Sicheres WiFi durch ganzheitlichen Security-Ansatz

Viele Unternehmen und Organisation bieten heutzutage freies WiFi an – von großen Einrichtungen wie Bahnhöfe, Flughäfen, Städte und Kommunen über Einkaufszentren, Hotels und Restaurants bis hin zum kleinen Cafe um die Ecke. Gäste machen davon stark Gebrauch und wählen sich sehr oft in öffentliche WiFi-Netze ein. Laut ein repräsentativen Umfrage von Bitcom nutzt jeder zweite Bundesbürger über 16 öffentliche, kostenlose WiFi-Hotspots. Doch wenn der Anbieter nicht genügend Wert auf die Sicherheit seines WiFi legt, lauern Security-Gefahren an jeder Ecke. So kann beispielsweise der Nutzer sein eigenes Gerät infizieren. Aber auch der Anbieter selbst kann sich infizieren, wenn sich unbekannte Nutzer mit einem infizierten Gerät einloggen. Es gibt aber einen sicheren Weg für Unternehmen, ihr Netzwerk zu schützen, indem das WiFi konsequent in die Security-Strategie integriert wird.

Access Points als vorderste Verteidigungslinie
Die effektivste Methode, das Unternehmens-WiFi zu schützen, ist die Verzahnung der Wireless Technik mit der IT-Security. Sophos hat beispielsweise in seinem Synchronized-Security-Konzept, bei dem Endpoints, Server und Firewalls als integriertes System agieren und unter anderem den Sicherheitszustand der Geräte austauschen, auch seine Access Points (AP) eingebunden. Damit kann ein WiFi-AP den Sicherheitszustand eines Geräts (Aktuelle Malware-Infektion, Aktualität des Betriebssystems oder Jailbreak/Rooting eines Smartphones) feststellen. Prinzipiell kann der Betreiber unsichere Geräte zwar im Gast-Netz zulassen, etwa im Cafe oder am Bahnhof. In das interne Netz kommen solch unsichere Devices durch eine gezielte Sicherheitsüberprüfung und eine zusätzliche Netzwerksegmentierung aber auf keinen Fall. Gesteuert wird die Sicherheit des WiFis zentral, ganz gleich, ob es sich in der Unternehmenszentrale oder beispielsweise in einer Filiale befindet – ein Regelwerk für die komplette Sicherheit inklusive WiFi im gesamten Unternehmen.

Gefahr durch IoT-Geräte
Auch bei der Einbindung von IoT-Geräten in das Unternehmens-WiFi besteht ein hohes Sicherheitsrisiko, da viele dieser Geräte vom Grundsatz her nicht auf Security ausgerichtet sind und somit ein Einfallstor für Angreifer in das drahtlose Netzwerk darstellen. Dazu gehören unter anderem Überwachungskameras, Displays oder auch proprietäre Scanner-Geräte, wie sie beispielsweise in der Logistik Verwendung finden. Der Herausforderung durch potenziell unsichere Geräte im eigenen Netzwerk muss ein Unternehmen mehrstufig begegnen, bei dem das WiFi in die Security integriert ist. Dazu gehört, dass sich Firmen- und BYOD-Geräte nur dann mit dem internen Netz verbinden dürfen, wenn sie den Unternehmensvorgaben entsprechen.

Ganzheitlicher Ansatz erforderlich
Zur Einbindung des WiFi samt Access Points in eine vernetzte und intelligente Security ist ein ganzheitlicher Ansatz mit Synchronisierung aller Endpunkte zwingend erforderlich. Denn so lässt sich der Datenverkehr im gesamten Unternehmensnetz kontinuierlich nach schädlichem Verhalten untersuchen und der Admin hat einen kompletten Überblick über den aktuellen Status des Netzes und der damit verbundenen Geräte. Zudem kann im Fall einer Unregelmäßigkeit sofort und automatisiert gehandelt werden. Ein infiziertes Gerät, das sich ins WiFi einklinken möchte, wird automatisch vom Rest des Netzwerks isoliert, um eine Ausbreitung der Gefahr zu unterbinden.

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