Security Lektion 3
Netzwerke

- Netzwerktypen
- Netzwerkverbindungen
- Schutzmaßnahmen
  Firewalls
  Drahtlose Netzwerke

✓ Ein Netzwerk ist eine Gruppe von miteinander verbundenen Rechnern. Der Sinn eines Netzwerkes besteht beispielsweise im gemeinsamen Zugriff auf Dateien oder Hardware (Drucker). Eine Verbindung zu einem Netzwerk kann sich jedoch negativ auf die Datensicherheit auswirken (Malware, unberechtigter Datenzugriff, Verletzen der Privatsphäre).
In dieser Lektion beschäftigen Sie sich darum auch mit dem Schutz eines Netzwerks vor unberechtigtem Zugriff.

Aufgabe

1. Netzwerktypen

Je nach Größe des Netzwerks wird zwischen verschiedenen Netzwerktypen unterschieden:

- **LAN**

  Ein *Local Area Network* (lokales Netzwerk) begrenzt die miteinander verbundenen Rechner auf ein Bürogebäude oder den privaten Haushalt.

- **MAN**

  Ein *Metropolitan Area Network* vernetzt Rechner über eine Stadt hinweg.

- **WAN**

  Ein *Wide Area Network* (auch Weitverkehrsnetz genannt) verbindet die Rechner über weite Entfernungen hinweg. Dehnt sich die Vernetzung weltweit aus, spricht man manchmal von einem GAN, einem *Global Area Network*.

- **VPN**

  Ein *Virtual Private Network* gestattet Zweigstellen, Außendienstmitarbeitenden und / oder Telearbeitenden den Zugang zum Firmennetzwerk. Diese sichern Tunnel werden auch für Fernwartungen genutzt.

- **PowerLan**

  Ein *PowerLan,* auch *Powerline Communication* (PLC) genannt, verbindet die Rechner nicht mit Kabeln, sondern nutzt das Stromnetz, also Steckdosen. Meist wird es in privaten Haushalten verwendet.

- **WLAN**

  Ein *Wireless Local Area Network* ist eine LAN-Variante. Zum Übertragen der Daten verwenden die Rechner Funktechnologie.

- **VLAN**
  Ein *Virtual Local Area Network* teilt einfach das LAN in einzelne Netzwerke, beispielsweise für verschiedene Arbeitsgruppen.

Die Vorteile von Netzwerken sind unter anderem:

- Daten werden im sogenannten *Datenverbund* gemeinsam genutzt
- Ressourcen werden im Netzwerk gemeinsam im sogenannten *Funktionsverbund* genutzt (Drucker)
- Sollten einzelne Komponenten ausfallen, kann im sogenannten *Verfügbarkeitsverbund* auf einem anderen Rechner weiter gearbeitet werden
- Datensicherungen sind in Netzwerken einfacher durchzuführen als auf vielen einzelnen Rechnern

2. Netzwerkverbindungen

Die Verbindungsmöglichkeiten innerhalb eines Gebäudes können sowohl drahtlos als auch über Kabel erfolgen. Sind die Rechner weiter voneinander entfernt, werden Telefonleitungen oder Satelliten genutzt. In privaten Haushalten funktioniert die Übertragung der Daten auch über das oben erwähnte PowerLan, also über die Steckdose. Die Netzwerkkarten sind dabei entweder schon im Gerät eingebaut oder können über einen USB-Stick oder über eine PCMCIA Karte eines Laptops angeschlossen werden.

Hotspot für Smartphones einrichten
Mit vielen Smartphones können Sie einen eigenen WLAN-Hotspot aufbauen. Besuchen Sie Ihren Handyshop oder die Website Ihres Providers. Hier finden Sie bestimmt detaillierte Anleitungen und Hilfen, um auf Ihrem Gerät einen persönlichen Hotspot einzurichten.

Durch das Aktivieren der Hotspot-Funktion können andere WLAN-fähige Geräte Ihre Internet-Verbindung per USB, Bluetooth oder WLAN nutzen. Ihr Smartphone wird so als WLAN-Netzwerk für alle internetfähigen Geräte in der Umgebung sichtbar. Das bietet unter anderem einige Vorteile:

- Sie möchten nur einmal für die mobile Datennutzung zahlen und nicht doppelt für Smartphone und Tablet.
- Sie haben ein Notebook auf eine Reise mitgenommen und möchten damit ins Internet, haben aber keinen Stick für mobiles Internet dabei.
- Sie sind mit einigen Personen unterwegs und möchten nur eine Internetverbindung nutzen.

Die WLAN-Hotspot-Funktion lässt sich auf den meisten Geräten relativ leicht und bequem einrichten. Meist finden Sie es in den EINSTELLUNGEN.

Betriebssystem Android
Android bietet drei Möglichkeiten, das Smartphone als WLAN-Hotspot zur Verfügung zu stellen. Eine davon ist per Kabel, die anderen beiden sind kabellos.[1]

[1] *Quellen: Eigene Recherchen am Smartphone, über das Internet und beim Provider „Drei" unter https://www.drei.at/portal/de/bottomnavi/kontakt-und-hilfe/tipps-und-tricks/handy-als-wlan-hotspot/*

- USB-Tethering
  Von Tethering spricht man, wenn ein internetfähiges Endgerät wie PC oder Tablet mit dem Smartphone zwecks Internetverbindung gekoppelt wird (USB-Tethering mittels Kabel, Bluetooth-Tethering kabellos).

  Der Zugriff für andere Geräte läuft über ein Mini-USB-Kabel. Am Smartphone wählen Sie in den EINSTELLUNGEN | DRAHTLOS UND NETZWERKE | TETHERING UND MOBILER HOTSPOT | TETHERING. (Diese Menüführung kann von Gerät zu Gerät variieren.)

  Zum Aktivieren reicht es, das Smartphone und das andere Gerät über ein Mini-USB-Kabel miteinander zu verbinden und die Funktion durch ein Tippen auf das Häkchen-Symbol zu aktivieren. In der Regel verbindet sich dann das Gerät automatisch mit dem Internet. Eine Passworteingabe ist nicht notwendig, da die Verbindung nur über das Kabel läuft und daher auch kein anderes Gerät zugreifen kann.

- Mobiler WLAN Hotspot
  Der Zugriff für andere Geräte ist kabellos. Am Smartphone wählen Sie in den EINSTELLUNGEN | DRAHTLOS UND NETZWERKE | TETHERING UND MOBILER HOTSPOT | MOBILER WLAN-HOTSPOT. (Diese Menüführung kann von Gerät zu Gerät variieren.)

  Nun müssen Sie den Hotspot unter MOBILER WLAN-HOTSPOT KONFIGURIEREN einrichten. Dabei können Sie das Passwort und den Netzwerknamen unter dem Ihr Handy später auf anderen Geräten aufscheint, ändern.

  Um den mobilen, kabellosen WLAN-Hotspot zu aktivieren, setzt man am Smartphone ein Häkchen bei dem gleichnamigen Menüpunkt.
  Wählen Sie dann am anderen Gerät Ihr Smartphone unter den drahtlosen Netzwerken aus.
  Nach der Aktivierung erscheint am Smartphone in der Navigationsleiste sowie bei den Benachrichtigungen ein Hinweis, dass der Hotspot jetzt aktiv ist. Berühren Sie diese Benachrichtigung, kommen Sie wieder zu den Hotspoteinstellungen, wo Sie den Hotspot jederzeit wieder deaktivieren können. Bis zur Deaktivierung ist Ihre Datenverbindung für andere internetfähige Geräte (Tablets, Handys, Laptops etc.) wie ein normales WLAN-Netzwerk verfügbar.

- Bluetooth Tethering
  Der Zugriff für andere Geräte ist kabellos. Am Smartphone wählen Sie in den EINSTELLUNGEN | DRAHTLOS UND NETZWERKE | TETHERING UND MOBILER HOTSPOT | BLUETOOTH-TETHERING. (Diese Menüführung kann von Gerät zu Gerät variieren.)

  Zum Aktivieren schalten Sie zuerst auf beiden Geräten Bluetooth ein und machen Sie dieses auch für andere Geräte sichtbar. Danach koppeln Sie die beiden Geräte und schalten dann am Smartphone das Bluetooth-Tethering wie oben beschrieben ein. Weil Sie selbst am Smartphone bestimmen welche Geräte gekoppelt werden dürfen, ist hier keine Passworteingabe notwendig.

Betriebssystem iOS
Bei iOS stehen ebenso drei Möglichkeiten zur Verfügung, das Endgerät mit dem WLAN des Smartphones zu verbinden. Zwei Möglichkeiten sind kabellos, eine per Kabel.

- USB-Tethering
  Der **Zugriff für andere Geräte läuft** über ein USB-Kabel. Am Smartphone wählen Sie in den EINSTELLUNGEN | MOBILE NETZWERKE BZW. MOBILES NETZ | PERSÖNLICHER HOTSPOT. Aktivieren Sie den Hotspot.

  Zum Aktivieren schließen Sie das andere Gerät und das iPhone an ein USB-Kabel an und folgen den Anweisungen am Bildschirm. Das angeschlossene Gerät verbindet sich automatisch mit dem Internet. Sobald die Internetverbindung funktioniert, wird die Navigationsleiste des iPhones blau. Die Verbindung besteht, bis man das USB-Kabel entfernt. Weil die Verbindung über ein Kabel läuft, ist keine Passworteingabe nötig.

- Mobiler WLAN Hotspot
  Der Zugriff für andere Geräte ist kabellos. Am Smartphone wählen Sie in den EINSTELLUNGEN | MOBILE NETZWERKE BZW. MOBILES NETZ | PERSÖNLICHER HOTSPOT. Aktivieren Sie den Hotspot.

  Nach dem Einrichten können Sie unter EINSTELLUNGEN | PERSÖNLICHER HOTSPOT diesen Hotspot ein- bzw. ausschalten und das Passwort ändern.

  Nachdem Sie Ihren persönlichen Hotspot aktiviert haben, wählen Sie am anderen Gerät Ihr iPhone unter den drahtlosen Netzwerken aus.
  Ist der Hotspot aktiv, wird die Statusleiste blau und zeigt an, wie viele Geräte verbunden sind. Die Datenverbindung ist so lange verfügbar, bis Sie sie in den EINSTELLUNGEN wieder deaktivieren.

- Bluetooth Tethering
  Der Zugriff für andere Geräte läuft kabellos. Am Smartphone wählen Sie in den EINSTELLUNGEN | MOBILE NETZWERKE BZW. MOBILES NETZ | PERSÖNLICHER HOTSPOT. Aktivieren Sie den Hotspot.

  Das Bluetooth-Tethering aktivieren Sie ebenfalls unter EINSTELLUNGEN | PERSÖNLICHER HOTSPOT. Die Geräte werden zuerst gekoppelt, dann kann der Laptop mit der Datenverbindung des Smartphones verbunden werden. Weil Sie am Smartphone bestimmen welche Geräte gekoppelt werden dürfen, ist eine Passworteingabe nicht notwendig.

Wenn Sie iOS 8 oder neuer nutzen, können Sie Ihre mobile Datenverbindung über den *Instant Hotspot* freigeben, ohne zuerst den persönlichen Hotspot einschalten zu müssen.[2]

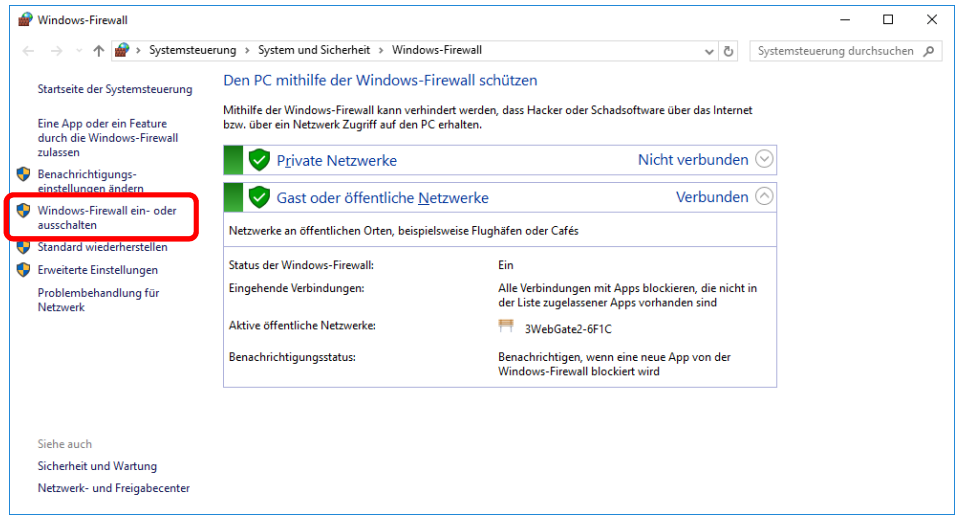
3. Schutzmaßnahmen

Firewalls
Eine Firewall wird analog zur physischen Feuermauer als Schutz in Netzwerken eingesetzt. Damit sollen unberechtigte Zugriffe von außen abgewehrt werden. Unter Windows ist die Firewall automatisch eingeschaltet. Leider bieten Firewalls alleine keinen ausreichenden Schutz vor Hackern.

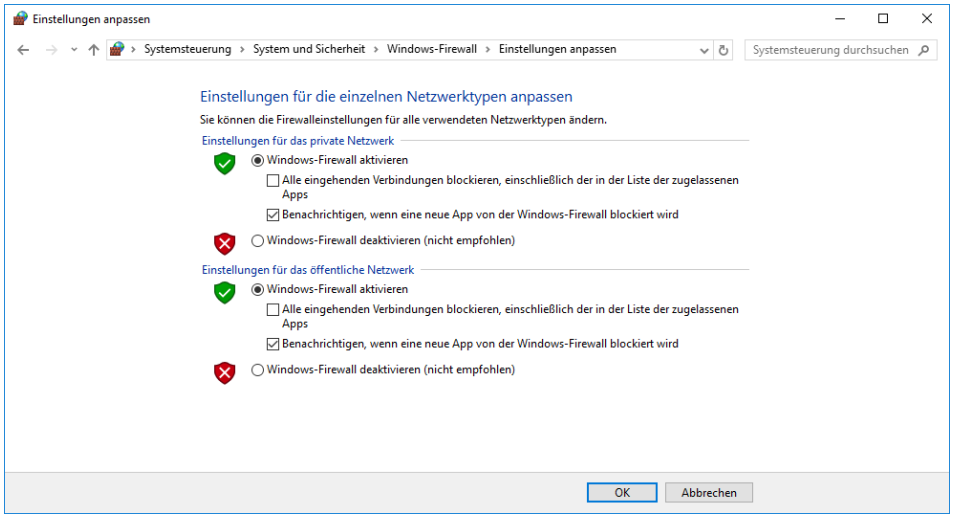
[2] *Quellen: Recherchen am eigenen Smartphone, online bei https://support.apple.com/de-at/HT204023 und meinem Provider „Drei" unter https://www.drei.at/portal/de/bottomnavi/kontakt-und-hilfe/tipps-und-tricks/handy-als-wlan-hotspot/*

Bedenken Sie, dass Firewalls auch keinen Schutz bieten, wenn Ihr Rechner bereits *kompromittiert* ist, dh bereits Schadensprogramme aktiv sind. Eine Spyware beispielsweise fordert und versendet selbständig Daten im Internet.

Klicken Sie unter **Windows 10** auf das Suchsymbol in der Taskleiste und geben Sie den Suchbegriff *Firewall* ein. Klicken Sie das Suchergebnis an, dann wird die Verwaltungsoberfläche angezeigt (siehe Abbildung). Alternativ öffnen Sie die SYSTEMSTEUERUNG und klicken hier unter SYSTEM UND SICHERHEIT auf WINDOWS-FIREWALL. Unter früheren Windows-Versionen müssen Sie so vorgehen.

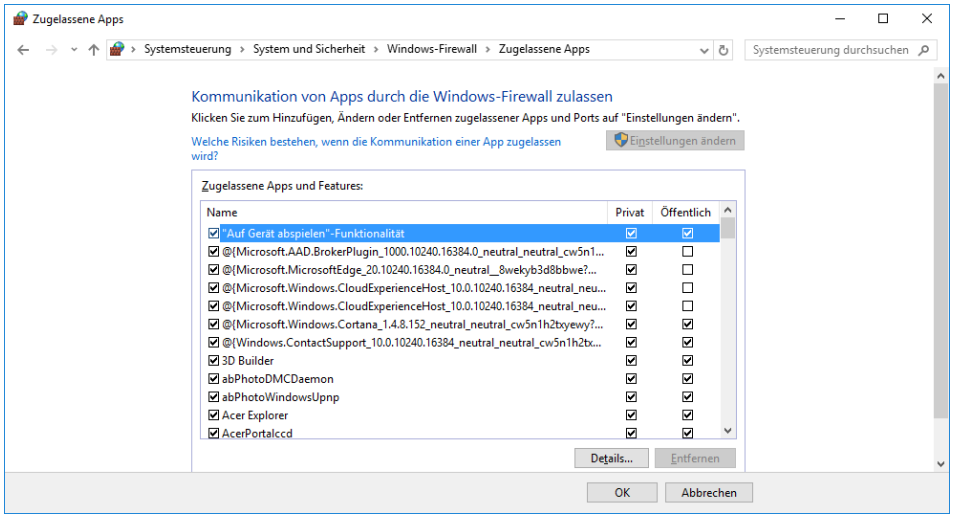


- Hier können Sie die Firewall ein- oder ausschalten (siehe Umrandung in der Abbildung oben).
- Im dann eingeblendeten Fenster aktivieren oder deaktivieren Sie die Firewall (siehe Abbildung unten).



Lassen Sie die Firewall auf jedem Fall eingeschaltet!

Möchten Sie bestimmte Anwendung zulassen oder verhindern, dann wechseln Sie zurück zur Verwaltungsoberfläche. Klicken Sie links auf EIN APP ODER EIN FEATURE DURCH DIE WINDOWS-FIREWALL ZULASSEN. Das Fenster ZUGELASSENE APPS wird geöffnet (siehe Abbildung). Hier sehen Sie, welche Apps zugelassen bzw. deaktiviert sind und können selber Einstellungen ändern.



Haben Sie die Administratorrechte, so können Sie über die Schaltfläche **Einstellungen ändern** bestehende Regeln anpassen.

Drahtlose Netzwerke

Drahtlose Netzwerke müssen unbedingt aus Sicherheitsgründen verschlüsselt werden. Der Benutzende gibt bei der Anmeldung ein Passwort ein und wird so mit dem Netzwerk verbunden. Nur so kann gewährleistet werden, dass lediglich Berechtigte auf das Netzwerk zugreifen und die Daten bei einer verschlüsselten Übertragung sicher sind.

Verschiedene Verfahren zum Schutz drahtloser Netzwerke sind *WEP* (Wired Equivalent Privacy), *WPA* (Wi-Fi Protected Access) oder *MAC-Listen* (Media Access Control). Haben Sie Ihr mobiles Gerät mit einem WLAN verbunden, können Sie die ausgesendete SSID[3] verbergen. Mit entsprechenden Tools werden diese unsichtbaren Netze aber auch aufgespürt. Darum sind passwortgeschützte Verfahren die zu empfehlende Variante.

Gefahren eines ungesicherten WLANs

Wenn Sie ein ungesichertes WLAN nutzen, kann jeder zugreifen, der sich in Reichweite befindet. Von einem Eindringling können durch Hijacking Daten, Benutzerkonten, E-Mail-Konten und Web-Accounts übernommen werden. Eindringlinge können eine verfügbare Internetverbindung nutzen und auf Kosten des WLAN-Besitzers surfen. Der Besitzer des WLANs trägt nicht nur die Kosten, sondern auch die Konsequenzen für illegal heruntergeladene Inhalte[4]. Erschwerend ist dazu die unterschiedliche Rechtslage in den einzelnen Ländern. In Österreich beispielsweise gibt es das Recht auf

[3] *SSID heißt Service Set Identifier. Wie Sie Ihre eigene SSID herausfinden, erfahren Sie unter anderem bei chip.de unter http://praxistipps.chip.de/eigene-ssid-herausfinden-so-gehts_28856*

[4] *Lesen Sie dazu einen Artikel vom 4. März 2016 unter http://derstandard.at/2000032256436/Filesharing-Fluechtlinge-werden-Geschaeft-fuer-Abmahn-Anwaelte*

Privatkopie und im Gegensatz zu Deutschland gibt es keine pauschale *Störerhaftung*. In Deutschland berichtet die Online-Ausgabe von derstandrad.at vom 4. März 2016 von einem geflohenen Syrer und Filmfreund: *„Er kam im August 2015 nach Deutschland und ist mittlerweile in der Nähe von Hannover ansässig. Ein Nachbar ermöglichte ihm Zugriff auf sein WLAN, den S. unter anderem dafür nutzte, sich den Film "Margos Spuren" via Bittorrent herunterzuladen. Ein Verhalten, das für ihn in Syrien sanktionslos geblieben wäre. Dem Nachbarn brockte dies als Anschlussinhaber allerdings ein Abmahnschreiben mit einer Forderung von 815 Euro, davon 600 Euro als Schadenersatz für den Rechteinhaber, ein.“* [5]

Sicherheit Schritt drei
Netzwerk schützen

Übung und Selbststudium

1. Finden Sie Beispiele für LANs, MANs und WANs.
2. Sie haben sicher schon in einem Netzwerk gearbeitet oder Informationen aus einem Netzwerk eingeholt. Was sind Vorteile von Netzwerken?
3. Wenn Sie das nächste Mal innerhalb der Reichweite eines öffentlichen Netzwerkes sind, dann verbinden Sie Ihr mobiles Gerät damit.
4. Wie erstellen Sie auf Ihrem Smartphone einen persönlichen Hotspot?
5. In dieser Lektion wurde gesagt, dass eine Firewall allein keinen ausreichenden Schutz vor unberechtigten Zugriffen bietet. Erarbeiten Sie, was Sie zusätzlich tun können, um Daten vor Eindringlingen zu schützen.

Testen Sie Ihr Wissen

1. Welche Aufgabe hat eine Firewall?
2. Wie kann man ein drahtloses Netzwerk schützen?
3. Was heißt WPA?
4. Wie nennt man ein Netzwerk, bei dem die Übertragung mittels Funk-technologie funktioniert?
5. Erklären Sie den Begriff Virtual Private Network.
6. Wozu wird ein persönlicher Hotspot am Smartphone erstellt?
7. Ist die Firewall am Laptop notwendig bzw. ist sie standardmäßig eingeschaltet?

Mehr zum Thema Zugriffskontrollen erfahren Sie in der nächsten Lektion.

[5] Selber Artikel unter *http://derstandard.at/2000032256436/Filesharing-Fluechtlinge-werden-Geschaeft-fuer-Abmahn-Anwaelte*