Stadt Köln

Der Oberbürgermeister

Dezernat, Dienststelle
I/12

Vorlagen-Nummer 24.10.2014
3000/2014

Beantwortung einer Anfrage nach § 4 der Geschäftsordnung

öffentlicher Teil

Gremium	Datum
Ausschuss Allgemeine Verwaltung und Rechtsfragen / Vergabe / Internationales	03.11.2014

Auswirkungen der Sicherheitslücke "Shellshock" auf die IT der Stadt Köln; Beantwortung der Anfrage (AN/1245/2014) der FDP-Fraktion gem. § 4 der Geschäftsordnung des Rates

Die Verwaltung nimmt wie folgt Stellung:

Frage 1:
Sind (bzw. waren) die IT-Systeme der Stadt Köln bzw. die eines beauftragten Dienstleisters von Shellshock selber oder verwandten Sicherheitslücken betroffen? Falls Ja:

Antwort:
Unmittelbar nach Veröffentlichung der Sicherheitslücke(n) Shellshock wurden intensive Prüfungen der UNIX basierenden Systeme durchgeführt, es gab keine Hinweise darauf, dass die IT-Infrastruktur der Stadt Köln kompromittiert wurde.

Externe Dienstleister der Stadt Köln stellen für einzelne Anwendungen Dienste außerhalb des Netzwerkes der Stadt Köln bereit und werden über entsprechende Verträge verpflichtet, die Vorgaben des Bundesamtes für Sicherheit in der Informationstechnik (BSI) umzusetzen.

Erläuterung:
Am 24. September 2014 wurde die Sicherheitslücke „Shellshock“ und nachfolgende ähnliche Angriffsszenarien veröffentlicht. Dieser Typ Sicherheitslücke ermöglicht einem Angreifer Programmiercode in Systeme einzubringen, der beim Start eines neuen Unix-Kommandofeldes (Unix-Shell) ungeprüft ausgeführt wird und somit unter Umständen weitreichende Rechte ermöglicht oder Schadcode implementieren kann.
Betroffen sind grundsätzlich alle Systeme, die auf der Basis von Unix arbeiten, darunter fallen bei der Stadt Köln alle Linux-Server und einige sog. Appliances (speziell auf Hardware optimierte Software) welche auf Unix basieren und dann von den jeweiligen Herstellern auf spezialisierte Funktionen angepasst wurden.

Im Rahmen der Einführung von ITIL-Prozessen* (Pro) Ende der 90er Jahre im Amt für Informationsverarbeitung der Stadt Köln wurde für alle eingesetzten Softwareprodukte, und somit auch Betriebssysteme, ein sogenannter Patch Management-Prozess etabliert. Dieser sorgt dafür, dass veröffentlichte Sicherheitslücken möglich schnell geschlossen werden und dieser Vorgang dabei auch überwacht wird.

Ein Restrisiko besteht in dem Zeitraum zwischen der Veröffentlichung einer Sicherheitslücke und ihrem Schließen durch die Installation eines Hotfixes. In der Praxis ist es den Herstellern jedoch technisch nicht immer möglich, kurzfristig Lösungen bereitzustellen.
Um dieses Restrisiko für die Stadt Köln zu minimieren sind sog. Intrusion-Prevention- und Intrusion-Detection-Systeme (IPS/IDS-Systeme) ergänzend zu den eingesetzten Firewall-Systemen in das Netzwerk der Sicherheitsinfrastruktur integriert. Diese Systeme erkennen definierte Angriffsmuster und wehren diese ab.

Grundsätzlich werden Serversysteme und Anwendungen, die für einen Internetauftritt bereitgestellt werden, in mehreren Sondernetzen vom internen Netzwerk autonom und getrennt voneinander betrieben. Die Systeme selbst werden zur Reduzierung der Angriffsfläche standardmäßig gehärtet und nach dem Minimalprinzip installiert, sodass ausschließlich die benötigten Rechte und Dienste installiert werden.

Im Falle der ersten Shellshock-Sicherheitslücke wurden für die Linux-Server bereits am folgenden Tag nach Bekanntwerden Hotfixes bereitgestellt, für einige andere Komponenten ist dies ein paar Tage später inklusive der Folgepatches erfolgt. Für den Zeitraum zwischen der Veröffentlichung und dem Patchen wurden die o.a. Intrusion-Prevention-Systeme für die Shellshock-Lücke scharf geschaltet.

Frage 2:
Welche diesbezügliche(n) Sicherheitslücke(n) wurden bekannt und welche (ausgelagerten) Systeme waren davon wie betroffen?

Antwort:
entfällt aufgrund der Ausführungen zu Frage 1

Frage 3:
Waren insbesondere Web- und/oder DHCP- Server betroffen?

Antwort:
Grundsätzlich waren alle auf Unix-basierende Serversysteme betroffen, folgend auch Webserver. Für DHCP werden ausschließlich Windows-Server mit dem entsprechenden Microsoft-Betriebssystemen eingesetzt.

Frage 4:
Welche Gegenmaßen wurden wann getroffen?

Antwort:
entfällt aufgrund der Ausführungen zu Frage 1

Frage 5:
Welche Schäden, insbesondere auch Imageschäden, sind dadurch entstanden?

Antwort:
entfällt aufgrund der Ausführungen zu Frage 1

*(ITIL steht für IT Infrastructure Library. Das ist das best practice framework, das PRO zugrunde liegt. Es handelt sich dabei um einen international anerkannten De-Facto-Standard für die Ablauforganisation in der IT-Serviceerbringung. PRO steht für Prozesse, Rollen und Organisation)

gez. Kahlen