Test Spicker (117) 08.09.23

1. Kennt die Einstellungen für ein Netzwerkgerät

- **IP-Adresse:** Jedes Gerät in einem Netzwerk benötigt eine eindeutige IP-Adresse, um erreichbar zu sein. Dies kann manuell oder automatisch (durch DHCP) festgelegt werden.
- **Subnetzmaske und Gateway:** Diese Parameter bestimmen, wie das Gerät mit anderen Netzwerken kommuniziert
- **DNS-Server:** Der Domain Name System (DNS) Server übersetzt Webadressen in IP-Adressen. Die Einstellung eines geeigneten DNS-Servers ist wichtig.
- **SSID und Passwort (bei WLAN-Geräten):** Für drahtlose Netzwerke benötigen Sie den Netzwerknamen (SSID) und das Passwort, um sich zu verbinden.
- **Verschlüsselung (bei WLAN-Geräten):** Die Wahl der richtigen Verschlüsselungsmethode (z. B. WPA2 oder WPA3) ist entscheidend für die Sicherheit Ihres WLANs.

2. Kennt die Informationen zu Störungen

Bei WLAN- und Internetverbindungen sind Störungen oft ein häufig auftretendes Problem. Hier sind einige Beispiele für Störungen in diesem Kontext:

- **Funkstörungen:** Drahtlose Netzwerke wie WLAN sind anfällig für Funkstörungen. Dies kann durch elektronische Geräte, Mikrowellen, Metallwände oder andere drahtlose Netzwerke in der Nähe verursacht werden.
- **Signalabschwächung:** Die Signalstärke eines WLANs nimmt mit der Entfernung zum Router ab.
- **Interferenz:** Interferenz tritt auf, wenn Signale von benachbarten WLAN-Routern oder anderen Funkquellen auf denselben Frequenzen stören.
- **Bandbreitenengpässe:** Wenn viele Geräte gleichzeitig auf das Internet zugreifen oder große Datenmengen übertragen, kann dies zu Bandbreitenengpässen führen, was zu langsameren Verbindungen führt.
- **DNS-Probleme:** Fehlerhafte DNS-Einstellungen können dazu führen, dass Websites nicht gefunden werden oder Verzögerungen beim Aufrufen von Webseiten auftreten.
- **Netzwerkprobleme des Internetdienstanbieters (ISP):** Störungen im Netzwerk des Internetdienstanbieters können die gesamte Internetverbindung beeinträchtigen.

Um Störungen bei WLAN- und Internetverbindungen zu beheben, können Sie folgende Schritte unternehmen:

- -Überprüfung der Hardware
- -Kanalwechsel
- -Positionierung des Routers
- -Aktualisierung von Treibern und Firmware
- -ISP-Kontakt

3. Kennt die Sicherheitskriterien für WLAN Geräte

Verschiedene Sicherheitskriterien von entscheidender Bedeutung:

- **Verschlüsselung:** Verwenden Sie starke Verschlüsselungsprotokolle wie WPA2 oder WPA3, um die Kommunikation zwischen WLAN-Geräten zu schützen.
- **Passwortschutz:** Vergeben Sie sichere, eindeutige Passwörter für Ihr WLAN und ändern Sie diese regelmäßig.
- **SSID-Versteck:** Deaktivieren Sie die Übertragung Ihres SSID-Namens, um das Netzwerk vor neugierigen Blicken zu schützen. (Ein SSID-Name ist der Name Ihres WLAN-Netzwerks)
- **MAC-Adressenfilterung:** Beschränken Sie den Zugriff auf Ihr WLAN nur auf autorisierte Geräte durch die Filterung von MAC-Adressen.
- **Firewall:** Aktivieren Sie eine Firewall, um den Datenverkehr zu überwachen und unerwünschte Zugriffe zu blockieren.

Nachteile der Verwendung von WLAN:

Die Nachteile von WLAN im Zusammenhang mit der Sicherheit sind:

1. Drahtlose Übertragung:

WLAN-Netzwerke senden Daten über die Luft, was sie anfällig für Abhörversuche macht. Unverschlüsselte oder schlecht verschlüsselte Verbindungen können leicht von Dritten abgefangen werden.

2. Passwortsicherheit:

Wenn schwache Passwörter verwendet werden oder Standardpasswörter nicht geändert werden, können Angreifer leicht auf das WLAN-Netzwerk zugreifen.

3. MAC-Adressen-Spoofing:

Angreifer können die MAC-Adresse eines autorisierten Geräts kopieren und sie verwenden, um Zugriff auf das WLAN-Netzwerk zu erhalten.

4. WPS-Schwachstelle:

Die Wi-Fi Protected Setup (WPS) -Funktion, die dazu dient, Geräte schnell mit einem WLAN-Netzwerk zu verbinden, kann unsicher sein und potenziell von Angreifern ausgenutzt werden.

5**. Kleinere Reichweite der Verschlüsselung:**

Selbst bei Verwendung von Verschlüsselungstechnologien wie WPA2 oder WPA3 kann die Reichweite der Verschlüsselung begrenzt sein, insbesondere wenn Schwachstellen in der Implementierung vorhanden sind.

4. Berechtigungen des Datenspeichers:

Lesen:

Diese Berechtigung ermöglicht es einem Benutzer oder einer Anwendung, auf gespeicherte Daten zuzugreifen und sie anzuzeigen.

Schreiben:

Mit dieser Berechtigung können Benutzer oder Anwendungen Daten ändern oder neue Daten in den Speicher schreiben.

Ausführen (bei ausführbaren Dateien):

Dies erlaubt das Starten von ausführbaren Dateien oder Programmen.

Besitzerrechte:

Der Besitzer von Daten hat oft mehr Berechtigungen als andere Benutzer und kann die Zugriffsrechte verwalten.

Gruppenberechtigungen:

In Unix-basierten Systemen können Benutzer in Gruppen organisiert sein, und Gruppenberechtigungen steuern den Zugriff von Mitgliedern dieser Gruppen auf bestimmte Daten.