Netz-Zugangsdienstleistung verschiedene weitere Basis- und Mehrwertdienste wie E-Mail-Relay, DNS, Krypto-Management, PKI-Dienste und Verzeichnisdienste.

Die Dienstleitungsangebote auf den Webplattformen Stadt-Koeln.de, koeln.de und Cologne.de unterteilen sich in reine Informationsangebote und Angebote zur Nutzung von Verwaltungsdienstleistungen. Die Webserver werden durch die Firma Netcologne im Auftrag gehostet. Grundsätzlich wird bei Dienstleistungsangeboten, bei denen personenbezogene Daten ausgetauscht werden, mittels HTTPS-Protokoll gesichert.

Die Stadtverwaltung Köln bietet folgende Möglichkeit der E-Mailverschlüsselung an. Ämter können den SMTP-Transport für offizielle E-Mail-Poststellen im Internet bis zum Empfänger automatisiert verschlüsseln (S/MIME). Bisher nutzen folgende zentralen Poststellen diese Funktionalität:

- 322-10-gueterverkehr@stadt-koeln.de
- fachdienst-fuer-pflegebeduerftige-503-21@stadt-koeln.de
- sozialamt.aokaustausch@stadt-koeln.de
- sozialamt.heimaufsicht@stadt-koeln.de
- vps@stadt-koeln.de (Zugangseröffnung)

Innerhalb des sicheren CAN werden die Inhalte unverschlüsselt transportiert, so dass alle vorhandenen Schutzmaßnahmen (z.B. Virenschutzsoftware zum Auffinden und deaktivieren von eingeschleuster Spionagesoftware) zum Einsatz kommen können.

Die Dienstleistungsangebote auf den Webplattformen Stadt-Koeln.de, koeln.de und Cologne.de unterteilen sich in Informationsangebote und Angebote zur Nutzung von Verwaltungsdienstleistungen und werden durch die Firma Netcologne im Auftrag gehostet. Hierbei sind alle Internetdienstleistungen, bei denen datenschutzrechtlich relevante Inhalte ausgetauscht werden, durch eine SSL-Verschlüsselung gesichert.

Frage 3:

Welche Maßnahmen hält die Verwaltung für vorstellbar, um den nun bekannten Gefahren für die Datensicherheit und das Recht auf informationelle Selbstbestimmung zu begegnen und den Schutz von Daten in Bezug auf die unter 2. genannten Bereiche zu erhöhen?

Antwort:

Zur weiteren Erhöhung der Sicherheit bei der elektronischen Kommunikation mit Bürgerinnen und Bürgern kann die verstärkte Nutzung von De-Mail geprüft werden. De-Mail ist der einfache Weg um elektronisch rechtssicher, vertraulich und verbindlich zu kommunizieren. Im Unterschied zur E-Mail ist De-Mail ein verschlüsselter Kommunikationsdienst und ermöglicht den sicheren Versand von offiziellen Dokumenten übers Internet. Die Nutzung ist aber in starkem Maße von der Akzeptanz zur Nutzung dieser kostenpflichtigen Kommunikation durch die Bürgerinnen und Bürgern abhängig.

Bei der Ausschreibung für den nächsten städtischen Mailprovider werden die Sicherheitsaspekte der Anbieter ein besonderes Entscheidungskriterium darstellen. Die Initiative „E-Mail made in Germany“ unter Federführung der Firmen Telekom, GMX und Web.de geben erste Anhaltspunkte für eine verbesserte Dienstleistung bei der IT-Sicherheit.

Frage 4:

Wie schätzt die Verwaltung in diesem Zusammenhang die folgenden Maßnahmen ein:

a. Erreichbarkeit aller Seiten der Domain stadt-koeln.de, der Domain koeln.de und cologne.de über HTTPS und eventuell die komplette Umstellung dieser Domains auf HTTPS,

Antwort:

Zu dieser Frage wurde die Firma NetCologne als städtischer Provider um Stellungnahme gebeten. Die NetCologne antwortet wie folgt:

Für die Nutzung verschlüsselter Verbindungen im Bereich von koeln.de wird eine Reihe von SSL-Zertifikaten je nach Bedarf für die folgenden Hostnamen
genutzt:
- www.koeln.de (Web)
- secure.koeln.de (Web)
- webmail.koeln.de (Webmail: Mailbearbeitung, Benutzerkonten)
- mail.koeln.de (Mail: IMAP, POP, SMTP)
- seit 09-2013: mailin.koeln.de (Mail - Server zu Server-Verschlüsselung)

Die Verschlüsselung wird eingesetzt, wo konkrete Benutzerdaten übermittelt werden, beispielsweise bei der Webmail, der sonstigen E-Mail- Benutzung mittels eigener Mailprogramme, der Benutzerverwaltung von Brancheneinträgen o.ä.

Darüber hinaus sind die Inhalte der Informationsportale koeln.de und cologne.de per Definition grundsätzlich öffentlich, nicht vertraulich und nicht behördlicher Natur. Sie können anonym und ohne jegliche Registrierung oder Datenspeicherung genutzt werden. Die praktische oder rechtliche Not-

wendigkeit einer Verschlüsselung besteht daher grundsätzlich für diese Webauftritte über das oben genannte Maß hinaus nicht.

b. Unterstützung von Perfect Forward Secrecy auf den HTTPS-unterstützenden Seiten der Domains stadt-koeln.de und koeln.de,

Antwort:

Zu dieser Frage wurde die Firma NetCologne als städtischer Provider um Stellungnahme gebeten.

Die NetCologne antwortet wie folgt:
Die zusätzliche Nutzung der sogenannten "Perfect Forward Secrecy" überall dort, wo bereits Verschlüsselung zum Einsatz kommt, ist noch in der Erprobung. Wo möglich, werden die für PFS erforderlichen Verschlüsselungsmethoden aktiviert und optional angeboten.

Die Nutzung dieser Methoden ist jedoch auch abhängig davon, dass die verwendeten Clientprogramme (Webbrowser und E-Mail-Programme) sie unterstützen. Bis das flächendeckend der Fall ist, wird PFS nur zusätzlich und mit der Möglichkeit, auch auf andere Verschlüsselungsmethoden zurückzufallen, angeboten.

c. Verwendung von SMTP TLS (Transport Layer Security) auf den Mail-Servern der Stadt Köln, von koeln.de und von cologne.de,

Antwort:

Zu dieser Frage wurde die Firma Netcologne als städtischer Provider um Stellungnahme gebeten. Siehe hierzu auch 2.Absatz der Antwort zu Frage 3.

Die NetCologne antwortet wie folgt:
Für den Bereich der E-Mail gehört das Angebot eines verschlüsselten Zugriffs schon seit geraumer Zeit zum Standard bei koeln.de. Die browserbasierten Webmail wird ausschließlich verschlüsselt (https) angeboten, hier kann von einer weitgehenden Kompatibilität aller verwendeten Benutzerprogamme ausgegangen werden.

Bei der Benutzung eigener Mailprogramme mit dem koeln.de-Mailsystem wird die Verschlüsselung für die Protokolle IMAP, POP und SMTP optional angeboten, aber nicht erzwungen. Fast alle aktuellen Mailprogramme sind jedoch so eingestellt, dass sie bei Vorhandensein der Verschlüsselung diese auch nutzen.
Die Weiterleitung von Mail an externe Mailadressen erfolgt immer dann verschlüsselt (SMTP/TLS), wenn die jeweilige Gegenstelle dies unterstützt.

Für eingehende Mail, die von externen Adressen an koeln.de-Adressen eingeliefert wird, wurde die Beschaffung und Aktivierung eines SSL-Zertifikats kürzlich abgeschlossen. Seit dem 03.09.13 kann also auch eingehende Mail im Server-to-Server-Verkehr verschlüsselt empfangen werden. Wie bei der ausgehenden Mail muss jedoch auch hier die Gegenseite die Verschlüsselung unterstützen.

d. Möglichkeit, auf Wunsch mit Mitgliedern der Stadtverwaltung mittels PGP-verschlüsselter E-Mails zu kommunizieren,

Antwort:

Innerhalb der Stadtverwaltung ist die Nutzung der Maildienste @stadt-koeln.de sicher. Unautorisierte Zugriffe von außen werden nach den aktuellen technischen Möglichkeiten geschützt.

Für Fraktionsmitglieder steht die in Outlook integrierte E-Mail-Verschlüsselungsanwendung GnuPG für den eigenverantwortlichen Einsatz bereit. Dabei wird eine clientseitige Verschlüsselung umge-

setzt, welche einen ausschließlich auf dem lokalen Client befindlichen Virenschutz aufweist und im Falle des Verlusts des Schlüssels/Passworts keine Widerherstellungsmöglichkeit bietet.

e. die Verwendung anonymisierender Browser in der Stadtverwaltung,

Antwort:

Internetzugriffe erfolgen aus der Stadtverwaltung grundsätzlich über einen sogenannten Proxyserver. Aus Sicherheitsgründen ist ausschließlich dieser Proxyserver in der Firewall für die Kommunikation über unsichere Netze freigeschaltet. Im Internet kommuniziert die Stadtverwaltung über eine IP-Adresse. Zuordnungen zu einzelnen Mitarbeitern des Stadt Köln können von außen nicht hergestellt werden. Die Verwendung anonymisierender Browser ist somit nicht notwendig. Siehe hierzu auch 1.Absatz der Antwort zu Frage 2.

f. einen Verzicht auf gefährdete Online-Dienste,

Antwort:

Die Notwendigkeit, aus dienstlichen Gründen auf gefährdete Online-Dienste zugreifen zu müssen, kann nur durch die Dezernate und Fachämter entschieden werden. Es werden alle realisierbaren technischen Möglichkeiten, eine genehmigte Kommunikation abzusichern, genutzt. Ein geringes Restrisiko kann nicht ausgeschlossen werden kann.

g. einen Verzicht auf Software der oben genannten Unternehmen und den Einsatz von Software mit offenem Quellcode?

Antwort:

Aufgrund der großen Komplexität heutiger Software- und Betriebssysteme sind Fehler bei der Entwicklung nur schwer zu vermeiden. Es ist zu beobachten, dass hohe Erwartungen der Anwender und zeitlich zu knapp bemessene Erscheinungstermine bei Standardsoftwareprodukten auch dazu führen, dass die Hersteller ihre Produkte teilweise unausgereift oder nicht fehlerfrei anbieten. Dies ist gerade im Bereich von neuen Betriebssystemversionen bekannter Marktanbieter zu beobachten.

Auch bei OpenSource Produkten wie SUSE Linux kommt es bei den Veröffentlichungen von neuen Versionen immer wieder zu Verzögerungen. Grund hierfür ist, dass die Zahl der Suse-Entwickler wie auch die Menge der durch die Nutzer eingeschickten Patches ständig gewachsen ist. Es fehlen auch hier erfahrene Entwickler, die eine intensive Prüfung der Funktionalität und eventueller vorhandener Sicherheitslücken durchführen.

Die ausschließliche Nutzung von OpenSource-Produkten verbessert die Sicherheitssituation und Gefährdungen z.B. durch nicht erkannte Sicherheitslücken (ZeroDay-Exploits) nicht.

gez. Kahlen