Der Oberbürgermeister

Dezernat, Dienststelle
I/12

04.02.2015

Vorlagen-Nummer
3850/2014

Beantwortung einer Anfrage nach § 4 der Geschäftsordnung

öffentlicher Teil

Gremium	Datum
Rat	05.02.2015
Ausschuss Allgemeine Verwaltung und Rechtsfragen / Vergabe / Internationales	16.03.2015
Unterausschuss Digitale Kommunikation und Organisation	10.03.2015

Schutz vor Angriffen auf kommunale IT-Systeme in Köln; Beantwortung der Anfrage der Gruppe der Piraten (AN/1805/2014) gem. § 4 der Geschäftsordnung des Rates

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

Die unter Punkt 1 definierten Fragen beziehen sich auf unterschiedliche Verwaltungsträger mit unterschiedlichen IT-Infrastrukturen, Schutzbedarfen und einer eigenständigen Zuständigkeit.
Die nachfolgenden Antworten beziehen sich auf den Verantwortungsbereich der Stadtverwaltung Köln infolge auf die IT-Infrastruktur des Cologne-Area-Networks (CAN).

Das Angebot des BSI zur Durchführung von Penetrationstests und/oder Web-Checks richtet sich im Wesentlichen an Bundesbehörden und Ministerien. Als Ausnahme bietet das BSI an, diese Tests auch bei Organisationen durchzuführen, die im besonderen öffentlichen Interesse stehen und bereits angegriffen wurden. Das Verwaltungsnetz der Stadt Köln steht sicher im besonderen öffentlichen Interesse, wurde allerdings – entgegen der in der Anfrage aufgestellten Behauptung – nicht korrumpiert. In den angesprochenen Snowden-Dokumenten gibt es keine Hinweise auf Zugriffe von Geheimdiensten wie dem britischen GCHQ auf Systeme der Stadtverwaltung Köln, noch wurden durch die im Verwaltungsnetz eingesetzten Überwachungssysteme (Intrusion-Prevention- und Intrusion-Detection-Systeme) Hinweise auf solche Angriffe registriert. Grundsätzlich entfällt damit eine Voraussetzung für das BSI-Angebot.
Am 15.12.2014 wurde durch den IT-Sicherheitsbeauftragten der Stadt Köln die mögliche Durchführung eines Penetrationstests und/oder Web-Checks bei der Stadt Köln durch das BSI erfragt. Das BSI lehnte diese Anfrage am 06.01.2015 mit Hinweis auf die begrenzten personellen Kapazitäten und die Vorrangigkeit von Bundesbehörden ab.

Frage 1-Frage 3::
Werden die IT-Systeme in der kommunalen Verwaltung, den kommunalen Unternehmen und den kommunalen Einrichtungen (Bibliotheken, Schulen, Jobcenter usw.) mithilfe von Penetrationstests und Webchecks regelmäßig überprüft? (Wenn nicht, begründen Sie bitte, warum nicht.)
Die IT-Systeme welcher kommunaler Einrichtungen, Behörden usw. wurden in den letzten fünf Jahren Penetrationstests und Webchecks unterzogen? (Bitte unter Angabe des Test-Datums.)
Welche Ergebnisse haben diese Tests ergeben? (Bitte nennen sie die gefundene Schwachstelle, wenn möglich.)

Antwort der Verwaltung:
Im Rahmen der nach einem internationalen Best-Practise-Standard (ITIL) organisierten Betriebsprozesse im Amt für Informationsverarbeitung werden standardmäßig im Inbetriebnahmeprozess für alle neuen Produkte (Soft- und Hardware) Sicherheitsprüfungen durchgeführt. Die Produkte werden zusätzlich vor Produktivsetzung anhand der umfangreichen BSI-Grundschutzkataloge auf evtl. Sicherheitslücken bzw. Implementierungsschwachstellen überprüft.
In den besonders gefährdeten Netzzonen der Stadt Köln sind ergänzend Intrustion Detection / Prevention-Systeme im Einsatz, die Angriffe auf Softwareschwachstellen erkennen und eindämmen können.
Im Rahmen der Zertifizierung eines Fachverfahrens zur elektronischen Unterstützung des Personenstandswesens wurde in 2014 eine Qualitätssicherung folgender Rechenzentrums-Bereiche durch einen externen Auditor und das BSI durchgeführt

- Sicherheitsmanagement (inkl. Sicherheitsprozessen)
- Gebäudeinfrastruktur Rechenzentren
- Server, Clients, Datenbanken, Dokumentenmanagement, Archivierung
- Netzwerkinfrastruktur
- Sicherheitsinfrastruktur einschließlich Firewall, Virenschutz und Detektion-Systemen

Das Zertifikat mit der ISO 27001-Prüfung auf Basis von IT-Grundschutz wurde am 02.10.2014 vom BSI ausgestellt.

Seit Anfang 2014 ist die Durchführung eines großen Penetrationstests für die sensible Webinfrastruktur inkl. aller nachgelagerten Komponenten projektiert, die Durchführung selbst ist für 2015 vorgesehen. Zur ergänzenden Qualitätssicherung wird eine Ausschreibung zur Durchführung des Tests durch externe Sicherheitsspezialisten erfolgen; geplant ist hier der Einsatz von BSI-zertifizierten Penetrationstestern.

Frage 4:
Welche Maßnahmen wurden aufgrund der Testergebnisse ergriffen, und wurden diese schon umgesetzt?

Antwort der Verwaltung:
Die Ergebnisse des geplanten Penetrationstests werden in den beim Amt für Informationsverarbeitung etablierten IT Security Management Prozess nach ITIL einfließen. Dabei wird überprüft, ob die Sicherheitsmaßnahmen und –Prozeduren immer noch im Einklang stehen mit den in den Sicherheitskonzepten bestimmten Risikoeinschätzungen. Die bereits getroffenen und umgesetzten Sicherheitsmaßnahmen werden dann aufgrund der gewonnenen Erkenntnisse gegebenenfalls erweitert oder angepasst.

Frage 5:
Wäre eine Vorführung eines Pentrationstesters und Webcheckers oder ein Hearing im Rat der Stadt Köln möglich, um die Mitarbeiter der Stadtverwaltung für Datensicherheit zu sensibilisieren?

Antwort der Verwaltung:
Die Stadt Köln gehört aufgrund der Komplexität der IT-Infrastruktur und der Vielzahl von bereitgestellten Services zu den größeren IT-Dienstleistern. Sowohl Penetrationstests als auch sog. Web-Checks liefern umfangreiche Informationen zum Sicherheitsstatus der eingesetzten IT-Systeme. Diese Tests basieren auf umfangreichen Informationsrecherchen und werden mit verschiedenen Tools durchgeführt und gegengeprüft. In der Regel laufen beide Testvarianten über mehrere Stunden bzw. Tage, je nach geprüfter Infrastruktur.
Effektiv sind die Tests, wenn sie im Produktivumfeld durchgeführt werden. Daher müssen Maßnahmen zur Aufrechterhaltung der Dienstleistungen und dem ordnungsgemäßen Dienstbetrieb eingeplant und sichergestellt werden. Aus diesem Grund werden die notwendigen Tests und Manipulationsversuche in den Nachtstunden bzw. am Wochenende durchgeführt. Die Auswertung erfordert im Anschluss ebenfalls noch einmal einen großen Zeitaufwand. Unter anderem aus diesen Gründen eignen

sich Penetrationstests und Web-Checks grundsätzlich nicht für eine Livevorführung.
Die Live-Präsentation eines Penetrationstest ist nicht realisierbar. Die Rückmeldungen der eingesetzten Tools erfolgen nicht im Klartext und erfordern eine nachfolgende fachliche Auswertung, Aufbereitung und Interpretation der Meldungscodes. Sie haben keinen direkten Informationswert für die angesprochene Zielgruppe.

gez. Jürgen Roters