Maßnahmen zur Absicherung von Netzwerken

Firewall

1. Beschreibe den Begriff *Port* im Zusammenhang mit einem Datennetz im OSI-Modell.

   Die Portnummer wird durch einen Doppelpunkt getrennt an die IP-Adresse angehängt.

   *Der **Port** ist dem TCP-Protokoll zuzuordnen, also der Schicht 4 des OSI-Modells.*

   Damit wird die Information übermittelt, welches Protokoll auf der

   Anwendungsebene zu verwenden ist.

Firewall–Einstellungen beim WLAN-Router am Beispiel der FritzBox

Jeder aktuelle WLAN-Router sollte mit einer Netzwerk-Firewall ausgestattet sein.

2. Formuliere kurz in eigenen Worten, wofür die Firewall zuständig ist.

   z. B.: Sie lässt nur die Verbindungen zu, die aus dem eigenen Netzwerk angefordert wurden.

Die Netzwerk-Firewall sollte im Prinzip nie deaktiviert werden! Wenn ein WLAN-Router (im Beispiel unten eine Fritzbox) die Internetverbindung eines anderen Routers nutzt (*Routerkaskade* bzw. *IP-Client-Modus*), ist die Firewall nicht aktiv. Dann sollte aber auf dem anderen Router eine Firewall eingerichtet sein.
Für manche Anwendungen, z. B. Smarthome-Komponenten oder Spiele können Portfreigaben eingerichtet werden. Damit leitet der Router Datenpakete an ein bestimmtes Gerät weiter.

Hinweise:

- Ein **VPN** (Virtual Private Network) ermöglicht, über das Internet auf Geräte in dem privaten Netzwerk zuzugreifen. Diesen Dienst bieten verschiedene Provider an. Von dem Provider erhält man u. a. eine DynDNS-Adresse (für „dynamisch“) die man oben unter dem Reiter VPN eingeben kann.
- **UPnP** (Universal Plug and Play) ist für die automatisierte Vernetzung von Geräten in einem Lokalen Netz zuständig (z. B. Drucker, Scanner, Smarthome-Komponenten). Durch UPnP erhalten Geräte die öffentliche IP-Adresse des NAT-Gateways mit den zu verwendenden NAT-Zuordnungen. Das Gerät kann diese Daten nutzen, um von außen über das Internet erreichbar zu sein.

3. Erläutere den Begriff *Port-Weiterleitung*.
(vgl. Arbeitsblatt 03, S. 3 und Lerninhalte 02, S. 2)

Der Router leitet Datenpakete, die über einen bestimmten Port eintreffen,

an ein zuvor festgelegtes Gerät im Lokalen Netz weiter.

Damit werden die Sicherheitsmechanismen des Routers untertunnelt,

damit die Geräte von außen erreichbar sind.

- Eine Firewall verhindert unerwünschte Zugriffe auf Geräte von außen. Wenn mit UPnP ein Zugriff über das Internet ermöglicht wird, umgeht man damit die Firewall.
Hier wird für die Nutzung der Daten ein anderes Protokoll verwendet als für die Kommunikation. Die Festlegung des Protokolls durch den Port wird also umgangen. Das ist bei vielen „smarten" Geräten der Fall, z. B. bei Smart-TVs oder bei Haushaltsrobotern.
Die Firewall erkennt aber **nicht**, ob es sich bei einem Zugriff um einen Angriff handelt.

- Immer wieder tauchen Meldungen über Sicherheitslücken im Zusammenhang mit UPnP auf, weshalb diese Funktionalität nur aktiviert sein sollte, wenn sie unbedingt benötigt wird, z. B.:

„**Der Bot im Babyfon** – Am Freitag vergangener Woche waren die Webseiten von Internetriesen wie Amazon, Twitter, PayPal oder Netflix über Stunden nur schwierig zu erreichen. Grund war eine digitale Attacke auf den Internetdienstleister Dyn. Dessen Aufgabe ist, die Domain-Namen wie amazon.com in die dazugehörigen IP-Adressen zu übersetzen. Mit einer sogenannten DDoS-Attacke ... wurde dieser derart überlastet, dass er unter der Last zusammenbrach und in der Folge die Webseiten seiner Kunden nicht erreichbar waren ... Neu an diesem Angriff ist, dass er mit einem Botnetz durchgeführt wurde, das zu großen Teilen aus mit dem Internet verbundenen Haushaltsgeräten (IoT-Geräte) besteht. Das sogenannte Mirai-Botnetz hat dabei auf Grund der großen Anzahl der Geräte eine Bandbreite erreicht, die weit über die bisher bekannter Botnetze hinausgeht. Die Netzwerkkameras, Babyfone oder Kühlschränke, die bereits zum Botnetz gehören, scannen offenbar selbstständig das Internet nach weiteren Geräten, um sie mit Schadsoftware zu infizieren und dem Botnetz hinzuzufügen. Das Mirai-Botnetz wächst also stetig weiter.
In ein Heimnetzwerk integrierte IoT-Geräte bauen oftmals selbstständig eine Verbindung zum Internet auf, indem sie den Router des Nutzers per UPnP (Universal Plug and Play) so konfigurieren, dass eine Portweiterleitung entsteht. Die Geräte können dann nicht nur ins Netz kommunizieren, sondern sind auch von außerhalb des Heimnetzwerkes sichtbar. Damit werden alle Schutzfunktionen des Routers und der entsprechenden Firewall ausgehebelt.
Für den Benutzer bedeutet dies nicht nur, dass sein Gerät Teil eines Botnetzes geworden ist, sondern auch, dass in sein Heimnetzwerk bereits Schadsoftware eingeschleust wurde. Diese Lücke kann theoretisch zu einem späteren Zeitpunkt auch für andere Aktivitäten genutzt werden.
Wie kann ich mich schützen?
  - Der Nutzer schützt sich am besten durch eine Deaktivierung der UPnP-Funktion am Router.
  - Nicht benötigte Dienste sollten deaktiviert oder über die Firewall eingeschränkt werden.
  - Muss eine Erreichbarkeit von außen, also über das Internet gewährleistet sein, sollte dies nur über eine ausreichend starke Authentisierung ... mit einem starken Passwortschutz geschehen.
  - Bei der Auswahl der Geräte sollte nicht nur die Funktionalität und das Preis-Leistungsverhältnis beachtet werden, sondern auch Aspekte der IT-Sicherheit. Im Zweifel hilft eine fachmännische Beratung durch IT-Spezialisten weiter.
  - Daten sollten nur verschlüsselt übertragen werden. Bietet das Gerät diese Funktion nicht an, sollte nur über einen VPN-Tunnel kommuniziert werden.

..."
(Bundesamt für Sicherheit in der Informationstechnik; https://www.bsi-fuer-buerger.de/BSIFB/DE/Service/Aktuell/Informationen/Artikel/Botnetz_iot_24102016.html vom 24. 10 2016)

4. Erläutere in Bezug auf den Artikel des Bundesamtes für Sicherheit in der Informationstechnik (BSI):
   - Die Funktion des Internetdienstleisters Dyn.
     Dyn bietet einen DNS-Dienst an.
   - DDoS-Attacke:
     Das massenhafte wiederholte Anfragen eines Dienstes mit Hilfe eines Botnetzes.
   - Bot:
     Geräte wie Computer, Smartphones, Tablets oder Smarthome-Komponenten, die mit Schadsoftware infiziert sind und durch diese - vom Nutzer unbemerkt – fremdgesteuert werden können.
   - Mirai-Botnetz:
     Ein Botnetz, das zu großen Teilen aus mit dem Internet verbundenen Haushaltsgeräten (IoT-Geräte) besteht.
   - Die Folgen für den Benutzer, wenn eines seiner Geräte Teil eines Botnetzes ist.
     Das Gerät ist Teil eines Netzes, das der Allgemeinheit schadet.
     Darüber hinaus kann die Schadsoftware, die auf dem Gerät installiert ist, weitere Schadfunktionen ausführen.

5. Das Mirai-Botnetz kann man –wie andere Botnetze auch – mieten. Schätze den Mietpreis.
   „... ein Botnetz mit 50.000 infizierten Geräten (kostet) über die Dauer der Mindest-Mietzeit von zwei Wochen zwischen 3000 bis 4000 US-Dollar.“
   (https://www.heise.de/security/meldung/Kriminelle-bieten-Mirai-Botnetz-mit-400-000-IoT-Geraeten-zur-Miete-an-3504584.html; 25.11.2016; 10:52 Uhr Dennis Schirrmacher)
   Anmerkung: Das Mirai-Botnetz verfügte zu diesem Zeitpunkt über etwa 400.000 IoT-Bots.
6. Fasse die vom BSI empfohlenen Schutzmaßnahmen in eigenen Worten zusammen.
   - *UPnP-Funktion am Router nach Möglichkeit abschalten.*
   - *Portfreigaben am Router für nicht benötigte Dienste löschen.*
   - *Wenn ein Gerät über das Internet erreichbar sein soll, darauf achten, dass dafür ein gutes Passwort verwendet wird.*
   - *Beim Kauf von Geräten nicht nur auf einen möglichst niedrigen Preis achten, sondern auch auf die IT-Sicherheit.*
   - *Nach Möglichkeit darauf achten, dass die Kommunikation über ein VPN-Tunnel und verschlüsselt erfolgt.*

   Anmerkung: Die Themen *VPN* und *Verschlüsselung* werden in den folgenden Kapiteln geklärt.

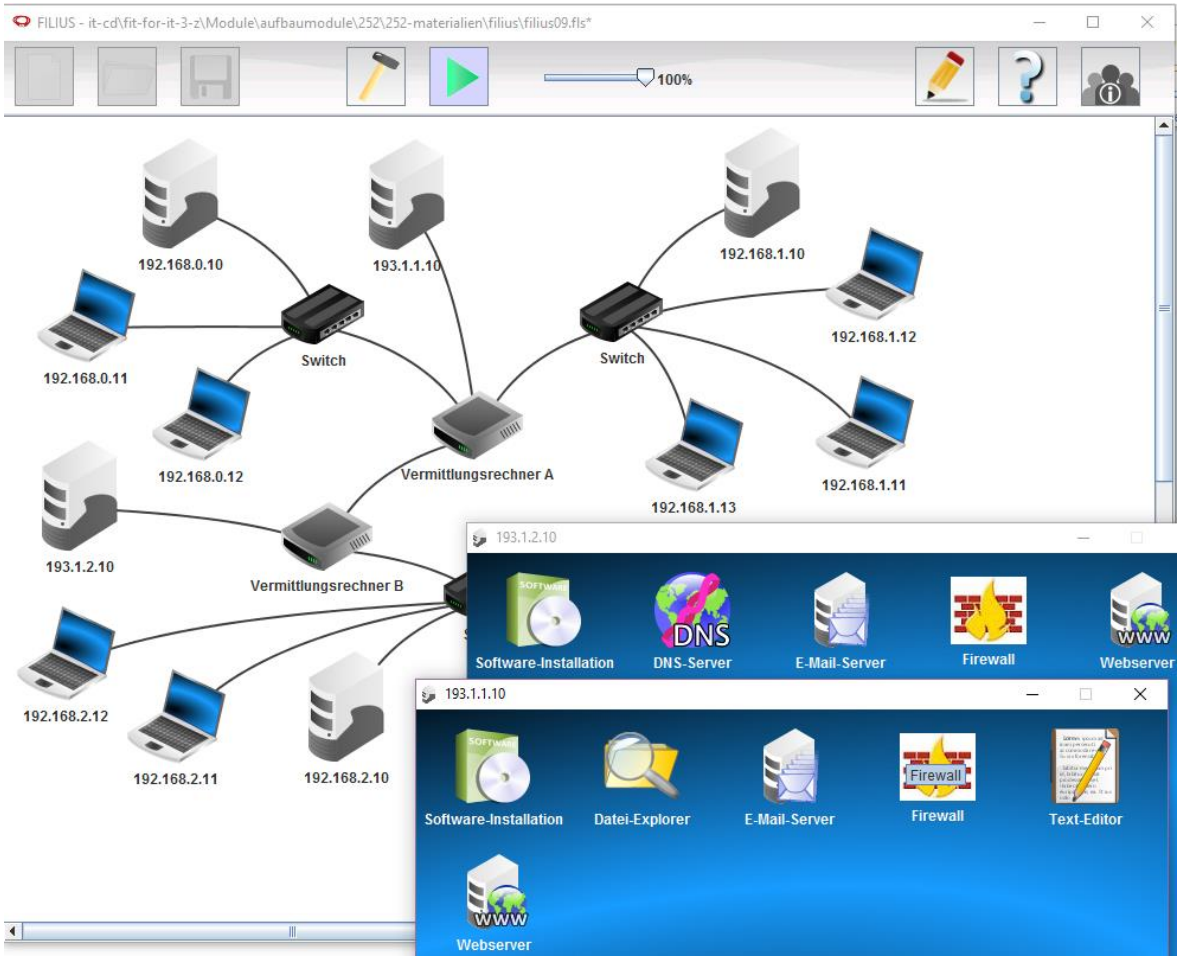
Simulation der Installation einer Firewall in FILIUS

7. Öffne dein zuletzt gespeichertes FILIUS-Netzwerk. (Vorlagedatei: v08-filius08.fls)
   Speichere das FILIUS-Netzwerk unter der Bezeichnung „Version09“.
   (*vgl. 252-materialien\filius\filius09.fls*)

   - Auf den Hosts 193.1.1.10 und 193.1.2.10 ist ein *Webserver* und ein *E-Mail-Server* installiert. Kontrolliere, ob der DNS-Server und die Webserver aktiv sind (auf der Konfigurationsseite muss in den oberen Schaltflächen jeweils *Beenden* bzw. *Anhalten* angezeigt werden).

   ➢ Eine **URL** (**U**niform **R**esource **L**ocator) wird umgangssprachlich als Internetadresse bezeichnet.

   - Mit Hilfe des Rechners, auf dem die erforderliche Client-Software installiert ist (in der Abbildung 192.168.1.12) kannst du die Konnektivität überprüfen: Jeweils *ping* (IP-Adresse), *ping* (URL) und im *Webbrowser* ebenso die IP-Adresse und die URL.
   - Installiere auf den Hosts im *Aktionsmodus* jeweils eine ***Firewall***.



   - Jetzt sollten beide Hosts nach wie vor auf ein ping antworten. Eine HTTP-Anfrage im Webbrowser führt aber zu der Fehlermeldung *Server konnte nicht erreicht werden*. Hier muss zuerst der Standardport Für HTTP (Port 80) als *zulässiger Port* hinzugefügt werden.