Thema: **Öffentliche WLAN-Hotspots – So gefährlich sind sie wirklich!**

Beitrag: 1:49 Minuten

Anmoderationsvorschlag: Bahnhöfe, Flughäfen, Hotels, Geschäfte, öffentliche Einrichtungen oder in unseren Innenstädten: WLAN-Hotspots schießen zurzeit wie Pilze aus dem Boden. Wer öfter unterwegs ist und mal eben schnell mit seinem Mobilgerät kostenlos ins Internet gehen will, weiß das natürlich zu schätzen. Problem dabei: Viele Betreiber dieser Hotspots bieten nur unverschlüsselte Verbindungen an und das ist ganz schön gefährlich. Warum, erklärt Ihnen zum Europäischen Datenschutztag am 28. Januar (Alternative: zum Safer Internet Day am 09. Februar) Helke Michael.

Sprecherin: Ungesicherte öffentliche WLAN-Netzwerke sind ein Paradies für Online-Kriminelle, weil sie dort supereinfach die unverschlüsselten Daten abgreifen können.

O-Ton 1 (Tim Berghoff, 0:28 Min.): „Sie können zum Beispiel Zugangsdaten mitlesen für Online-Shops, für Bankkonten oder eben die Zugangsdaten von sozialen Netzwerken, und diese Daten dann eben in Geld verwandeln. Es gab auch schon Fälle, in denen Kriminelle einfach in der Innenstadt beispielsweise sich einen Hotspot eingerichtet haben, um einen Surfer in die Falle zu locken. Alles, was der Kriminelle dann tun muss, ist darauf warten, dass jemand sich auf seinem Hotspot einloggt und diesen dann eben nutzt."

Sprecherin: Erklärt der G DATA Sicherheitsexperte Tim Berghoff und rät:

O-Ton 2 (Tim Berghoff, 0:24 Min.): „Öffentliche Hotspots sollte man generell nur dann nutzen, wenn man auf dem Smartphone, auf dem Tablet, auf dem Notebook eine aktuelle Sicherheitslösung installiert hat. Und alle Apps, die auf diesem Gerät installiert sind, wie zum Beispiel der Internetbrowser, sollten immer auf dem neuesten Stand sein. Nicht benötigte Funkverbindungen, wie jetzt zum Beispiel WLAN oder Bluetooth, sollte man grundsätzlich abschalten, wenn man sie gerade nicht braucht."

Sprecherin: Ein Restrisiko bleibt aber trotzdem, denn öffentliches WLAN ist nie so sicher wie das eigene, gut geschützte zu Hause. Aber auch unterwegs kann man heutzutage eine sichere Verbindung aufbauen – und zwar mithilfe eines sogenannten „Virtual Private Networks".

O-Ton 3 (Tim Berghoff, 0:26 Min.): „Eine VPN-Verbindung, man spricht hier auch von einem VPN-Tunnel, sorgt dafür, dass alle Daten, die zwischen dem Laptop, dem Smartphone oder dem Tablet und dem Internet übertragen werden, verschlüsselt sind. Dafür braucht man eine spezielle VPN-Software. Die ist beispielsweise in der G DATA INTERNET SECURITY PRIVACY EDITION bereits enthalten. Damit ist man gleichzeitig vor aktuellen Online-Bedrohungen geschützt und kann sich in öffentlichen WLAN-Netzwerken sicher bewegen."

Abmoderationsvorschlag: Wenn Sie das gerade Gehörte noch mal in Ruhe nachlesen wollen: Alle Infos sowie die passende Sicherheitssoftware finden Sie im Netz unter www.gdata.de.

Thema: **Öffentliche WLAN-Hotspots – So gefährlich sind sie wirklich!**

Interview: 2:13 Minuten

Anmoderationsvorschlag: Bahnhöfe, Flughäfen, Hotels, Geschäfte, öffentliche Einrichtungen oder in unseren Innenstädten: WLAN-Hotspots schießen zurzeit wie Pilze aus dem Boden. Wer öfter unterwegs ist und mal eben schnell mit seinem Mobilgerät kostenlos ins Internet gehen will, weiß das natürlich zu schätzen. Problem dabei: Viele Betreiber dieser Hotspots bieten nur unverschlüsselte Verbindungen an und das ist ganz schön gefährlich. Warum, erklärt Ihnen zum Europäischen Datenschutztag am 28. Januar (Alternative: zum Safer Internet Day am 09. Februar) der G DATA Sicherheitsexperte Tim Berghoff, hallo.

Begrüßung: „Hallo, ich grüße Sie“

1. ***Herr Berghoff, warum kann das Surfen in öffentlichen WLAN-Hotspots gefährlich werden?***

O-Ton 1 (Tim Berghoff, 0:36 Min.): „Weil öffentliche WLAN-Netzwerke in vielen Fällen eben keine ausreichende Sicherheit gewährleisten – und Online-Kriminelle können das eben ausnutzen. Sie können dann zum Beispiel Zugangsdaten mitlesen für Online-Shops, für Bankkonten oder eben die Zugangdaten von sozialen Netzwerken, und diese Daten dann eben in Geld verwandeln. Es gab auch schon Fälle, in denen Kriminelle einfach in der Innenstadt beispielsweise sich einen Hotspot eingerichtet haben, um einen Surfer in die Falle zu locken. Alles, was der Kriminelle dann tun muss, ist darauf warten, dass jemand sich auf seinem Hotspot einloggt und diesen dann eben nutzt.“

2. ***Und was machen die Diebe mit den gestohlenen Daten?***

O-Ton 2 (Tim Berghoff, 0:30 Min.): „Es gibt hier zwei Möglichkeiten. Die Diebe können entweder diese Daten direkt weiterverwenden und damit dann auf Einkaufstour gehen, eben auf Kosten anderer. Oder wenn sie die Zugangsdaten zu einem Bankkonto gestohlen haben, dann einfach direkt das Konto leeräumen. Die zweite Möglichkeit ist, dass diese Daten dann weiter verkauft werden, in speziellen Untergrundmärkten. Insgesamt geht man davon aus, dass hier mehr umgesetzt wird, als im internationalen Drogenhandel. Wir bewegen uns also hier im Bereich von mehreren Milliarden Euro, die hier bewegt werden.“

3. ***Wie kann man trotzdem möglichst sicher an öffentlichen WLAN-Hotspots surfen?***

O-Ton 3 (Tim Berghoff, 0:24 Min.): „Öffentliche Hotspots sollte man generell nur dann nutzen, wenn man auf dem Smartphone, auf dem Tablet, auf dem Notebook eine aktuelle Sicherheitslösung installiert hat. Und alle Apps, die auf diesem Gerät installiert sind, wie zum Beispiel der Internetbrowser, sollten immer auf dem neuesten Stand sein. Nicht benötigte Funkverbindungen, wie jetzt zum Beispiel WLAN oder Bluetooth, sollte man grundsätzlich abschalten, wenn man sie gerade nicht braucht.“

4. ***Ein Restrisiko bleibt aber trotzdem, denn öffentliches WLAN ist ja nie so sicher wie das eigene, gut geschützte zu Hause. Gibt’s denn vielleicht noch eine andere Alternative, um unterwegs eine sichere Verbindung aufzubauen?***

O-Ton 4 (Tim Berghoff, 0:31 Min.): „Die gibt es, und zwar sogenannte Virtual Private Networks, kurz VPN. Eine VPN-Verbindung, man spricht hier auch von einem VPN-Tunnel, sorgt dafür, dass alle Daten, die zwischen dem Laptop, dem Smartphone oder dem Tablet und dem Internet

übertragen werden, verschlüsselt sind. Dafür braucht man eine spezielle VPN-Software. Die ist beispielsweise in der G DATA INTERNET SECURITY PRIVACY EDITION bereits enthalten. Damit ist man gleichzeitig vor aktuellen Online-Bedrohungen geschützt und kann sich in öffentlichen WLAN-Netzwerken sicher bewegen."

G Data Sicherheitsexperte Tim Berghoff mit Tipps für alle, die gern ohne Bedenken sicher im Internet surfen. Besten Dank dafür!

Verabschiedung: „Danke, tschüss!"

Abmoderationsvorschlag: Wenn Sie das gerade Gehörte noch mal in Ruhe nachlesen wollen: Alle Infos sowie die passende Sicherheitssoftware finden Sie im Netz unter www.gdata.de.