Stadt Köln

Der Oberbürgermeister

Dezernat, Dienststelle
I/12

Vorlagen-Nummer28.01.2013
0336/2013

Beantwortung einer Anfrage nach § 4 der Geschäftsordnung

öffentlicher Teil

Gremium	Datum
Unterausschuss Informations- und Kommunikationstechniken	28.01.2013
Ausschuss Allgemeine Verwaltung und Rechtsfragen / Vergabe / Internationales	28.01.2013

Beantwortung einer Anfrage der FPD-Fraktion AN/0146/2013 "Hackerangriff auf die Einwohnerdatenbank der Stadt Köln"

Die FDP-Fraktion hat folgende Anfrage an den UA IuK gestellt:

Mit Bezug auf die Berichterstattung im Kölner Stadt Anzeiger bittet die FDP-Fraktion um Beantwortung folgender Fragen:

1. Inwieweit hat nur ein Angriffsversuch stattgefunden oder wurde erfolgreich auf personenbezogene Daten zugegriffen?
2. Inwieweit liegt mittlerweile eine IT-forensische Analyse des Vorfalls vor und was sind die wesentlichen Ergebnisse daraus?
3. Welche Erkenntnisse konnten ermittelt werden (z.B. Identität bzw. Profil des Angreifers; Ursprung, Muster und Durchführung des Angriffs; Dauer und Umfang; potentielles Tatmotiv; potentielle Schäden)?
4. Wurde dieser oder ein ähnlicher Angriff nochmals erkannt?
5. Welche Verbesserungsmaßnahmen wurden bereits initiiert und sind zukünftig vorgesehen?

Die Verwaltung nimmt wie folgt Stellung:

Zu Frage 1

Nach Abschluss der Untersuchungen kann zweifelsfrei festgestellt werden, dass es keinen Angriffsversuch und demzufolge auch keinen erfolgreichen Zugriff auf personenbezogene Daten gegeben hat. Die Ursache für den Ausfall der Anwendung war ein technisches Problem der Datenbank.

Das Fehlerbild stellte sich zunächst so dar, als ob der Zugriff auf das Einwohnerwesen, auf den sogenannten Haupt-User-Account, über den alle zugelassenen Mitarbeiterinnen und Mitarbeiter auf das Einwohnerwesen zugriffberechtigt werden, gesperrt gewesen wäre. Später wurde jedoch festgestellt, dass die Anwendung insgesamt bzw. der Zugriff auf die Einwohnerdatenbank insgesamt unterbrochen war. Da zu diesem Zeitpunkt aufgrund des Publikumsverkehrs die Störungsbeseitigung höchste Priorität hatte, wurde die betroffene Datenbankinstanz neu gestartet. Danach war die Anwendung wieder verfügbar.

Als Auslöser für den Ausfall der Datenbank bzw. genauer gesagt für den fehlenden Zugriff auf die Daten wurde im Nachhinein ein Hintergrundprozess des Datenbank-

Managementsystems ausgemacht, der die Einwohnerdatenbank immer wieder versuchte, neu zu starten, bis ein im System implementierter Zähler von 999 Prozessen erreicht war. Danach war das Einwohnerwesen nicht mehr betriebsbereit. Eine entsprechende Störungsanzeige per Mail wurde wegen der Betriebsferien nicht wahrgenommen.

Der als Fehlerursache identifizierte Prozess dient u.a. der Performanceverbesserung. Er bearbeitet auch die Anfragen des datenbankeigenen Überwachungs-Agenten. Da dieser Prozess nach dem Ausfall keine Informationen mehr zum Zustand der Datenbank lieferte, wurden auch keine Alarme mehr gesendet.

Zu Frage 2

Die IT-forensische Prüfung wurde bereits am 27.12.2012 begonnen und am 02.01.2013 abgeschlossen. Es handelt sich hierbei um ein Standardvorgehen, welches mit dem IT-Sicherheitsverantwortlichen für solche Fälle festgelegt worden ist. In die Überprüfung wurden folgende Sicherheitssysteme einbezogen:

- Überprüfung der Firewall-Log-Einträge (Außenfirewall) auf Besonderheiten und Auffälligkeiten wie z.B. vermehrte Anfragen auf die IP-Adresse des Webservers (Denial-of-Service), ungewöhnliche Quell-IP-Adressen, etc. Es konnten keine Auffälligkeiten festgestellt werden.
- Überprüfung des E-Mail-Postfachs Antivirus auf mögliche Meldungen von Schadcode auf den beteiligten Serversystemen. Auch hier konnten keinerlei Auffälligkeiten festgestellt werden.
- Überprüfung des Intrusion Prävention Systems auf Auffälligkeiten im Datenstrom, welche auf einen Angriff schließen lassen könnten. Es konnten keine Auffälligkeiten festgestellt werden.
- Überprüfung der Firewall-Log-Einträge (Innere Firewall) auf Besonderheiten, ebenfalls ohne dass Auffälligkeiten festgestellt werden konnten.

Zu Frage 3

Entfällt, da es keinen Angriff gab.

Zu Frage 4

Es ist bisher auch kein ähnlicher Fall bei der Stadt Köln erkannt worden.

Zu Frage 5

In Zukunft wird organisatorisch dafür Sorge getragen, dass bei längeren Unterbrechungen des Dienstbetriebs auch zu Beginn der Rufbereitschaft die Verfügbarkeit der Dienste und Anwendungen proaktiv überprüft wird.

Hinsichtlich der Optimierung der automatisierten Systemüberwachung wird ein Skript im Oracle Enterprise Manager (OEM) implementiert, das für den identifizierten Prozess die Anzahl der Prozesse kontrolliert und bei Überschreitung eines Schwellwertes eine automatisierte Störungsmeldung an die Bereitschaftskräfte auslöst.

Sofern die Haushaltsmittel dafür bereit gestellt werden können, wird in 2013 eine Zertifizierung des RZ-Betriebs nach BSI-IT-Grundschutz auf der Basis von ISO 27001 gestartet. Entsprechende Planungen wurden bereits vor dem Störfall im Dezember verabschiedet und in die Haushaltsplanungen eingebracht.

gez. Kahlen