Presseinformation

KFV-Cybersicherheitsstudie

Unterschätztes Risiko WLAN: KFV Untersuchung zeigt Nutzer sind sich Risiken oft nicht bewusst.

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 aktuelle Untersuchung des KFV. Vor allem Smartphone-Nutzer machen es Kriminellen besonders leicht, dabei sind die Sicherheitsrisiken nicht zu unterschätzen. Mit ein paar einfachen Sicherheitsvorkehrungen kann man sich gut schützen.

Wien, 07. August 2018. Ob zum Checken der Whats-App Nachrichten oder E-Mails, 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. Dabei ist vor allem bei der beliebten WLAN-Nutzung besondere Vorsicht geboten. „Je nach Sicherung und Verschlüsselung der angebotenen Netzwerke können Hacker personenbezogene Daten, Bankverbindungen und Passwörter ablesen. Solche Daten können für Online-Einkäufe oder Bankgeschäfte missbraucht werden“, erläutert **Dr. Armin Kaltenegger, Leiter des Bereichs Eigentumsschutz im KFV.**

Erhebung zeigt: Schneller Einstieg statt Sicherheit

Im Rahmen einer Studie, die im Zeitraum von Mai bis Juni 2018 an elf hochfrequentierten (Infrastruktur-)Knotenpunkten in Wien durchgeführt wurde, hat das KFV Sicherheitseinstellungen von WLAN-Netzwerken und die Netzwerknutzung der Endgeräte anonym erfasst, um zu analysieren, welche Risiken durch die Nutzung dieser Netzwerke im öffentlichen Raum entstehen. 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 sowohl den WLAN-Betreibern als auch den Nutzern selbst 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!“, so **Kaltenegger**. „Unsere Analysen vor Ort haben darüber hinaus gezeigt, dass potentielle Hacker in Wien durch unsichere WLAN Verbindungen die Möglichkeit haben, rund 50 internetfähige Geräte pro Minute zu kapern.“ 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: „Unser im Rahmen dieser Studie aufgesetztes WLAN war völlig harmlos. In einer Alltagssituation wäre ein leichtfertiges Einloggen in beliebige WLAN-Netzwerke aber sehr fahrlässig“, erklärt **Kaltenegger.**

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 sollte 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.

KFV-Tipps zum Schutz gegen WLAN Übergriffe

- 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.

Rückfragehinweis:
Pressestelle KFV (Kuratorium für Verkehrssicherheit)
Tel.: 05-77077-1919 I E-Mail: pr@kfv.at I www.kfv.at