Universitätsstadt Gießen
Stadtverordnetenversammlung

Büro der Stadtverordnetenversammlung

Anfrage

Vorlagennummer: **ANF/1633/2013**
Öffentlichkeitsstatus: öffentlich
Datum: 09.07.2013

Amt: Büro der Stadtverordnetenversammlung
Aktenzeichen/Telefon: - Al -/1032
Verfasser/-in: Christian Oechler, Piraten-Fraktion

Beratungsfolge	Termin	Zuständigkeit
Magistrat		Zur Kenntnisnahme
Stadtverordnetenversammlung		Zur Kenntnisnahme

Betreff:
Anfrage gem. § 28 GO des Stv. Oechler vom 09.07.2013 - IT-Sicherheit -

Anfrage:
„Für die PIRATEN-Fraktion stelle ich nachfolgende Fragen an den Magistrat und bitte um Weiterleitung.

Sicherer Aufruf der Website:

1. Warum bietet die Universitätsstadt Gießen keine Möglichkeit an, die Website www.giessen.de über eine gesicherte Verbindung (https://) zu besuchen?
2. Ist es seitens der Verwaltung geplant, dass dies zukünftig möglich ist? Wird es dabei eine Zwangsumleitung auf die so gesicherte Website geben, um sicherzugehen, dass an die Stadt Gießen übertragene Nutzerdaten nicht unverschlüsselt übertragen werden?
3. Soll dabei ein Extended-Validation-Zertifikat zum Einsatz kommen, damit die Besucher schon in ihrer Adresszeile des Browsers die Integrität der Verbindung zur Stadt Gießen erkennen können?
4. Wird dabei an das - durch Prism und Tempora nicht mehr ganz so unrealistische - Szenario einer Man-in-the-Middle-Attacke gedacht und die Verwendung von ‚Perfect Forward Secrecy' in Betracht gezogen?
5. Wie werden an die Stadt Gießen übertragene Nutzerdaten gespeichert und welche Verschlüsselungsmethoden werden dabei verwendet, um sicherzustellen, dass im Falle einer technischen Kompromittierung so wenige persönliche Daten wie möglich entwendet und verwertet werden können?

E-Mail-Verkehr:

1. Ist die Universitätsstadt Gießen in der Lage, verschlüsselte E-Mails zu empfangen, zu bearbeiten und auch verschlüsselt zu senden?
2. Falls nein, ist es geplant, dies einzuführen? Wenn ja, wann ist die Einführung geplant? Wenn nein, warum nicht?

Arbeitsplätze der Bediensteten:

1. Gibt es einen IT-Sicherheitsplan (der z.B. kritische Daten definiert, die Datensicherung regelt, Nutzerrechte definiert, auf den Krisenplan verweist, etc.), der regelmäßig überarbeitet und an alle städtischen Angestellten kommuniziert wird?
2. Ist es Bediensteten möglich, externe Datenträger (CD, DVD, Blu-ray, USB-Sticks) an die Informationssysteme der Stadt anzuschließen? Wenn ja, wie werden Sicherheit und Integrität des städtischen EDV-Systemes gewährleistet?
3. Können Bedienstete eigene Software installieren?
4. Sind die Computer mit zeitgemäßem Viren- und Spamschutz ausgestattet? Wenn nein, warum nicht?
5. Werden die Festplatten der städtischen Arbeitsplatzrechner verschlüsselt? Wenn nein, warum nicht?

Penetration des Gesamtsystems:

1. Gab es bereits bemerkte, erfolgreiche Angriffe durch Hacker auf Computersysteme der Stadtverwaltung? Wenn ja, welche Auswirkungen hatten diese?
2. Werden die Netzwerke der Stadt Gießen Penetrationstests unterzogen?
3. Haben die Mitarbeiter der Stadt Gießen Handreichungen zu Gefährdungspotenzialen durch Social-Engineering-Angriffe? Wurden die Mitarbeiter geschult, solche zu erkennen? Wurden Social-Engineering-Penetrationstests durchgeführt?

Systemsicherheit:

1. Hat die Stadt Zugriff auf Quellcodes der verwendeten Betriebssysteme?
2. Hat die Stadt Zugriff auf den Quellcode der verwendeten Netzwerkkomponenten?
3. Wie stellt die Stadt sicher, dass sich in den Binaries der Systeme kein Backdoor befindet?
4. Wie lange dauert es im Durchschnitt, bis vom Hersteller freigegebene Updates auf allen Systemen der Stadt Gießen eingespielt werden?
5. Gibt es einen Krisenplan, dessen Durchführung geübt wird für den Fall, dass durch höhere Gewalt o. ä. eine größere Datenmenge verloren geht? Wo werden die

ausgelagerten Datensicherungen gelagert? Wie lange würde es im Krisenfall dauern, bis die IT-Systeme der Stadt wieder einsatzbereit wären?

6. Gibt es Richtlinien im Zusammenhang mit der Abfallentsorgung, so dass ausgeschlossen werden kann, dass Papierabfälle in internen Papierkörben oder Sammelboxen oder in externen Containern Auskunft über vertrauliche Informationen geben? Gibt es Medienmanagement-Richtlinien zur Entsorgung elektronischer Medien?
7. Wie werden ausgemusterte oder nicht mehr benötigte EDV-Komponenten von ihren Daten befreit?“