



Anfragenbeantwortung

01. ordentliche öffentliche/nicht öffentliche Sitzung des Hauptausschusses am 13.08.2019

8.1. Sicheres WLAN

Herr F. Thier führt aus, dass bei der Einwahl in das Rathaus-WLAN eine Mitteilung erscheint, dass es sich offenbar um ein ungesichertes/offen auslesbares Netz handelt. Damit wären alle über dieses Netz gesandten und empfangenen Daten von außen einsehbar. Gerade mit Blick auf die persönlichen Zugangsdaten und die abgerufenen nicht öffentlichen Vorlagen sieht er dies hoch problematisch.

Zum Thema wird es eine schriftliche Antwort geben, so **Frau Herzog-von der Heide**.

Antwort der Verwaltung – Abt. IT-Management und -Service:

Im Rathaus erfolgt derzeit die Umstellung von einer einfachen Lösung mit einem einzelnen WLAN-Access-Point (AP) im Sitzungssaal hin zu einer mit speziellem WLAN-Controller gemanagten und erweiterbaren Lösung mit mehreren verteilten AP's.

Aktuell gibt es 3 AP's im Bereich des Sitzungssaales, dem Bürgermeisterbüro und dem Wirtschaftsförderungsamt. Darüber können mehrere verschiedenen berechnigte WLAN-Netze (SSID's) aufgespannt und der aktuelle WLAN-Standard 802.11ac genutzt werden.

Seit Ende 2018 wird die SSID: „Rathaus-Gast“ mit einem 6-stelligen Berechnigungsschlüssel genutzt, welcher für mehrere Nutzer mit tageszeitlicher Begrenzung eigentlich für Gäste im Rathaus und bei Sitzungen angewendet werden soll. Der Verbindungsaufbau vom mobilen Endgerät des Benutzers zum AP erfolgt hier unverschlüsselt. Das WLAN-Management sorgt durch die sogenannte AP-Isolation dafür, dass die mobilen Geräte keine Verbindung untereinander sondern nur zum Internet herstellen können. Die AP's der Telekom funktionieren ähnlich.

Der Verbindungsaufbau zum Ratsinformationssystem über einen https-Aufruf erfolgt in jedem Fall über eine sichere Ende-zu-Ende Verschlüsselung. Mit diesen Hintergrundinformationen kann also der Verbindung, trotz der berechtigten Warnung durch das mobile Endgerät, zugestimmt werden.

Für die Stadtverordneten wird die Nutzung der ebenfalls von den AP's ausgestrahlten SSID: „Rathaus“ vorbereitet. Hier wird nach Abfrage eines wpa2-Schlüssels (wie aus den Heim-WLANs bekannt) auf einer Vorschaltseite zur Eingabe von Benutzerdaten aufgefordert. Diese werden nur einmal abgefragt und auf dem speziellen mobilen Gerät mit dem Gerätezugangspasswort bzw. Fingerabdruck- oder Gesten-Sicherheitsmechanismus gekoppelt und gelten für die Legislaturperiode.

Trotz der Lockerung der gesetzlichen Regelungen zur Betreiberhaftung sind organisatorische Regelungen zur Identifizierbarkeit des jeweiligen Nutzerkreises umzusetzen. Daher sind die Erfassung der Namen und Geräteadressen (MAC) mit einer unterschriebenen Nutzererklärung notwendig.

i. A. Thomas Bergmann
Abteilungsleiter