Netzwerktrennung
Mehr Sicherheit bei der Arbeit im Homeoffice

Netzwerktrennung für mehr Sicherheit

Im Jahr 2020 waren etwa 96% der Haushalte in Deutschland mit einem Internetzugang ausgestattet[1]. Gleichzeitig arbeiteten im Januar 2021 etwa 24% aller Beschäftigten in Deutschland im Homeoffice.[2]

Viele Unternehmen konnten durch die vermehrte Bereitstellung von Homeoffice-Arbeitsplätzen ein positives Resümee für sich ziehen - auch in Corona-Zeiten. Dieser Trend hat positive Auswirkungen auf die zukünftige Entwicklung von Homeoffice-Arbeitsplätzen. Eine Kehrseite kann jedoch ein unzureichender Schutz des Heimnetzwerkes und damit des Homeoffice-Arbeitsplatzes bedeuten.

> Besuchern kann durch die WLAN-Nutzung Zugriff auf alle Endgeräte freigegeben werden, die sich im gleichen WLAN-Netz befinden. Daher ist hier auf die Trennung von Geräten, die Firmendaten beinhalten, besonders zu achten.
> Schadsoftware, die auf ein Endgerät geladen wurde, kann sich im schlimmsten Fall auch innerhalb eines Firmennetzwerkes ausbreiten und Dateien verschlüsseln und/oder Daten ausspähen.

Netzwerksegmentierung - So geht es!

Viele Hersteller von WLAN-Routern implementieren die Funktion der Gastnetzwerke. Über die Admin-Oberfläche des Routers kann die Gastnetzwerkfunktion aktiviert werden. Das Gastnetzwerk stellt, bildlich gesprochen, einen „unsicheren“ WLAN-Bereich neben einem „sicheren“ WLAN-Bereich dar. Wenn ein solches Gastnetzwerk eingerichtet ist, sollte dies von Geräten, die ansonsten im sicheren WLAN eingebunden sind, getrennt werden. Gästehandys, Spiele-PCs oder SmartHome Komponenten können über das unsichere Netzwerk mit dem Internet verbunden werden. Getrennt davon arbeiten sensible Geräte in dem zweiten WLAN-Netz.

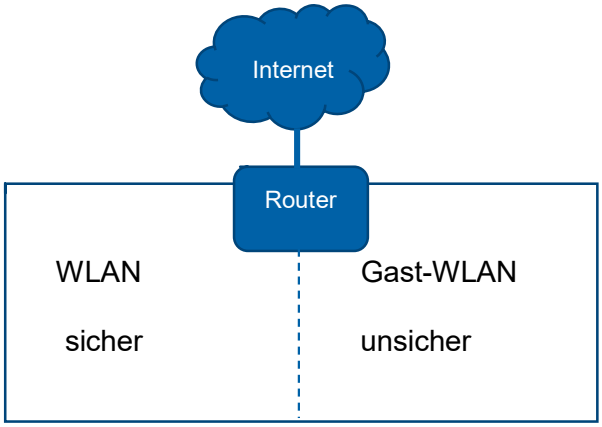

Abb. 1: Segmentierung via Gastnetzwerk

[1] Vgl. Statista 2021 - Haushalte, die mind. ein Mitglied im Alter von 16-74 Jahre besitzen

[2] Vgl. Statista 2021 (veröffentlicht 27.04.2021) - Entwicklung der Nutzung von Homeoffice vor und während der Corona-Pandemie bis 2021

Kontakt:
Landeskriminalamt Nordrhein-Westfalen
Völklinger Straße 49
40221 Düsseldorf

Stand: Juli 2021

Eine weitere Möglichkeit, für die Einrichtung eines zweiten sicheren Netzwerkes, ist die Implementierung eines zweiten Routers im vorhandenen Netzwerk. Der erste Router ist mit dem Internet verbunden und dient somit als Tor zum Internet für den dahinter geschalteten zweiten Router.

Der Vorteil an einer solchen Installation ist, dass alle Endgeräte, die im Netzwerk des zweiten Routers liegen, nicht direkt mit dem Internet verbunden sind und auch dort nicht durch mögliche Sicherheitslücken plötzlich zu Einfallstoren für Hacker werden.

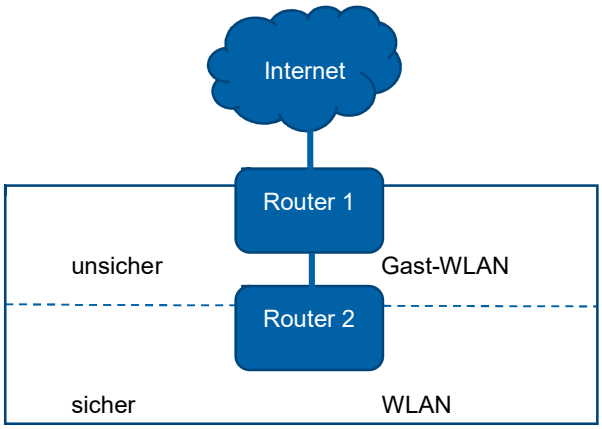

Abb. 2: Segmentierung via Kaskadierung

Diese kaskadenartige Aneinanderreihung von Routern kann ausgeweitet werden, um beispielsweise das Heimnetz vom sensiblen Homeoffice Bereich zu trennen und gleichzeitig Gästen oder unkritischen Smarthome-Endgeräten ein eigenes Netzwerk zuzuweisen.

Zur Verbesserung der Sicherheit kann darüber hinaus die Kommunikation der einzelnen WLAN-fähigen Endgeräte untereinander unterbunden werden. Dies ist insbesondere erforderlich, wenn zwei Endgeräte in den unterschiedlichen Netzwerken (unsicheres und sicheres WLAN) eingebunden sind und eine Verbindung der beiden Endgeräte aus Sicherheitsgründen nicht vertretbar ist.
Im Folgenden wird beispielhaft die Konfigurationseinstellung eines WLAN-Routers dargestellt:

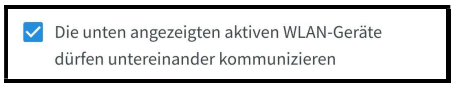

Abb. 3: WLAN Konfiguration

Der blau hinterlegte Haken in der Abbildung muss abgewählt werden, um die Kommunikation zwischen den Endgeräten zu unterbinden.

Leider bleibt bei allen Empfehlungen in der heutigen digitalen Welt ein Restrisiko. Sollten Sie Opfer einer Straftat geworden sein, steht Ihnen jede Polizeidienststelle für die Erstattung einer Strafanzeige zur Verfügung.

Kontakt:
Landeskriminalamt Nordrhein-Westfalen
Völklinger Straße 49
40221 Düsseldorf

Stand: Juli 2021