HANDY IM (AN-)GRIFF

CYBERSICHERHEITSSTUDIE WLAN-RISIKEN 2018

Ob zum Checken von Chat-Nachrichten, Posten von Fotos oder für eine schnelle Arbeitsstunde im Kaffeehaus – WLAN-Hotspots werden von Smartphone-, Tablet- und Notebooknutzern gerne genutzt – jedoch aber ohne über die eigene Sicherheit nachzudenken. Eine Studie des KFV (Kuratorium für Verkehrssicherheit) zeigt nun gravierende Sicherheitslücken und unterschätzte Risiken bei der WLAN-Nutzung auf.

LEICHTES SPIEL

Potenziell haben Hacker in einer Großstadt wie Wien die Möglichkeit pro Minute mehr als 50 internetfähige Geräte durch unsichere WLAN-Verbindungen zu kapern – das zeigt eine Untersuchung des KFV. Je nach Sicherung und Verschlüsselung der angebotenen Netzwerke können Hacker so leicht personenbezogene Daten, Bankverbindungen und Passwörter ablesen.

BEQUEMLICHKEIT VOR SICHERHEIT?

Im Rahmen der Studie wurden an elf hochfrequentierten (Infrastruktur-)Knotenpunkten in Wien Sicherheitseinstellungen von WLAN-Netzwerken und die Netzwerknutzung der Endgeräte anonym erfasst, um die Risiken, die durch die Nutzung dieser Netzwerke im öffentlichen Raum entstehen, zu analysieren. Insgesamt wurden dabei rund 16.300 WLAN-Zugangspunkte und rund 66.000 Endgeräte untersucht.

PRO STUNDE KONTAKT MIT BIS ZU 350 UNSICHEREN WLAN-VERBINDUNGEN MÖGLICH

Die Ergebnisse zeigen deutlich, dass vielen Nutzern die Risiken oft nicht bewusst sind: Pro Stunde kann man in Wien mit rund 700 möglichen Internetzugangspunkten in Kontakt kommen. Rund die Hälfte aller dieser WLAN-Netzwerke sind nicht optimal gesichert. Darüber hinaus suchen sich rund zehn Prozent der untersuchten Geräte durch den Automatik-Modus ohne Aktion des Besitzers diverse Netzwerke und waren somit höchst empfangsbereit für Hacker. 255 User haben sich im Rahmen der Erhebung in ein frei erfundenes „Fantasie-WLAN“ eingewählt. Die im Rahmen der Studie aufgesetzten WLAN-Netzwerke waren harmlos, in einer Alltagssituation wäre ein leichtfertiges Einloggen aber fahrlässig. Denn auf diese Weise hätte ein Hacker Zugriff auf alle Informationen, die über das Internet übermittelt werden: vertrauliche E-Mails, Kreditkartendaten oder Zugangsdaten. Besitzt er diese Informationen erst einmal, kann der Hacker nach Belieben auf die persönlichen Systeme zugreifen.

HANDY GEHACKT? WER TRÄGT DEN SCHADEN?

Grundsätzlich ist der Schädiger (z.B. ein Hacker) stets dann verantwortlich, wenn er durch ein rechtswidriges und schuldhaftes Verhalten einen Schaden verursacht hat. Ist der Täter nicht auffindbar, hat – neben weiteren potentiellen Haftungsträgern wie z.B. Banken im Rahmen der für sie geltenden gesetzlichen Vorschriften – der Nutzer seinen Schaden soweit selbst zu tragen. Darüber hinaus bieten Versicherungen und Mobilfunk-Anbieter ihren Kunden die Möglichkeit einer Versicherung gegen Cyberkriminalität. Für WLAN-Betreiber gilt: Wer sein WLAN mit allen zum Stand der Technik gehörenden Maßnahmen gegen den Missbrauch durch Dritte absichert, ist auf der sicheren Seite.

METHODIK

Im Auftrag des KFV wurden an elf (Infrastruktur-) Knotenpunkten in Wien Messungen durchgeführt. Insgesamt wurden rund 16.300 WLAN-Zugangspunkte und rund 66.000 Endgeräte analysiert.

Studienzeitraum: Mai – Juni 2018

HANDY IM (AN-)GRIFF: WLAN Sicherheitslücken in Wien

KFV

Analyse

16.300
WLAN-Zugangspunkte

rund
66.000 Endgeräte

11 (Infrastruktur-) Knotenpunkte

Ergebnisse

700
Internetzugangspunkte
pro Stunde in Wien.

50% dieser **WLAN-Netzwerke** sind nicht optimal gesichert.

Potentielle **Kapermöglichkeit** durch **unsichere WLAN-Nutzung:**

pro Minute bei rund **50**
internetfähigen Geräten
möglich!

10% der **WLAN-Nutzer** loggen sich in **unsichere WLAN-Netzwerke** ein.

255 User
tappten in eine
„Fantasie-WLAN"
Falle

TIPP

Gut zu wissen: WLAN-Buchstabengruppen

OPN	nicht verschlüsselt und unsicher
WEP	verschlüsselt aber unsicher (veraltet)
WPA	verschlüsselt und unsicher (neuer als WEP aber ebenso veraltet)
WPA2 WPA	Mischmethode zwischen alt und neu
WPA2	aktuellster und sicherster Standard

SCHWACHSTELLE TECHNIK

- Fehlende Verschlüsselung
- Veraltete oder fehlerhafte Sicherheitsstandards
- Unsichere Konfiguration
- Schlechtes Softwaredesign (Apps und Operationssystem)

SCHWACHSTELLE MENSCH

- Unreflektierte Nutzung fremder WLAN-Angebote
- Schlechtes Passwortmanagement
- Bequemlichkeiten vor Sicherheit
- Starke Beeinflussbarkeit (z.B. durch Hacker)

RISIKEN

- **Auslesung personenbezogener Daten**, Bankverbindungen und Passwörter.
- **Identitätsdiebstahl** z.B. für Online-Einkäufe im Namen des Users.
- **Phishing** (z.B. Daten über Bankverbindungen) und **Adware** (bösartige Werbungssoftware, z.B. Abofallen).

METHODEN

- Nutzung von **Rogue Access Points** bzw. **Evil Twins** (gefälschte WLAN-Zugangspunkte).
- **Deauthentication-Attacken** (Unterbrechung der bestehenden Verbindung eines Endgeräts mit WLAN-Zugangspunkt, um es mit einem gefälschten WLAN zu verbinden).
- **Angriff auf den Standard** (Ausnutzung der im Handy gespeicherten WLAN-Netzwerke, die das Handy automatisch sucht, wenn nicht in Reichweite).

RECHT

Handy gehackt – wer trägt den Schaden?

- Der **Schädiger** (z.B. ein Hacker) ist stets dann verantwortlich, wenn er durch ein **rechtswidriges und schuldhaftes Verhalten** einen **Schaden verursacht** hat.
- Ist der **Täter nicht auffindbar**, hat der **Nutzer** seinen **Schaden selbst zu tragen** (neben potentiellen Haftungsträgern wie z.B. Banken im Rahmen des Zahlungsdienstgesetzes).

Quelle: KFV (Kuratorium für Verkehrssicherheit)

APA-AUFTRAGSGRAFIK

PRÄVENTIONSTIPPS

> Loggen Sie sich nur in Netzwerke ein, **die Ihnen bekannt sind** und die sich physisch in unmittelbarer Nähe bzw. Reichweite befinden.

> Achten Sie auf **Sicherheitsstandards** und Verschlüsselungsmethoden der angebotenen Netzwerke und nutzen Sie offene WLAN-Verbindungen vorsichtig!

> Die Aktivierung des WLAN sollte **nur bei Bedarf** erfolgen.

> Misten Sie die lokale WLAN-Liste regelmäßig aus, um **automatische Verbindungen zu reduzieren.**

> Führen Sie **regelmäßige Updates** durch und installieren Sie Anti-Viren-Software.

WLAN **NUR BEI BEDARF** AKTIVIEREN

Mit ein paar Handgriffen und Einstellungen können sich mobile Internetnutzer im Wesentlichen gegen ungewollten Zugriff auf ihre Daten absichern. Grundsätzlich gilt: Updates machen. Das Betriebssystem des Mobilgeräts sowie alle Apps sollten auf dem aktuellsten Stand, bei Notebooks eine etwaige Firewall aktiviert sein. Zudem sollte die WLAN-Verbindung nur bei Bedarf aufgerufen werden und nicht dauerhaft aktiviert sein.

Das Löschen bzw. „Ausmisten“ der lokalen WLAN-Liste hilft, das unbemerkte Einwählen in Netzwerke zu reduzieren. Hat sich das Smartphone einmal in ein mit Passwort gesichertes WLAN-Netz eingebucht, merkt sich das Handy die Zugangsdaten und meldet sich an dem bereits bekannten Hotspot automatisch an, sobald der Nutzer erneut in Reichweite ist. Die Aktivierung des WLAN sollte nur bei Bedarf erfolgen.

Quelle: KFV-Cybersicherheitsstudie
WLAN-Risiken 2018
Bildrechte: KFV/APA, iStock

Medieninhaber und Herausgeber:
KFV (Kuratorium für Verkehrssicherheit)
Schleiergasse 18, A-1100 Wien
Tel.: +43 5 77077-0
E-Mail: kfv@kfv.at