Gefahren im WLAN und warum das auch für 5G von Bedeutung ist

Kabellose Sicherheit

Im Unternehmensumfeld wie im öffentlichen Bereich – beispielsweise im Hotel- und Gaststättengewerbe, in Ladengeschäften oder Verkehrsmitteln – sprießen WLAN-Strukturen seit Jahren wie Pilze aus dem Boden. Hohe Übertragungsgeschwindigkeiten und optimale Ausleuchtung sind dabei meist die vorrangigen Qualitätsmerkmale. Der Aspekt der Sicherheit wird nach wie vor eher stiefmütterlich behandelt, obwohl die Gefahr durchaus präsent ist. Nicht zuletzt aufgrund des zunehmenden Bandbreitenbedarfs im Mobilfunknetz sind allgemein verbindliche Sicherheitsstandards im WLAN künftig wichtiger denn je.

Auch wenn die Schlagzeilen rund um die Aufdeckung von Sicherheitslücken im Hinblick auf WLAN-Strukturen nicht abreißen, unterschätzen viele Unternehmen und Anbieter mit einem WLAN-Angebot nach wie vor die konkrete Gefahr. Denn Access Points sind nicht zuletzt ideale Einfallstore für den Zugriff auf die weitere Netzwerkinfrastruktur oder zum Abgriff von Nutzerdaten. Allein die Kombination aus WPA2-Verschlüsselung mit einer unsichtbar ausgestrahlten SSID bietet keinen ausreichenden Schutz. Beachtet werden müssen nicht nur aktive Angriffe von Cyberkriminellen, die Systeme unter anderem zum Datendiebstahl manipulieren, sondern ebenfalls das bewusste oder unbewusste Fehlverhalten der WLAN-Nutzer. Sechs Aspekte fallen im Zusammenhang mit verlässlichen und sicheren kabellosen Verbindungen besonders ins Gewicht: benachbarte Access Points, Rogue Access Points, Evil Twin Access Points mit gefälschten SSID sowie Rogue Clients, Adhoc-Netzwerke und falsch konfigurierte Access Points.

Gefahrenaspekte bei WLANs

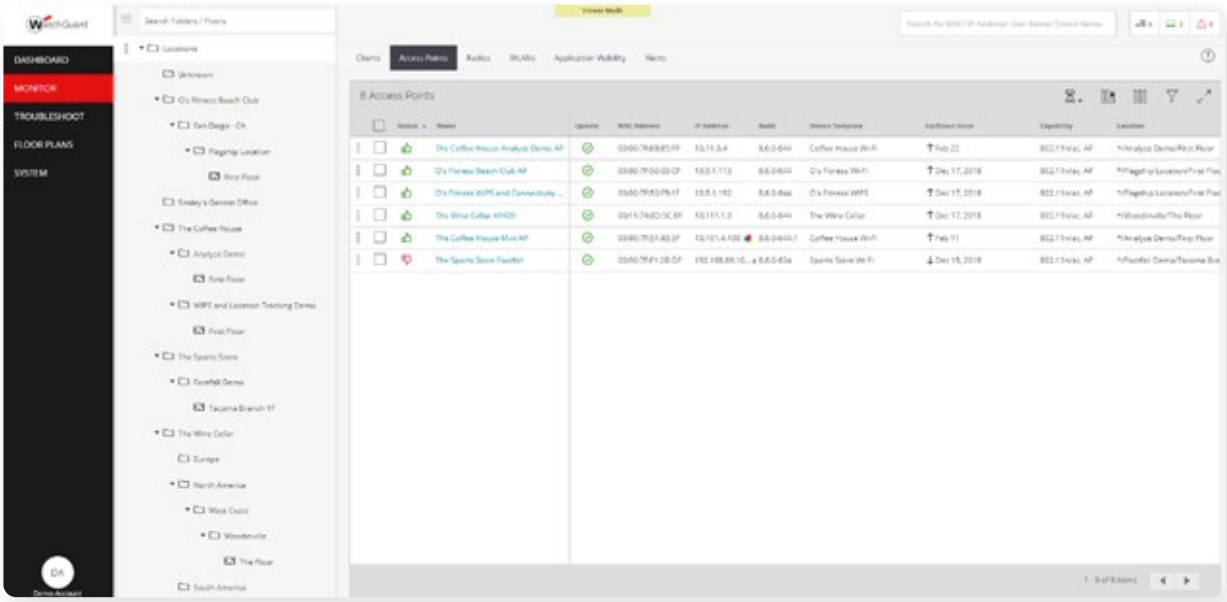
1. Benachbarte Access Points

In vielen Unternehmen ist es den Mitarbeitern untersagt, das Firmen-Internet für private Zwecke zu nutzen, etwa für soziale Medien wie Facebook oder Twitter. Über entsprechende Einstellungen (in diesem Fall Blacklists) in der Gateway-Firewall lässt sich der Verbindungsaufbau zu diesen und weiteren Seiten beispielsweise über URL-Content- und DNS-Filter zuverlässig unterbinden. Doch wer oder was hindert den Mitarbeiter daran, den Zugang über den Firmen-Laptop in Verbindung mit einem eigenen Smartphone-Hotspot oder den Gast-Hotspot eines Unternehmens in Reichweite des WLANs aufzubauen? Die Gefahr in diesem Szenario besteht darin, dass jeglicher Datenverkehr parallel zur eigenen Infrastruktur stattfindet und daher nicht kontrolliert werden kann. Falls sich ein Rechner auf diesem Weg mit Malware infiziert, ist dies für den Administrator zudem nicht mehr nachvollziehbar, da in den Logfiles keinerlei Hinweise zu finden sind.

2. Rogue Access Points

Bei Rogue Access Points handelt es sich um Hardware, die an der IT-Abteilung vorbei ins Unternehmen eingeschleust und an einen internen LAN-Port oder Switch angesteckt wird. Das kann das Werk von Cyberkriminellen sein, die sich Zugang ins Unternehmen verschafft haben, aber häufiger geschieht dies über eigene Mitarbeiter, die auf diese Weise eine vielleicht schlechte WLAN-Performance an ihrem Arbeitsplatz verbessern wollen. Das stellt insbesondere ein Problem für Unternehmen dar, die ihr

Foto: © StockLite/Shutterstock.com



Mit Visualisierungslösungen – wie WatchGuard Discover – können unter anderem Access Points in Reichweite und im WLAN genutzte Anwendungen gezielt im Blick behalten werden. (Quelle: WatchGuard)

WLAN gemäß dem Payment Card Industry Data Security Standard (PCI DSS) eingerichtet haben. Ein Rogue Access Point stellt einen direkten Verstoß dagegen dar. Wie im Fall zuvor hat der IT-Administrator auch hier keine Ahnung davon, was da überhaupt eingerichtet wurde und wie das Gerät aus sicherheitstechnischer Sicht konfiguriert ist. Häufig handelt es sich hierbei jedoch um keine gezielte, böswillige Attacke, sondern ein unbewusstes Fehlverhalten von Mitarbeitern, die eine Problematik im Netzwerkbereich in Eigenregie lösen wollen und sich über die Konsequenzen nicht klar sind. Zu Rogue Access Points zählen unter anderem WLAN-fähige Drucker und Faxgeräte ohne ausreichende Verschlüsselung, die über den LAN-Port ans interne Netzwerk angeschlossen sind.

3. Evil Twin Access Points

Im Falle eines Evil Twin Access Points wird seitens eines Cyberkriminellen der Versuch gestartet, Unternehmensgeräte, wie Laptops oder Smart Devices, dazu zu bringen, sich mit einem gefälschten Access Point zu verbinden. Das setzt allerdings voraus, dass der Angreifer sich wirklich in Reichweite des Unternehmens-WLANs befindet. Das Gerät des Angreifers sendet dazu die gleichen SSID- und MAC-Adressen aus, wie der reguläre Access Point. Diese Kennungen lassen sich übrigens selbst bei einer „unsichtbaren" Ausstrahlung problemlos mit frei im Internet verfügbaren Tools finden und auslesen. Mit weiteren Werkzeugen können in der Folge Mitarbeiter dazu verleitet werden, eine Verbindung mit dem falschen Access Point aufzubauen. Sobald das passiert, hat der Angreifer Kontrolle über den gesamten Datenverkehr. Im Sinne einer Man-in-the-Middle-(MitM-)Attacke kann er sämtliche Eingaben manipulieren, mitschneiden, verändern und umlenken, oder einfach nur Informationen sammeln – im schlimmsten Fall erhält er auf diese Weise Zugriff auf Usernamen und Passwörter für Social-Media-Plattformen oder sogar Unternehmensanwendungen.

4. Rogue Clients

Rogue Clients sind ganz allgemein Rechner mit unautorisiertem WLAN-Adapter oder entsprechende Smart Devices, die sich in Reichweite des Unternehmens-WLANs befinden und sich mit diesem verbinden wollen. In minderschweren Fällen wird dabei nur die Firmen-Internetverbindung mitgenutzt, was beim Aufruf illegaler Inhalte allerdings auf den WLAN-Betreiber zurückfallen kann. Tiefergehende Attacken könnten darüber hinaus geschützte Bereiche des Netzwerks zum Ziel haben. IT-Administratoren sollten jederzeit Kenntnis darüber haben, welche Geräte sich überhaupt mit dem Unternehmens-WLAN verbinden dürfen und diejenigen erkennen, denen dies trotz richtiger Anmeldedaten nicht erlaubt ist – wie etwa mitgebrachten privaten Smart Devices von Mitarbeitern.

5. Ad-hoc-Netzwerke

WLAN-Umgebungen sind in der Regel für den Einsatz im Infrastruktur-Modus konfiguriert. Das bedeutet, dass die Kommunikation aller angemeldeten Geräte über einen definierten Zugriffspunkt erfolgt. Alternativ oder als Option dazu kann jedoch auch der Ad-hoc-Modus aktiviert werden. Das versetzt die Geräte im WLAN in die Lage, untereinander zu kommunizieren. Dadurch lassen sich beispielsweise Druckaufträge direkt an einen WLAN-Drucker senden. Das Problem dabei: Oftmals sind diese Verbindungen entweder überhaupt nicht, oder nur mit einer schwachen und schnell knackbaren Verschlüsselung – wie WEP/WPA – gesichert. Darüber hinaus werden auf diesem Übertragungsweg vorhandene Network Security Policies umgangen. Außerdem läuft jeglicher Datenverkehr in einer Ad-hoc-Verbindung ohne Kenntnis des IT-Administrators ab. Bei Clients im Ad-hoc-Modus be-

Auch durch die neue Mobilfunkgeneration wird die Sicherheit im WLAN zum Thema. (Foto: © iStock.com/scanrail)

steht zudem die Gefahr, dass bestehende Ordnerfreigaben auf einem Laptop den Zugriff auf eigentlich nicht beabsichtigte Bereiche zulassen oder lokale Adressbücher etc. ausgelesen werden können.

6. Falsch konfigurierte Access Points

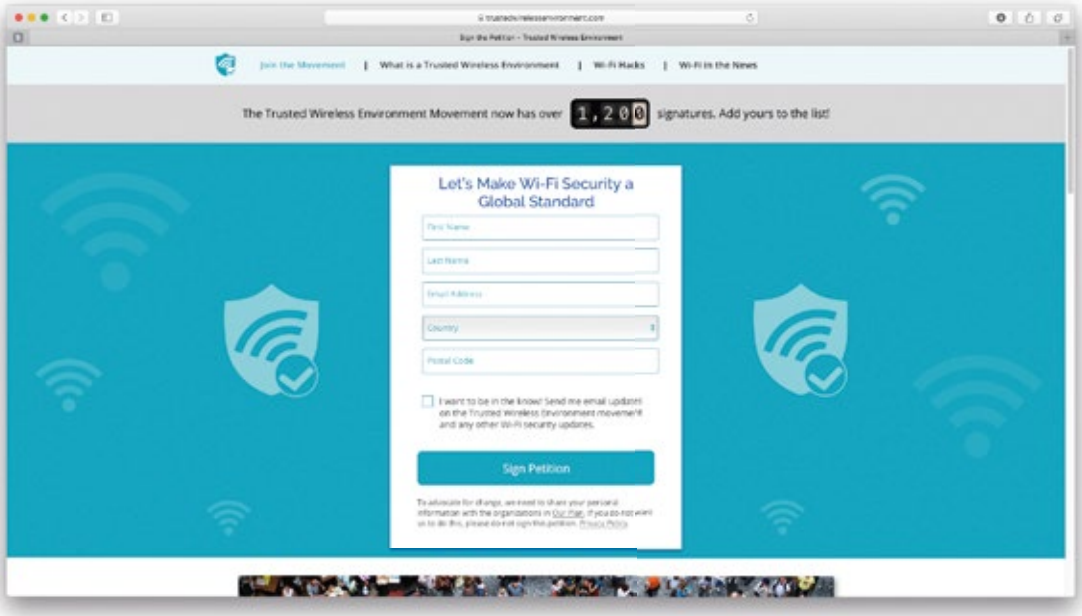
Zu den Basics in diesem Bereich gehört, dass alle Access Points über die aktuelle Firmware, identische SSID und Einstellungen beziehungsweise Policies sowie mindestens WPA2-Enterprise-Verschlüsselung verfügen müssen. Der Zugang zur Benutzeroberfläche sollte mit einem starken Passwort geschützt und nur von einer zentralen Stelle aus möglich sein. Es empfiehlt sich, unnötige Ports für Telnet, HTTP und FTP etc. zu schließen. Ein entsprechender „Health Check" in Form von Verbindungstests zu Clients und Unternehmensapplikationen hinsichtlich Geschwindigkeit und Qualität sollte regelmäßig erfolgen.

Trusted Wireless Environment als Best Practise

Um all diesen Gefahrenquellen effektiv den Riegel vorschieben zu können, bedarf es des Aufbaus eines „Trusted Wireless Environments", das nicht nur reibungslosen Datentransfer gewährleistet, sondern darüber hinaus auch einfach zu managen ist und hohe Sicherheit bietet. Alle Vorkommnisse darin werden über ein Wireless Intrusion Prevention System (WIPS) erkannt, Bedrohungen proaktiv unterbunden, protokolliert sowie zu Analysezwecken transparent aufbereitet. Dadurch schützen sich Unternehmen nicht nur vor Cyberkriminellen und unvorsichtigen Mitarbeitern: In Verbindung mit geeigneten Visualisierungslösungen bietet sich ihnen des Weiteren die Möglichkeit, das Verhalten aller unternehmenseigenen und fremden Geräte in WLAN-Reichweite zu kontrollieren und zu steuern. Die sechs großen WLAN-Bedrohungen verlieren durch mehr Transparenz ihren Schrecken. Zudem lassen sich übliche Problemsituationen im Netzwerk – wie Clients mit einer schlechten Verbindung, sich immer wieder an- und abmeldende Systeme oder die Eingabe falscher Pre-shared-Keys – automatisiert verarbeiten und in Form eines Dashboards darstellen. Individuelle Anfragen von Anwendern können bis zu einer Woche rückwirkend abgerufen und im Rahmen eines Drilldowns bis auf das jeweilige Endgerät bearbeitet werden.

WLAN-Sicherheit als Thema im Zuge von 5G

Die Sicherheit im WLAN rückt aber nicht nur im klassischen Unternehmensumfeld zunehmend in den Fokus, sondern auch im Zuge der neuen Mobilfunkgeneration 5G. Beim Zugriff auf sensible Informationen via



Auf www.trustedwirelessenvironment.com kann jeder seine Stimme abgeben, um die Entwicklung verbindlicher Sicherheitsstandards im WLAN voranzutreiben. (Screenshot der Webseite vom 30.10.2019, 11.57h)

SmartPhone oder Tablet – beispielsweise beim Onlinebanking, aber ebenso bei der Nutzung von Cloud-Anwendungen im geschäftlichen Umfeld – vertrauen viele heute eher dem Mobilfunknetz als einem öffentlichen WLAN: Ein Ansatz, der durchaus nicht verkehrt ist. Dass damit den potenziellen Gefahren einer WLAN-Umgebung jedoch vollumfänglich ein Riegel vorgeschoben wird, kann sich künftig immer öfter als Trugschluss herausstellen. Fakt ist, dass Mobilfunkanbieter trotz 5G nicht mit den steigenden Bandbreitenanforderungen Schritt halten können und dem Konzept des WLAN-Offloadings via Hotspot 2.0 oder Passpoint immer mehr Bedeutung zukommt.

Hierbei wird die Mobilfunkverbindung nahtlos auf ein entsprechend verfügbares WLAN umgeleitet. Cisco beispielsweise geht davon aus, dass weltweit künftig 71 Prozent des gesamten 5G-Verkehrs über WLAN laufen werden. Das Prekäre daran: Oftmals wissen die Mobilfunknutzer gar nicht, dass sie gerade über ein WLAN surfen und der damit einhergehenden Gefahr ausgesetzt sind. In dem Zusammenhang ist die Bedrohung, die von Evil Twin Access Points ausgeht, am eklatantesten. Der Nutzer wiegt sich in der Annahme, dass der Schutz seiner Daten über die gültigen Sicherheitsstandards der Mobilfunktechnologie gewährleistet ist und läuft dabei gleichzeitig Gefahr, dass seine Verbindung auf einen Evil Twin umgeleitet wird, der den Angreifer in die Lage versetzt, Informationen einzusehen und abzugreifen. Selbst wenn beim WLAN-Offloading die Unternehmensversionen der Sicherheitsprotokolle WPA2 oder WPA3 zum Tragen kommen, die grundsätzlich als sicherer gelten, zeigten die Vorfälle rund um „KRACK" und „Dragonblood" auch in dem Fall klare Schwächen der Verschlüsselung auf. Insofern sollten Unternehmen wie Privatpersonen ihren Umgang mit diesem Thema genau hinterfragen.

Standardisierung forcieren

WLAN-Anbieter, die sich für die Umsetzung eines „Trusted Wireless Environment" entscheiden, können nur gewinnen: Sie profitieren in den eigenen Reihen von einem wichtigen zusätzlichen Schutzschirm. Im öffentlichen Bereich lassen sich Kunden durch vertrauenswürdige Strukturen an sich binden – potenziellen Reputationsverlusten durch geglückte Hacker-Attacken wird wirkungsvoll das Fundament genommen. Doch solche Einzelbestrebungen sind meist nur ein Tropfen auf dem heißen Stein. Essenziell ist vor allem die Einführung und Durchsetzung weltweit gültiger Standards für sicheres WLAN. Genau dafür macht sich die Initiative „Trusted Wireless Environment" stark. Ziel ist hier, die Verfügbarkeit sicherer WLAN-Verbindungen weltweit zu erhöhen, damit sich Anwender weniger Sorgen machen müssen. Jede gesammelte Unterschrift soll dazu beitragen, diese Vision gemeinsam mit Organisationen wie dem PCI Security Standards Council, IEEE oder der Wi-Fi Alliance voranzutreiben.

Weitere Informationen und die Möglichkeit der Teilnahme unter: www.trustedwirelessenvironment.com. ■

JONAS SPIECKERMANN,
Senior Sales Engineer,
WatchGuard Technologies