Free WiFi! Aber nicht wenn es um die Security geht

Viele haben sich daran gewöhnt, kostenloses und freies WiFi überall dort zu nutzen, wo es angeboten wird – darunter Hotels, Bahnhöfe, Gaststätten oder Einkaufszentren. Dabei entstehen gleich drei Gefahrenpotenziale: Der unbekannte Nutzer könnte sich mit einem infizierten Gerät einloggen und das Netzwerk des Anbieters infizieren. Der Nutzer könnte sein eigenes Gerät infizieren, da der Anbieter des WiFi nicht genügend Wert auf Security legt. Und sowohl Nutzer als auch Anbieter sind gefährdet, wenn man zum Einloggen in das „freie" WiFi persönliche Daten angeben muss, die der WiFi-Anbieter sammelt und in einer nicht sicheren Umgebung speichert.
Diese drei Szenarien hat Sophos etwas genauer unter die Lupe genommen und gibt Free WiFi-Anbietern Tipps für mehr Sicherheit aller Beteiligten, indem das WiFi konsequent in die Security integriert wird.

Fall 1: Der Nutzer infiziert das Netz des Free WiFi-Anbieters
Die Forschungsergebnisse der SophosLabs belegen, dass mobile Endpoints, also Smartphones, Tablets oder Laptops besonders gefährlich sind, sobald der WiFi-Anbieter keine Kontrolle über deren Security-Zustand hat. Die jüngsten Angriffe der Malware Emotet beweist dies eindrücklich. Im Februar 2020 attackierte Emotet erstmals auch WLANs. Die Malware klinkt sich in schlecht gesicherte Funknetze ein und nutzt diverse Methoden, sich weiter zu verbreiten. Emotet infiziert weitere im Netzwerk befindliche Rechner, um an Dateifreigaben und Windows- beziehungsweise Active-Directory-Konten zu gelangen. Alle Informationen, darunter auch Passwörter, meldet der Schädling seinem Command and Control Server (C2), sprich dem Hacker.

Fall 2: Der Anbieter infiziert den Nutzer
In diesem Fall existieren zwei Szenarien. Ist das Netzwerk des Free WiFi-Anbieters einmal infiziert, wird sich die Malware ausbreiten. Dabei verschont diese selbstverständlich auch nicht die vielen Endgeräte, die sich ständig neu mit dem WiFi verbinden. So bekommt der arglose Nutzer einen Schädling verpasst, den er dann vielleicht sogar beim nächsten Free WiFi oder an seine Kollegen in anderen Netzwerken weitergibt.
Das zweite Szenario sind Rogue Access Points oder sogar Evil Twins, die sich als das Free WiFi des Anbieters ausgeben, jedoch Fake sind. Diese Fake WiFi werden absichtlich von Hackern an lohnenswerten Orten aktiviert. Auf diesem Weg erlangen sie direkten Zugriff auf viele Mobilgeräte und können bequem Daten und Informationen (darunter auch Passwörter) sammeln, oder Malware verbreiten.

Fall 3. Der WiFi-Anbieter und der Nutzer haben keine Sicherheit über persönliche Daten
Einige „Free" WiFi-Anbieter verlangen zwar kein Geld für die Nutzung des Internets, dafür aber persönliche Daten bevor man sich einloggen kann. Man kann sich streiten, ob dies überhaupt ein Free WiFi ist, denn persönliche Daten haben ja offensichtlich einen Wert, sonst würde sie der Anbieter nicht abfragen und sammeln. Und genau darin liegt die Krux. Selbst wenn man damit einverstanden ist, dass der Anbieter im Gegenzug für ein freies WiFi einige persönliche Daten speichern und nutzen darf, sind diese allzu oft nicht sicher gespeichert und aufgrund ihres Wertes oft Ziel von Cyberkriminellen. So geschehen in Großbritannien, als Jeremiah Fowler von Security Discovery Mitte Februar 2020 einen Free WiFi-Anbieter genauer unter die Lupe nahm, der Daten von seinen Nutzern sammelte. Das WiFi-Unternehmen hatte über 146.000.000 Datensätze in einer nicht sicheren Cloud-Umgebung gespeichert. Für den Nutzer wird es unangenehm, wenn seine Daten in fremde beziehungsweise falsche Hände geraten, für den Anbieter ist es eine eindeutige Verletzung von Vorschriften, die in Zeiten der DSGVO empfindliche Strafen nach sich ziehen können.

6 Tipps für Free WiFi-Anbieter, ob klein oder groß
Unternehmen, die eine freies WiFi anbieten gibt es in allen Kategorien, von großen Einrichtungen wie Bahnhöfen, über Hotelketten bis hin zum kleinen Cafe um die Ecke. Alle haben jedoch eines gemein: sie sollten sich selbst und den Nutzern ein genügendes Maß an Sicherheit bieten. Dafür gibt Sophos Free WiFi-Anbietern vier grundlegende Tipps.

- **Segmentierung:** Das Free WiFi sollte auf keinen Fall im selben Sub-Netz wie das interne LAN- oder WiFi-Netzwerk des WiFi-Anbieters sein. Damit kann ein direktes Durchgreifen von Malware auf andere Teile des Netzwerks und die darin befindlichen Endpoints unterbunden werden.
- **Client-Isolierung:** Im Free WiFi muss der Access Point die mit ihm verbundenen Clients voneinander isolieren. Dadurch wird verhindert, dass ein infizierter Rechner sich mit anderen Rechnern im WLAN verbinden und diese ebenfalls infizieren kann.
- **WiFi in Security integrieren:** Geeignete Schutzmechanismen, beispielsweise eine integrierte oder auch Synchronized Security von Firewall, Netzwerksicherheit und den dazugehörigen Access Points, die ebenfalls in die Gesamt-Security integriert sind, können die Sicherheit nicht nur für den WiFi-Anbieter, sondern auch für den Nutzer deutlich erhöhen.
- **Automatische Erkennung und Isolierung infizierter Geräte:** Eine integrierte und automatisierte Security schützt sowohl den Free WiFi-Anbieter als auch die Nutzer indem mit Malware infizierte Geräte vom Netz isoliert werden – automatisch und bevor andere Teilnehmer im Netz infiziert werden.
- **Intelligenter Malware-Schutz für sensible Daten:** Wenn schon Daten von WiFi-Nutzern gesammelt werden, dann müssen diese vor möglichen Cyber-Attacken geschützt werden. Dabei hat Next Generation Security mit Unterstützung von Künstlicher Intelligenz (KI) höchste Priorität.
- **Security für sensible Daten in der Cloud:** Die Cloud und insbesondere die Public Cloud sollte nur dann für sensible Daten genutzt werden, wenn der Anbieter einen gesetzeskonformen Schutz garantiert. Zudem sind oft Konfigurationsfehler bei der Einrichtung der Cloud ein Einfallstor für Cyberkriminelle. Diese können durch Tools wie Cloud Optix von Sophos mit Hilfe von KI auf ein Minimum reduziert werden.

Pressekontakt:

Sophos
Jörg Schindler, PR Manager CEEMEA
joerg.schindler@sophos.com, +49-721-25516-263

TC Communications
Arno Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617
Ulrike Masztalerz, +49-30-55248198
Ariane Wendt +49-172-4536839
sophos@tc-communications.de