Universitätsstadt Gießen

Die Oberbürgermeisterin

Universitätsstadt Gießen • Dezernat I • Postfach 110820 • 35353 Gießen

PIRATEN-Fraktion
Herrn Oechler

über
Büro der Stadtverordnetenversammlung

Berliner Platz 1
35390 Gießen

Auskunft erteilt: Dietlind Grabe-Bolz
Zimmer-Nr.: 02-009
Telefon: 0641 306-1001
Telefax: 0641 306-2001
E-Mail: dietlind.grabe-bolz@giessen.de

Datum: 16. August 2013

Anfrage gem. § 28 GO des Stv. Oechler vom 09.07.2013 – IT-Sicherheit; Drucksache-Nr. ANF/1633/2013

Sehr geehrter Herr Oechler,

zu dem Fragenkatalog nehme ich wie folgt Stellung:

Sicherer Aufruf der Website:

Frage 1:
Warum bietet die Universitätsstadt Gießen keine Möglichkeit an, die Website www.giessen.de über gesicherte Verbindung (https://) zu besuchen?

Antwort:
Der Magistrat sieht derzeit in der Regel keinen Bedarf, die Informationen auf www.giessen.de über eine gesicherte Verbindung abzurufen. Ausnahme bilden hier jedoch die aufgeführten Subdomänen, bei denen eine benutzerbezogene Anmeldung mit entsprechendem Schutzbedarf vorhanden ist:

- www.mandatsinfo.giessen.de
- www.stadtbibliothek.giessen.de
- www.vhs.giessen.de

Gemäß den Anforderungen der Fachämter bzw. den Empfehlungen der Fachverfahrenshersteller wurden hierfür SSL-Zertifikate beschafft und auf den jeweiligen Webservern installiert.

Frage 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?

Antwort:
Sämtliche Bereiche, die benutzerbezogene Daten abfragen, sind bereits geschützt. Weitergehende Planungen existieren nicht.

Frage 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?

Antwort:
Dies wäre von den entsprechenden Anforderungen abhängig.

Frage 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?

Antwort:
Es werden alle sicherheitsrelevanten Aspekte berücksichtigt.

Frage 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?

Antwort:
Es werden im Rahmen der Analyse der Webseitennutzung www.giessen.de die von den Seitenbesuchern verwendeten Webbrowser und die verweisende Herkunft, der so genannte Referrer, in einer Protokolldatei erfasst (Format "%v %b 127.0.0.1 %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\"" ispcplog). Darüber hinaus gibt es laut Verfahrensverzeichnis keine weiteren personenbezogenen Daten. Diese Protokolldatei kann von der Systemadministration ausgewertet werden. Nach sieben Tagen erfolgt die automatische Löschung. Eine weitergehende Speicherung anderer Nutzerdaten findet nicht statt.

Zu den Nutzerdaten bei den fachverfahrensbezogenen Subdomänen:
Server für www.mandatsinfo.giessen.de:
Nutzerkennung und Passwort werden über https übertragen und zusätzlich ist das Passwort nach dem Algorithmus MD5 (128 bit) verschlüsselt gespeichert.
Die mit Zustimmung der Mandatsträger veröffentlichten Daten (z. B. Name und Adresse, Telefonnummer und E-Mail-Adresse) sind in der Datenbank nicht verschlüsselt gespeichert.
Server für www.stadtbibliothek.giessen.de:
Nach Auskunft des Herstellers des Fachverfahrens der Stadtbibliothek findet keine Speicherung von Benutzerdaten und -transaktionen statt.
Server für www.vhs.giessen.de:
Eine diesbezügliche Anfrage an den Lieferanten ist bis heute noch nicht beantwortet worden.

E-Mail-Verkehr:

Frage 1:
Ist die Universitätsstadt Gießen in der Lage, verschlüsselte E-Mails zu empfangen, zu bearbeiten und auch verschlüsselt zu senden?

Antwort:
Grundsätzlich ist dies technisch möglich. Trotzdem müsste hierfür die notwendige technische Infrastruktur erst geschaffen werden, was zusätzliche Ressourcen binden würde.

Frage 2:
Falls nein, ist es geplant, dies einzuführen? Wenn ja, wann ist die Einführung geplant? Wenn nein, warum nicht?

Antwort:
Bisher liegen keine entsprechenden Anforderungen vor.

Arbeitsplätze der Bediensteten:

Frage 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?

Antwort:
Die Datensicherung ist amtsintern geregelt. Hinsichtlich der Definition von Nutzerrechten wird derzeit eine Dienstanweisung/Dienstvereinbarung erarbeitet.

Frage 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?

Antwort:
Für die IT-Arbeitsplätze gilt, dass keinerlei externe Geräte ohne Zustimmung des Fachamtes angeschlossen werden dürfen. Für besonders schützenswerte PC-Arbeitsplätze - wie z. B. die öffentlichen Internetarbeitsplätze - ist der Anschluss von externen Geräten unterbunden.

Frage 3:
Können Bedienstete eigene Software installieren?

Antwort:
Es kann keine Software durch Bedienstete installiert werden, die Administratorenrechte voraussetzt.

Frage 4:
Sind die Computer mit zeitgemäßem Viren- und Spamschutz ausgestattet? Wenn nein, warum nicht?

Antwort:
Alle an das städtische Netzwerk angeschlossenen Endgeräte werden mit einem aktuellen Viren- und Spamschutz ausgestattet. Die Aktualität und Verteilung auf allen Arbeitsplatzrechnern wird täglich kontrolliert. Zusätzlich werden alle ein- und ausgehenden E-Mails bei unserem Provider auf Viren und Spams untersucht.

Frage 5:
Werden die Festplatten der städtischen Arbeitsplatzrechner verschlüsselt? Wenn nein, warum nicht?

Antwort:
Die vorgehaltenen lokalen Datenträger aller mobilen Endgeräte wie z. B. Notebooks, Tablets, Smartphones, USB-Sticks werden grundsätzlich verschlüsselt. Für die stationären PC´s wird auf eine Verschlüsselung verzichtet, da auf den lokalen Datenträgern keine Daten gespeichert werden dürfen.

Penetration des Gesamtsystems:

Frage 1:
Gab es bereits bemerkte, erfolgreiche Angriffe durch Hacker auf Computersysteme der Stadtverwaltung? Wenn ja, welche Auswirkungen hatten diese?

Antwort:
Nein.

Frage 2:
Werden die Netzwerke der Stadt Gießen Penetrationstests unterzogen?

Antwort:
Nein.

Frage 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?

Antwort:
Nein.

Systemsicherheit:

Frage 1:
Hat die Stadt Zugriff auf Quellcodes der verwendeten Betriebssysteme?

Antwort:
Ja, teilweise. Es besteht die Möglichkeit auf die Quellcodes von einigen im Einsatz befindlichen Linux-Derivaten zuzugreifen.

Frage 2:
Hat die Stadt Zugriff auf den Quellcode der verwendeten Netzwerkkomponenten?

Antwort:
Nein.

Frage 3:
Wie stellt die Stadt sicher, dass sich in den Binaries der Systeme kein Backdoor befindet?

Antwort:
Wir setzen ein professionelles Antivirus Programm auf allen Systemen ein
und verlassen uns auf das Firewallkonzept unseres ISO-27001 zertifizierten Providers (ekom21).

Frage 4:
Wie lange dauert es im Durchschnitt, bis vom Hersteller freigegebene Updates auf allen Systemen der Stadt Gießen eingespielt werden?

Antwort:
Dies ist nicht pauschal zu beantworten.

Frage 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?

Antwort:
Die ausgelagerten Datensicherungen werden in einem weiteren Spezial-Datensafe in einem zweiten Data-Center gelagert, das sich in einem separaten Brandabschnitt befindet. Je nach Krisenlage (Sabotage, Erdbeben, etc.) könnte es einige Tage dauern, bis alle IT-Systeme wieder zur Verfügung stehen.
Die hierfür notwendigen Aktivitäten sind bekannt und können somit umgesetzt werden.
Aussagen zu den Recovery-Zeiten unseres Providers können nicht getroffen werden. Für die zu verantwortenden Telekommunikations-Systeme liegt die Downtime zwischen einem und drei Arbeitstagen.
Netzausfälle des Providers können nicht geschätzt werden.
Ausfälle von zentralen Netzwerkgeräten bei der Stadt Gießen können in der Regel in zwei Arbeitstagen behoben werden.

Frage 6:

a) Gibt es Richtlinien im Zusammenhang mit der Abfallentsorgung, sodass ausgeschlossen werden kann, dass Papierabfälle in internen Papierkörben oder Sammelboxen oder in externen Containern Auskunft über vertrauliche Informationen geben?
b) Gibt es Medienmanagement-Richtlinien zur Entsorgung elektronischer Medien?

Antwort:
a) Kleine Datenmüllmengen werden mit den im Hause existierenden Schreddern zerkleinert und mit dem normalen Papiermüll entsorgt. Größere Datenmüllmengen sammeln die Ämter in entsprechenden Behältnissen, welche in den aus Datenschutzgründen verschlossenen Aktenräumen gesammelt werden. In Abständen werden die größeren Datenmüllmengen zu einem externen Unternehmen gebracht, welches diese sicher vernichtet.

In den Büros werden lediglich die Papiermülleimer vom Reinigungspersonal geleert. Bei Beachtung der Verfahrensweise zur Entsorgung von Datenmüll, kann sich in diesen Papiermülleimern kein Datenmüll befinden.

b) Ja, die Anwender sind angewiesen, jegliche Medien über das Fachamt zu entsorgen.

Frage 7:
Wie werden ausgemusterte oder nicht mehr benötigte EDV-Komponenten von ihren Daten befreit?

Antwort:
Daten von Datenträgern werden über zertifizierte Unternehmen vernichtet, die die elektronischen Datenträger unter Einsatz eines speziellen Schneidgranulators in Sicherheitsstufe 3 vernichten. Dadurch sind Rückinformationen ausgeschlossen.

Mit freundlichen Grüßen

D. Grabe-Bolz

Dietlind Grabe-Bolz
Oberbürgermeisterin