Technische Maßnahmen zur Absicherung von Netzwerken

Virenschutz

Virenschutzprogramme versuchen, Schadprogramme aufzuspüren und zu beseitigen. Zuverlässig erkannt werden aber nur bekannte Schadprogramme (vgl. Lerninhalte 1.8–04, S. 7-8).

Benutzerkennungen und Passwörter

Zur Anmeldung bei Internetdiensten ist die Kombination aus E-Mail Adresse und Passwort weit verbreitet. Durch deren Nutzung werden unweigerlich Daten des Anwenders gespeichert. Damit wird die Wahrscheinlichkeit erhöht, dass persönliche Daten in fremde Hände gelangen, denn laufend werden Anbieter gehackt und Benutzerdaten gestohlen. Beachte also (vgl. Lerninhalte 1.8–04, S. 9):

- **Nicht sicher** sind Passwörter, die sich aus einem Wort mit vorangestellten oder angehängten Ziffern oder Sonderzeichen zusammensetzen wie z. B. *Superpasswort92* oder *@Bello05*.
- Man sollte **nicht** für alle Zwecke dasselbe Passwort verwenden.
- Benutzerkennungen und Passwörter sollten **nie** unverschlüsselt gesendet werden.
- Ein Kennwort sollte möglichst lang sein und sollte Zahlen, Satz- und Sonderzeichen beinhalten. Groß- und Kleinbuchstaben sollten gemischt werden. Vermeiden sollte man Anführungszeichen und das kaufmännische Und (&), weil diese Zeichen manchmal nicht zulässig sind.
  Um sich dennoch mehrere Passwörter merken zu können, kann man zum Beispiel ein Grundpasswort verwenden und mit einem Schema erweitern, das von dem verwendeten Dienst abhängt.
  Man kann sich auch eine Eselsbrücke bauen. Beispielsweise das Kinderlied „**E**s **t**anzt **ein B**i-**B**a-Butzemann in unserm Haus herum“ könnte zu dem folgenden Gerüst führen:
  Et1B-b!@28 (! Wäre der Butzemann, @ zu Hause und 28 die eigene Hausnummer)
  Dieses Grundpasswort kann man dann um einen dienstabhängigen Teil ergänzen, z. B. für den privaten bzw. beruflichen E-Mail-Account:
  Et1B-b!E-MPr@28 bzw. **Et1B-b!E-MBer@28**
- Achte darauf, ob Anbieter besser abgesicherte Login-Verfahren anbieten als nur die Kombination aus E-Mail Adresse und Kennwort, z. B.:
  - PIN über Tastatur, zusätzliche PIN mit Maus schützt gegen Keylogger.
  - Benutzerkennung (nicht E-Mail Adresse) mit PIN; zusätzlich eTAN für Transaktionen.
  - Zwei-Faktor-Authentifizierung durch SMS-Code auf das Handy oder ein mit einer App generierten Einmal-Passwort (z. B. bei Facebook, Google, Microsoft, PayPal).
  - Multifaktor-Authentifizierung mit biometrischen Daten, z. B. Fingerabdruck oder Iris-Scan.
  - Zertifikat für den Benutzer, das in einer Datei oder in einer App auf dem Smartphone gespeichert wird, oder noch besser auf einem speziell dafür eingerichteten USB-Speicherstick.

Zwei getrennte Netze bzw. Zonen im WLAN

IoT-Geräte sind angreifbar und stellen ein Sicherheitsrisiko dar. Dieses Risiko lässt sich verringern, indem man zwei getrennte Netze bzw. Zonen im WLAN installiert (vgl. Arbeitsblatt 2.5.1–12, S. 6-7):

- Manche Router verfügen über die Option, ein **Gastnetz** zu aktivieren.
- Wenn das nicht möglich ist, kann mit einem zweiten Router eine **Routerkaskade** gebildet und ein zweites WLAN aufgespannt werden.
- Es gibt Router, die mehrere Zonen im Netzwerk unterstützen. Um diese zu konfigurieren, muss man sich aber intensiv mit IP-Adressierung beschäftigen (vgl. z. B. c’t 2017, Heft 14, S. 114-120)

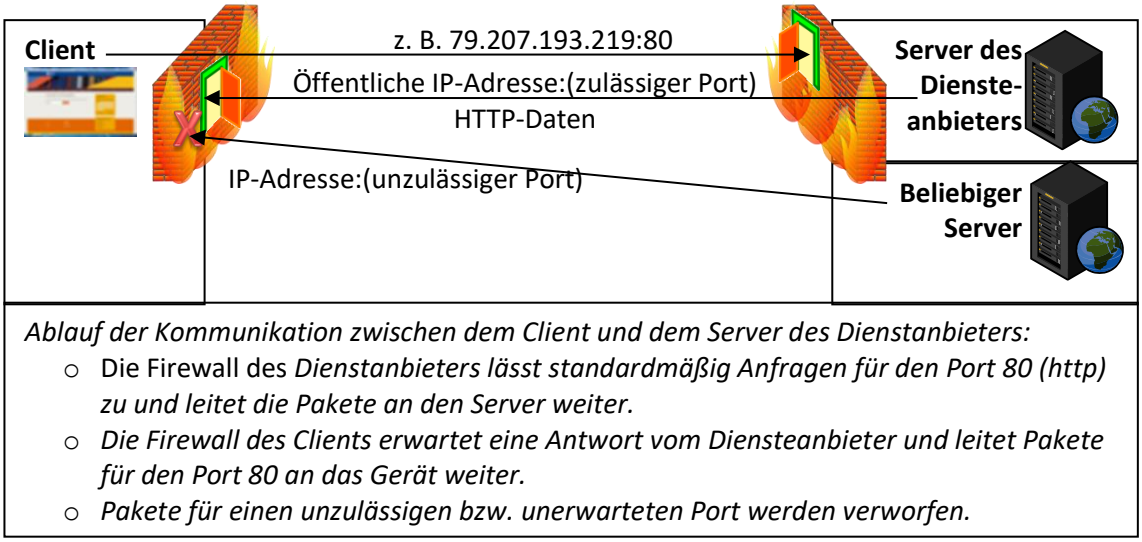
Firewall

Gleich vorab: Die Firewall ersetzt **nicht** den Virenschutz. Sie erkennt nicht, ob es sich bei einem Zugriff um einen Angriff, um eine gewollte Anwendung oder eine durch ein Schadprogramm initiierte Aktion handelt. Auch ersetzt die Netzwerk-Firewall **nicht** die Personal Firewall, die den Datenverkehr auf dem Gerät filtert.

Funktionsweise einer Netzwerk-Firewall

- Die Aufgabe der Firewall ist, die Teilnehmer im Netzwerk vor unerwünschten Zugriffen zu schützen. Die Firewall soll also nur IP-Pakete zu dem jeweiligen Gerät weiterleiten, die aufgrund des Ports als erwünscht eingestuft werden.

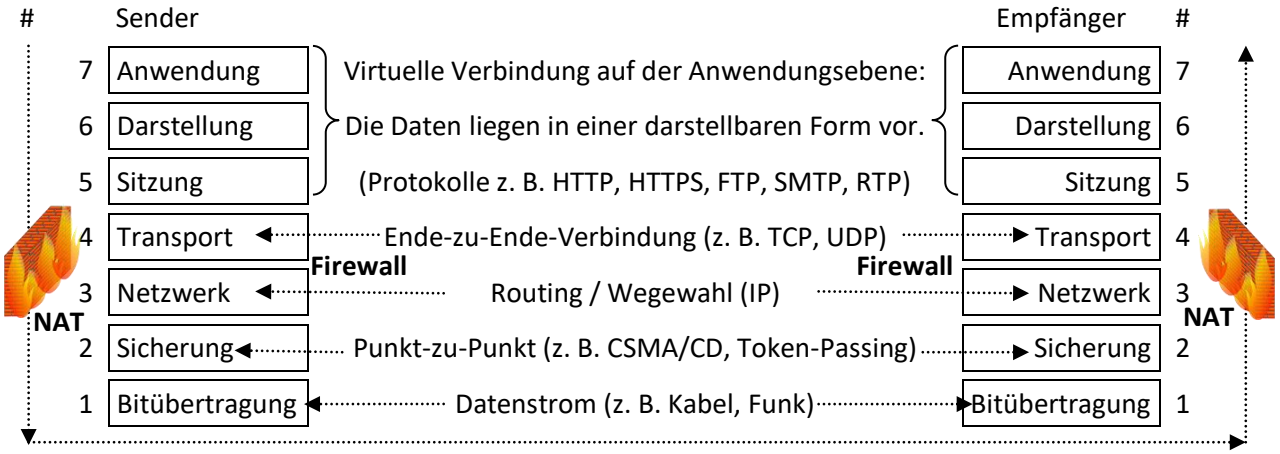
  Es gibt viele Variationen in der Funktionalität von Firewalls. Hier wird eine Firewall betrachtet, wie sie in WLAN-Routern verfügbar ist, die in den OSI-Schichten 3 und 4 angesiedelt ist.
  Beispiel: Der Standardport beispielsweise für HTTP ist 80.
  Eine IPv4-Adresse könnte unter Angabe des Ports zum Beispiel lauten: http://79.207.193.219:80



Ablauf der Kommunikation zwischen dem Client und dem Server des Dienstanbieters:
- Die Firewall des *Dienstanbieters lässt standardmäßig Anfragen für den Port 80 (http) zu und leitet die Pakete an den Server weiter.*
- *Die Firewall des Clients erwartet eine Antwort vom Diensteanbieter und leitet Pakete für den Port 80 an das Gerät weiter.*
- *Pakete für einen unzulässigen bzw. unerwarteten Port werden verworfen.*

- Im Internet ist nur die öffentlich IP-Adresse des Routers sichtbar. Für die Zuordnung der Pakete zu der privaten IP-Adresse des Clients ist die **NAT** (Network Address Translation) zuständig, wofür das Gateway eine Zuordnungstabelle aufbaut.

Um die Funktionsweise einer Firewall wirklich verstehen zu können, ist zusätzlich noch ein Blick in das OSI-Modell erforderlich: Die Portnummer ist Teil der IP-Adresse (Schicht 3). Auf der Schicht 4 kann kontrolliert werden, ob die Anfrage erwartet wird oder nicht.



A Bearbeite das Arbeitsblatt 05: Maßnahmen zur Absicherung von Netzwerken

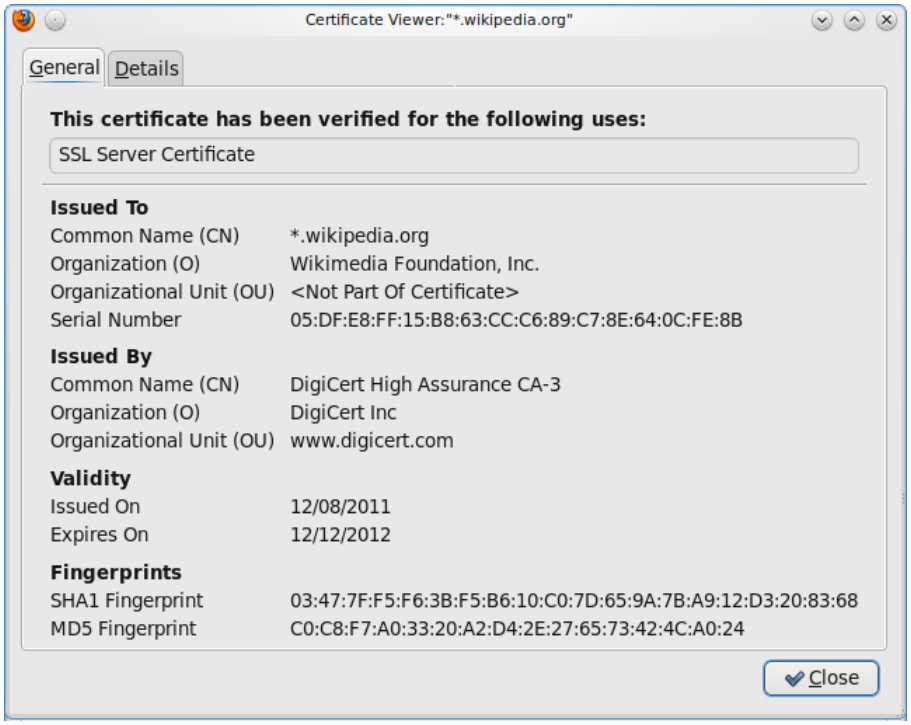
Verschlüsselung

- Bearbeite das Arbeitsblatt 06, S. 1 – 3: Verschlüsselung (Wiederholung)

SSL-Verschlüsselung ohne Forward Secrecy

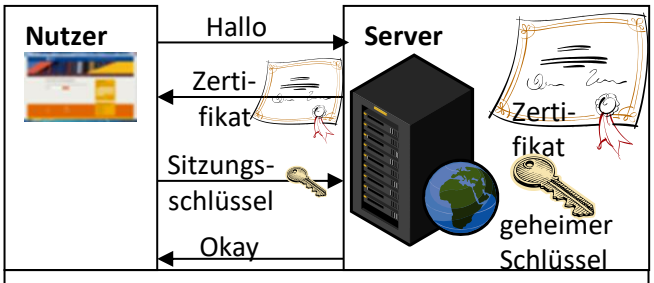
Zwischen den Protokollen HTTPS und TCP werden die Daten in der OSI-Schicht 5 (Sitzung) mit SSL (Secure Sockets Layer) bzw. dessen Weiterentwicklung TLS (Transport Layer Security) ver- und entschlüsselt. Dabei werden asymmetrische (z. B. RSA) und symmetrische Verschlüsselungsverfahren (z. B. AES) kombiniert. Hier spricht man von *hybrider Verschlüsselung*.
Beispielhaft wird hier der Ablauf einer Schlüsselvereinbarung mit RSA beschrieben:

- Dienstanbieter verfügen über ein Schlüsselpaar: Einen öffentlichen und einen geheimen (privaten) Schlüssel. Nachrichten, die mit dem öffentlichen Schlüssel verschlüsselt werden, können nur mit dem zugehörigen geheimen Schlüssel entschlüsselt werden.
- Der Browser des Nutzers Kontaktiert den Server Eines Dienstanbieters. Der Server sendet ein Zertifikat mit einem öffentlichen Schlüssel.
- Dafür muss sichergestellt werden, dass der Partner auch derjenige ist, für den er sich ausgibt. (**Authentifizierung**) Das geschieht mit Hilfe eines *Zertifikats*. Die Echtheit des Zertifikats überprüft eine Zertifizierungsstelle. Im Beispiel rechts ist das „DigiCert Inc“. Im Prinzip kann jedes Unternehmen Zertifikate anbieten. In Deutschland werden die Anbieter durch die Bundes-Netzagentur kontrolliert.



Beispiel für ein Zertifikat (Quelle: http://upload.wikimedia.org/wikipedia/commons/4/4b/ServerCertificate.png)

- Der Browser prüft die Unterschrift der Zertifizierungsstelle, verwendet den vom Anbieter erhaltenen Schlüssel und sendet eine damit verschlüsselte Zufallszahl als Sitzungsschlüssel, den der Server bestätigt. Damit liegt ein einmalig benutzbarer symmetrischer Schlüssel vor, der *Sitzungsschlüssel* bzw. Session-Key. Der Server bestätigt den Sitzungsschlüssel, mit dem jetzt beide Partner Daten verschlüsseln.



Ablauf der Schlüsselvereinbarung ohne Forward Secrecy

- Der geheime Schlüssel kann nur mit extrem hohem Aufwand aus dem öffentlichen Schlüssel berechnet werden. Dass aber zu Beginn der Kommunikation ein Sitzungsschlüssel übermittelt werden muss, ist der Schwachpunkt dieser Methode. Denn wenn ein Lauscher irgendwann den geheimen Schlüssel des Anbieters erhält, kann er im Nachhinein den Sitzungsschlüssel und damit den aufgezeichneten Datenverkehr entschlüsseln.

Schlüsselerzeugung nach Diffie-Hellman

Besonders geeignet für die Verschlüsselung von Daten ist das Potenzieren, weil die Umkehrung – das Logarithmieren – rechnerisch sehr aufwändig ist.
Mit Hilfe des Diffie-Hellman-Schlüsselaustauschs können zwei Kommunikationspartner einen geheimen Schlüssel vereinbaren, ohne dass dieser Schlüssel jemals gesendet wird. Es handelt sich also um ein *symmetrisches Verfahren*.

Beschreibung des Diffie-Hellman-Schlüsselaustauschs für mathematisch Interessierte:

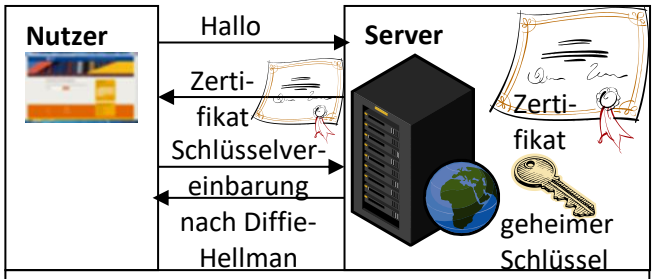
- Dafür wird eine große Primzahl p und eine weitere beliebige Zahl z benötigt.
  Diese beiden Zahlen können auch öffentlich bekannt sein.
- Partner A erzeugt eine Zufallszahl x und berechnet als Ergebnis a den Rest der Division von z^x geteilt durch p: $\mathbf{a = z^x \bmod p}$
- Partner B erzeugt eine Zufallszahl y und berechnet als Ergebnis b den Rest der Division von z^y geteilt durch p: $\mathbf{b = z^y \bmod p}$
- Die Partner A und B tauschen das Ergebnis ihrer Berechnungen a und b aus.
- Dann berechnen die Partner A und B den Rest der Division von z^{xy} geteilt durch p. Dadurch erhalten sie den Schlüssel s als Ergebnis der Rechnung $\mathbf{s = z^{xy} \bmod p}$.
  Dazu muss Partner A das Ergebnis Zahl b, das er von Partner B erhalten hat, mit seiner Zufallszahl x potenzieren und den Rest der Division durch p berechnen: $\mathbf{s = b^x \bmod p}$
  Partner B berechnet den Rest der Division von a^y geteilt durch p: $\mathbf{s = a^y \bmod p}$

Die Schlüsselerzeugung nach Diffie-Hellman bietet dadurch ein hohes Maß an Sicherheit:

- Sollte der Datenverkehr zur Schlüsselerzeugung belauscht worden sein, kann der Lauscher nur entweder zx oder zy berechnen, nicht aber zxy. Das könnte er nur, wenn er x oder y kennen würde, die aber nie bekannt gegeben wurden.
  Um von zx auf x zurückzuschließen, müsste man den Logarithmus – die Umkehrung des Potenzierens - berechnen. Dies ist aber so aufwändig, dass auch die schnellsten Rechner das nicht in einem vertretbaren Zeitraum schaffen.
- Ganz sicher ist aber auch dieses Verfahren nicht: Kann ein Angreifer den gesamten Datenaustausch während des Kommunikationsvorgangs belauschen und manipulieren, ist er in der Lage, beiden Partnern unterschiedliche Schlüssel unterzuschieben. Bei einem solchen **Man-In-The-Middle-Angriff** ist also auch der Diffie-Hellman-Schlüsselaustausch nicht sicher. Um diese Gefahr zu verringern, müssen die Kommunikationspartner mittels digitaler Signaturen authentifiziert werden.

Verschlüsselung mit Perfect Forward-Secrecy (PFS)

Bei einer Schlüsselvereinbarung nach Diffie-Hellman kann eine verschlüsselte Übertragung von Daten erreicht werden, ohne dass der Sitzungsschlüssel übermittelt werden muss.
Damit ist sichergestellt, dass ein belauschter Kommunikationsvorgang auch dann nicht entschlüsselt werden kann, wenn irgendwann ein geheimer Schlüssel ausgespäht wird:
Beide Kommunikationspartner löschen den Schlüssel nach Beenden der Sitzung.

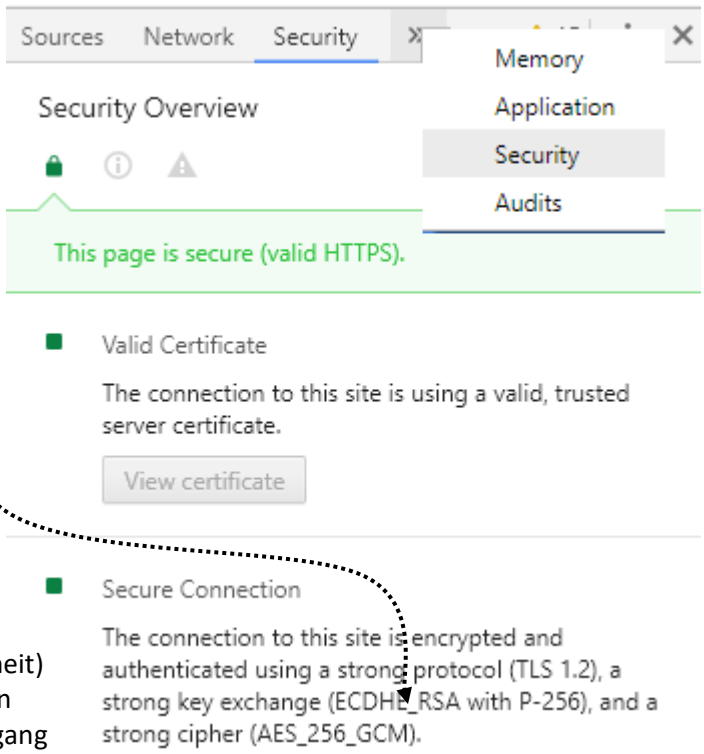


Ablauf der Schlüsselvereinbarung mit Forward Secrecy

Lediglich bei einem erfolgreichen Man-in-the-Middle Angriff nützt auch das nichts.
Asymmetrische Verschlüsselung ist aber nicht sehr schnell. Deshalb wird sie nur dafür verwendet, einen Schlüssel für **Symmetrische Verschlüsselung** auszuhandeln: Dann verwenden beide Partner denselben Schlüssel, der aber vorher über einen sicheren Kanal ausgetauscht werden muss.
Der „Cäsar-Code“ im Arbeitsblatt 06 war ein symmetrisches Verfahren.

Prüfen des verwendeten Verschlüsselungsverfahrens

Google Chrome liefert genaue Informationen zu dem verwendeten Verfahren zur Schlüsselvereinbarung (Stand: August 2017).
Dazu müssen die *Entwicklertools* aktiviert (Taste <F12>) und dort die Option *Security* ausgewählt werden.
Der Schlüsselaustausch mit *DHE* oder *ECDHE*… (Elliptic Curve Diffie-Hellman) verwendet Perfect Forward-Secrecy.
Ein typisches Beispiel für einen Schlüsselaustausch ohne PFS wäre *RSA*.



- Kennwörter sollten beim Dienstanbieter *gehasht* werden, damit sie nirgends im Klartext lesbar sind.
  Eine Information über verwendete Hashverfahren erhält man aber äußerst selten. Hier muss man dem Anbieter vertrauen. (vgl. Lerninhalte 1.8–04, S. 9: Datensicherheit)
  Das Hashen ist mit der Verschlüsselung von Daten vergleichbar. Nur soll der Hash-Vorgang nicht rückgängig gemacht – also nie wieder im Klartext sichtbar gemacht – werden können.

E-Mail

Die Verschlüsselung von E-Mails ist genauso wichtig wie die von Webseiten, denn: Werden E-Mails im Klartext versendet, kann jeder mitlesen, durch dessen Hände sie gehen.
Die Authentifizierung und Verschlüsselung von E-Mails ist aber komplizierter als die von Webseiten. Auch kann man die Verschlüsselung beim Versand und Empfang von E-Mails nicht mit einem Browser überprüfen. Mit Tools wie z. B. Wireshark kann man aber den Datenaustausch zwischen dem heimischen PC und dem Provider analysieren, indem man den eigenen Netzwerkverkehr belauscht.
Ansonsten kann man auch versuchen, verlässliche Informationen im Internet zu recherchieren.

Grundsätzlich gibt es für den Versand und die Speicherung von E-Mails zwei Wege. Darüber hinaus wurden zur Übermittlung elektronischer Post zwei nationale Systeme entwickelt:

- Beim Versand und Empfang mit einem E-Mail Client ist eine durchgängige Verschlüsselung vom Sender bis zum Empfänger mit (Open-)PGP (Pretty Good Privacy) möglich.
- Bei Verwendung von Webmail-Frontends sollte die Kommunikation vom PC zum Provider durch eine verschlüsselte Verbindung des Browsers abgedeckt sein. Die E-Mails und der Schlüssel liegen aber bei den Anbietern, denen man also vertrauen muss.
- Das gilt auch für die Dienste E-Postbrief der Deutschen Post bzw. De-Mail der Telekom und 1&1. Hier ist eine Authentifizierung durch persönliche Registrierung der Teilnehmer (durch PostIdent bzw. Paketzustelldienste) gewährleistet. Außerdem handelt es sich um geschlossene Systeme, die Daten gelangen also nicht ins Internet. Die Kommunikation zwischen Servern findet SSL-verschlüsselt statt.

Hier muss man abwägen, ob ein auf dem eigenen PC gespeicherter Schlüssel sicherer ist als ein bei einem Provider gespeicherter Schlüssel. Dienstanbieter sind verpflichtet, Daten auf richterlichen Beschluss herausgeben. Auch können Daten durch einen Angriff von Kriminellen bzw. Geheimdiensten entwendet werden. Dasselbe gilt aber auch für den eigenen PC.
Man sollte gewährleisten, dass für elektronische Post dieselbe Sicherheit wie bei einem Brief erreicht wird, nämlich dass sie gegen Kenntnisnahme gesichert wird. Damit kann den Brief nicht jeder lesen, dem er in die Hände fällt – und wer es dennoch tut, macht sich strafbar.

VPN (Virtuelles privates Netzwerk)

Bislang sollte klar geworden sein:

- In unverschlüsselten oder unsicher verschlüsselten **WLAN**s keine vertraulichen Daten wie Passwörter senden! Der Schlüsselaustausch mit ECDHE kann zwar im Nachhinein nicht mehr geknackt werden. Ein Krimineller kann sich aber in die Kommunikation einklinken, sich gegenüber dem Client und dem Host jeweils als deren Kommunikationspartner ausgeben und ein weiteres Schlüsselpaar erzeugen. Ein solcher **man-in-the-middle-Angriff** erfordert deutlich mehr Know How als die weiter verbreitete Methode, sich im Darknet einen Trojaner und E-Mail Adressen zu besorgen, ein paar E-Mails zu schreiben und auf einen DAU (von **D**ümmster **a**nzunehmender **U**ser) zu warten, der den Dateianhang mit dem Trojaner öffnet. Das wird aber praktiziert und damit ist auch diese Verschlüsselung nicht vollkommen sicher – wenn sich der Kriminelle in eine unverschlüsselte Kommunikation wie z. B. in einem WLAN einklinken kann.
- IoT Geräte untertunneln die Firewall, wenn über das Internet darauf zugegriffen werden soll.

➢ Um die Angriffsfläche zu verkleinern, bietet es sich an, einen VPN-Dienst zu nutzen.

Ein VPN ermöglicht eine verschlüsselte Internetverbindung zwischen einem Gerät und einem Server, der den VPN-Dienst anbietet. Der VPN-Server vergibt eine neue – virtuelle – IP-Adresse und leitet die Anfrage an den eigentlichen Diensteanbieter weiter. So erklärt sich die Bezeichnung *Virtuelles privates Netzwerk*: Es wird ein Netzwerk zwischen zwei Geräten aufgebaut, das nur solange besteht wie der Client mit dem VPN-Server kommuniziert. Außerhalb dieses Netzwerks kann die Kommunikation nicht mehr mitgelesen oder verändert werden kann. Man spricht hier deshalb auch von einem *VPN-Tunnel*.

- Dadurch werden Hacking-Angriffe erschwert, denn die eigentliche IP-Adresse ist nicht sichtbar.
- Da der VPN-Server stellvertretend für den eigentlichen Client auftritt, können mit einem VPN-Dienst auch Geobeschränkungen umgangen werden, die beispielsweise das Abspielen von Videos außerhalb bestimmter Regionen verhindern.
- Sofern die Abschirmungsmaßnahmen nicht so ausgefeilt sind wie beispielsweise in China, kann damit eventuell auch in Ländern mit einer Zensur auf beliebige Inhalte im Internet zugegriffen werden.
- Die Nutzung eines VPN-Dienstes verlangsamt die Internetverbindung geringfügig.

Es gibt kostenlose VPN-Dienste, die für eine gelegentliche Nutzung ausreichen können. Diese Dienste sind aber auch beliebte Angriffsziele für Hacker und Spammer.
Beispielsweise bietet der Hersteller AVM für die Fritzbox eine kostenlose Lösung an, die man auf dem WLAN-Router zu Hause einrichten kann (vgl. Arbeitsblatt 05, S. 1). Man reduziert aber die Geschwindigkeit auf die Bandbreite, die für den privaten Internetzugang zur Verfügung steht.
Werden regelmäßig öffentliche WLANS genutzt, ist es empfehlenswert, Beträge in der Größenordnung von 50 € pro Jahr für diesen Sicherheitszuwachs zu bezahlen. Ebenso bei der Nutzung von IoT-Geräten.
Bei der Auswahl eines VPN-Anbieters sollte man sorgfältig vorgehen, denn der gesamte Internetverkehr wird über einen Anbieter geleitet. Er erhält damit theoretisch Zugriff auf alle Daten, die gesendet werden. Hier liegt ein Vorteil bei der Lösung über den privaten WLAN-Router. Auch Verschlüsselungsverfahren und Protokolle sollten hinterfragt werden, denn hier zeigen sich Unterschiede (Stand: September 2017):

- Z. B. IPSec, OpenVPN, SSTP und L2TP verwenden SSL/TLS oder IPsec und gelten derzeit als sicher.
- PPTP beispielsweise ist zwar schnell, dafür aber nicht so sicher.
- Derzeit können für die Verschlüsselung folgende Einstellungen empfohlen werden:
  - Verschlüsselung mit AES–256
  - RSA–Schlüssel mit einer Länge von mindestens 2048 Bit, besser ECDSA (EC steht für Elliptic Curve)
  - Für die Hashfunktion SHA–2 (SHA–1 gilt als nicht mehr sicher, SHA–3 ist bereits spezifiziert)

  Zu beachten ist dabei, dass die Geschwindigkeit umso mehr absinkt, je stärker die Verschlüsselung ist. Man sollte auf jeden Fall immer wieder aktuelle Daten bei vertrauenswürdigen Quellen einholen.

A Bearbeite das Arbeitsblatt 06, S. 4–6

Ausblick: Wenn eines Tages Quantencomputer verfügbar sind, werden die bisherigen Sicherheitsstandards hinfällig. Bis dahin sollten dann aber neue kryptografische Verfahren verfügbar sein.