5G stellt viele Herausforderungen an die IT-Sicherheit – aber nur wenige an Hacker

Die 5G-Technologie bringt immense Verbesserungen für die vernetzte Gesellschaft mit sich. Damit einher gehen jedoch auch neue Anforderungen für die IT-Sicherheit, da der neue Funkstandard eine Überwachung potentieller Hackeraktivitäten noch schwieriger macht. Dan Schiappa, Executive Vice President und Chief Product Officer bei Sophos kommentiert Gefahren und Möglichkeiten zum Schutz.

Schon heute sehen wir den Anfang der 5G-Implementierung, hauptsächlich noch in Headsets und Laptops. In Kürze, mit dem Boom an 5G-fähigen IoT-Geräten, wird die Technologie bei beinahe allen Arbeitsplätzen omnipräsent sein. Ob Mitarbeiter in den Büros oder im heimischen Arbeitszimmer sitzen – 5G-Frequenzen werden in eine Vielzahl an Geräten eingebunden sein, vom Computer über den Drucker bis zum Süßigkeitenautomat im Pausenraum. Nun, da immer mehr Menschen remote arbeiten und Organisationen sich damit auch mit den IoT-Geräten der Mitarbeiter zu Hause auseinandersetzen müssen, ist es für Unternehmen noch wichtiger geworden, ihre Daten überall und unabhängig von eigenen Netzwerken zu schützen.

5G wird also neue Sicherheitsherausforderungen für Unternehmen schaffen – und neue Möglichkeiten für Cyberkriminelle. Welche Bedrohungen sehen wir bereits auf uns zukommen, und welche erwarten wir mit der Ausbreitung von 5G-Technologien? Und wie können wir uns bereits heute schützen?

5G macht sich unsichtbar

Der Mangel an Sichtbarkeit, der bereits bei 3G und 4G bestand, wird bei 5G ein noch größeres Problem darstellen. Aufgrund der rasanten Geschwindigkeit der neuen Funktechnologie und ihres Potenzials, exponentiell mehr Daten zu bewegen, sowie der Konnektivität, die das gängige Breitband übertrifft, wird die nicht vorhandene Sichtbarkeit ein entscheidendes Thema in Sachen Sicherheit darstellen.

Was wir im besten Fall in einer 5G-Umgebung sehen werden, ist, ob ein Gerät 5G-Frequenzen nutzt. Aber es gibt keine Klarheit darüber, was über die Frequenzen übermittelt wird, so dass es eine echte Herausforderung ist, verdächtige Aktivitäten zu erkennen. Wir können 5G-Aktivitäten zwar entdecken, zum Beispiel mit einem Spektrometer, aber wir werden nicht in der Lage sein, gute versus schadhafte Aktivitäten auszumachen, da wir schlichtweg nicht sehen können, was in den Kommunikationsweg eingebettet ist.

Nicht verwaltete Geräte als hohes Risiko

Besonders hoch ist das Sicherheitsrisiko bei nicht verwalteten Geräten. Cyberkriminelle könnten hier in der Lage sein, unentdeckt Daten zu exfiltrieren. Doch auch bei verwalteten Geräten bestehen Herausforderungen. So bleiben Angreifer während der Attacke zwar nicht mehr gänzlich inkognito, doch sie können immer noch den 5G-Backchannel nutzen, um Daten herauszufiltern. Davon unabhängig bleibt es nahezu unmöglich, alle Risiken richtig einzuschätzen, wenn kein Einblick darüber möglich ist, was in der eigenen Umgebung passiert. Darum ist die Sichtbarkeit bei 5G solch ein Problem.

Um diese Gefahrenquelle zu minimieren, könnten Organisationen die verbindliche Einbindung von IoT-Geräten an das Unternehmens-WiFi beschließen, damit zumindest etwas Einblick in den Datenverkehr entsteht und so möglicherweise verdächtige Kommunikation entdeckt

werden kann. Wenn verwaltete Geräte mit einem Agent ausgestattet sind, ist zumindest erkennbar, dass seitens eines nicht verwalteten Geräts via 5G kommuniziert wird. Man kann allerdings nicht entschlüsseln, was das Gerät genau sagt, und das macht es sehr schwierig, Attacken zeitnah zu orten.

Vorteile von 5G bedeuten leider leichtes Spiel für Hacker
5G-Technologie übertrifft seine Vorgänger mit höherer Geschwindigkeit, größerer Bandbreite und geringerer Latenz, was wahrscheinlich dazu führen wird, dass es wesentlich flächendeckender verbreitet sein wird als 4G es je war. Diese allgegenwärtige Verfügbarkeit – und seine Effektivität – liefert Cyberkriminellen große Möglichkeiten. Ein Hacker kann sich zum Beispiel unsichtbar Zugang zum Kopierer verschaffen, in dem eine 5G-Frequenz eingebunden ist, und damit Zugang zu sämtlichen sensiblen Informationen auf dem Gerät erhalten. Mithilfe von 5G können Angreifer sehr schnell alle Daten abschöpfen – und zwar ohne in der betroffenen Organisation für Alarm zu sorgen. Die Technologie erfordert von Cyberkriminellen dabei keinerlei neuen Fähigkeiten, sie können einfach ihre bewährten Angriffsmethoden auf das Netzwerk nutzen.

Wie kann man sich gegen 5G Angriffe schützen?
Unternehmen sollten nun nicht versuchen Geräte mit 5G unbedingt zu vermeiden, weil sie ein potenzielles Sicherheitsrisiko darstellen. Stattdessen sollten sie sich ins Bewusstsein rufen, dass sich in ihren Unternehmensinfrastrukturen in Zukunft zahlreiche 5G-Geräte befinden werden und bereits jetzt notwendige Vorsichtsmaßnahmen umsetzen:

- 5G kann eine Hintertür ins Unternehmensnetzwerk darstellen. Deshalb sollten sich Unternehmen über Netzwerk-Trennungen und deren Verwaltung Gedanken machen. Für die IT-Sicherheitsabteilung bedeutet das: Sie sollten alles einsehen können, es darf keine „schwarzen Löcher“ und damit potenzielle Überraschungen geben.

- Der Fokus sollte auf den nicht verwalteten Geräten in der Unternehmensumgebung liegen. Sie lassen sich via Netzwerkscans oder über ein spezielles EDR-Produkt (Endpoint Detection and Response) erkennen. Das Unternehmen sollte sich zudem eine Strategie überlegen, wie man diese Geräte sicherer machen kann.

- Nach wie vor gilt: Unternehmen sollten bewährte Verschlüsselungs- und Zugangs-Kontrollen benutzen, die ein solides Level an Sicherheit für die Daten und den Zugang zu diesen liefern.

Da im Arbeitsalltag kontinuierlich neue Infrastrukturen und Dienste implementiert werden, sollten IT-Abteilungen die oben genannten Risiken auf dem Schirm haben. Letztendlich wird die Ankunft von 5G die Notwendigkeit verstärken, jede einzelne Ebene der Unternehmensumgebung zu schützen. Je früher Organisationen damit anfangen, desto besser.

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