dsb
datenschutzbeauftragter
kanton zürich

Merkblatt

WLAN-Angebot durch öffentliche Organe

1 Einleitung

Ein WLAN (Wireless Area Network / drahtloses Netzwerk) ermöglicht den drahtlosen Zugang zu einem Netzwerk, zum Beispiel zum Internet. Ein öffentliches Organ kann ein WLAN in seinen Räumlichkeiten einrichten und öffentlich zur Verfügung stellen.

Dieses Merkblatt nennt Massnahmen, die dabei zu berücksichtigen sind.

2 Massnahmen

Stellt das öffentliche Organ den WLAN-Zugang öffentlich zur Verfügung, muss es Massnahmen treffen zum Schutz seiner eigenen Daten. Das öffentliche Organ kann zusätzliche Massnahmen treffen, um Missbrauch vorzubeugen. Die Verantwortung für die Benutzung des WLANs tragen die Benutzerinnen und Benutzer selbst.

2.1 Trennung der Netze

Um die Sicherheit für die Informationen des öffentlichen Organs zu gewährleisten, muss das öffentliche Organ das interne Netzwerk vom öffentlich zugänglichen WLAN trennen (§ 7 Gesetz über die Information und den Datenschutz, IDG, LS 170.4). Die Mitarbeitenden der öffentlichen Organe müssen für ihre Aufgabenerfüllung das sichere interne Netzwerk nutzen.

2.2 Massnahmen gegen Missbrauch

Zur Verhinderung von Missbrauch kann das öffentliche Organ folgende Massnahmen umsetzen:

- Sperrung von Seiten mit illegalem Inhalt (Pornografie, Rassismus usw.)
- Identifizierung und Authentifizierung der Benutzerinnen und Benutzer (zum Beispiel Registrierung mittels Handynummer oder Benutzername und Passwort)
- Sichere Verschlüsselung (WPA2) zum Access Point oder Hinweis auf unverschlüsselte Verbindung mit Empfehlung der Verwendung einer Sicherheitssoftware (VPN)
- Ausschliessliche Aktivierung des WLAN während der Öffnungszeiten
- Isolierung der WLAN-Geräte voneinander
- Schutz der WLAN-Geräte durch Änderung und Unterdrückung der Netzwerkkennung

2.3 Nutzungsbestimmungen

Im Sinne der Transparenz kann das öffentliche Organ die Nutzungsbestimmungen veröffentlichen. Diese können zum Beispiel auf der Anmeldeseite für das WLAN angezeigt werden. Die Nutzungsbestimmungen können beinhalten:

- Hinweis, dass die Verantwortung beim Nutzenden des WLAN liegt und nicht beim öffentlichen Organ
- Hinweis auf die Risiken der Nutzung, insbesondere der Möglichkeit der Einsicht in Daten des Nutzenden durch Dritte
- Hinweis auf die Haftung des Nutzenden bei rechtswidrigen Handlungen
- Verbot zur Änderung der Konfigurationseinstellungen durch die Nutzenden

3 Geltungsbereich BÜPF

Das zur Verfügung stellen eines öffentlichen WLAN-Zugangs fällt unter Umständen in den Geltungsbereich des Bundesgesetzes betreffend die Überwachung des Post- und Fernmeldeverkehrs (Art. 2 lit. e BÜPF, SR 780.1). Daraus können sich Mitwirkungspflichten ergeben (Art. 29 BÜPF). Bei professionell betriebenen WLAN-Zugängen besteht eine Identifikationspflicht der Endbenutzerinnen und -benutzer mittels geeigneten Mitteln sowie die Pflicht, diese Identifikationsdaten dem Dienst ÜPF zu liefern (Art. 21 Abs. 1 lit. d BÜPF i.V.m. Art. 19 Abs. 2 Verordnung über die Überwachung des Post- und Fernmeldeverkehrs, VÜPF, SR 780.11). Erläuterungen hierzu enthält das Merkblatt WLAN des Dienstes ÜPF.

Bietet ein öffentliches Organ einen WLAN-Zugang in seinen Räumlichkeiten an, ist das BÜPF nicht anwendbar und das öffentliche Organ hat weder Mitwirkungspflichten noch muss es die Endbenutzenden identifizieren. Beispiele dafür sind das WLAN eines Spitals für Patientinnen und Patienten oder dasjenige einer Gemeinde im Gemeindehaus.

dsb

datenschutzbeauftragter
kanton zürich

Datenschutzbeauftragter
des Kantons Zürich
Postfach, 8090 Zürich

Telefon 043 259 39 99
datenschutz@dsb.zh.ch

www.datenschutz.ch
twitter.com/dsb_zh