

Abteilung Gymnasium

Arbeitskreis Link-Ebene Wirtschaftsinformatik

Schellingstr. 155 · 80797 München · Tel.: 089 2170-2153 · Fax: -2125

E-Mail: tobias.tyll@isb.bayern.de

**WIn 10.3: Aufgabe „Wie schütze ich meinen Computer?“**

Häufig sind private Netzwerke aufgrund mangelnder Kenntnisse auf dem Gebiet der technischen Datensicherung durch Soft- und Hardware nur schlecht oder gar nicht gesichert. Die folgenden Aufgaben ermutigen die Jugendlichen, sich intensiv mit dem Thema auseinanderzusetzen, um gegebenenfalls auch zu Hause das Netzwerk und den Internetanschluss besser schützen zu können.

Ausgehend von der aktuellen Situation der Lernenden (Eintritt in die Qualifikationsstufe des Gymnasiums) werden verschiedene Möglichkeiten des Internetanschlusses erarbeitet. Im Folgenden wird die Gefahr eines schlecht gesicherten Internetzugangs anhand eines Zeitungsartikels problematisiert und die Schülerinnen und Schüler suchen Möglichkeiten, sichere Netzverbindungen aufzubauen. In den Aufgaben 3 und 4 erarbeiten die Jugendlichen die Funktionsweise und den Umgang mit einer Firewall.

Hinweis:

Tiefe und Umfang dieser Unterrichtssequenz übersteigen die im Lehrplan vorgesehene Stundenzahl, im Blick auf die Förderung der Informations- und Datenkompetenz im Rahmen der ökonomischen Verbraucherbildung erscheint diese Ausweitung gleichwohl gerechtfertigt.

Die Materialien eignen sich alternativ auch als Grundlage für ein Projekt (10.5).

**Wie schütze ich meinen Computer?**

Mit dem bevorstehenden Einstieg in die Qualifikationsstufe stellen Sie im Hinblick auf die Seminararbeit fest, dass Sie einen eigenen PC benötigen. Ihr Zimmer ist nicht in direkter Nähe zu einem Internetzugang, Ihre Eltern besitzen einen eigenen PC, der bereits über ein LAN-Kabel mit dem Internet verbunden ist.

**Aufgabe 1**

Informieren Sie sich über Möglichkeiten, wie Sie Ihren neuen PC an das häusliche Internet (DSL, Kabelnetz oder Satellitenverbindung) anschließen können und erstellen Sie eine beschreibende Übersicht!

**M 1**

Im Mai 2010 erschien in einer großen deutschen Zeitung ein Artikel über die Sicherung privater Drahtlosnetzwerke. Dort heißt es, dass Internet-Nutzer ihr eigenes WLAN mit einem Passwort sichern müssten, ansonsten drohe im Falle einer unbefugten Nutzung durch andere Personen eine Abmahnung in Höhe von 100 Euro. Dies sei einem Urteil des Bundesgerichtshofs (BGH) zu entnehmen, mit dem Unterlassungsansprüche der Musikindustrie gestärkt würden.

Laut der Bundesrichter habe aber der WLAN-Betreiber keine Verpflichtung zu Schadensersatzzahlungen. Zur Begründung hieß es, wenn sich Dritte in der Abwesenheit des Anschlussinhabers Zugang verschafften und unbefugt Musiktitel herunterladen würden, treffe den Inhaber kein Verschulden.

**Aufgabe 2**

Beschreiben Sie zunächst eine Situation, wie es einem Dritten möglich wäre, ein WLAN unbefugt zu nutzen!

Erklären Sie, was grundsätzlich mit einer Abmahnung in obigem Sinne (M 1) gemeint ist und welcher Unterschied zu Schadensersatzforderungen besteht! Finden Sie Beispiele, bei denen Sie von einer Abmahnung bedroht sein könnten!

Recherchieren Sie nach drei möglichen Maßnahmen der „individuellen Sicherung“ eines Drahtlosnetzwerkes und erstellen Sie eine Checkliste!

**M 3**

In Ihrem Router ist eine integrierte, externe Firewall vorhanden, der neue PC enthält eine „Personal Firewall“-Software. Die Firewall-Software dient dazu, den Netzwerkzugriff zu beschränken, basierend auf Absender- oder Zieladresse und genutzten Diensten. Sie überwacht den durch sie hindurch laufenden Datenverkehr und entscheidet anhand festgelegter Regeln, ob bestimmte Netzwerkpakete durchgelassen werden oder nicht. Auf diese Weise versucht sie, unerlaubte Netzwerkzugriffe zu unterbinden. Abhängig davon, wo die Firewall-Software installiert ist, wird unterschieden zwischen einer Personal Firewall (auch Desktop Firewall) und einer externen Firewall (auch Netzwerk- oder Hardware-Firewall genannt).

Sie sind sich nicht sicher, welches der beiden Produkte Sie aktivieren sollen. Im Internet finden Sie dazu zwei Abbildungen, welche die Wirkungsweisen einer externen und einer „Personal Firewall“-Software auf ihrem Rechner beschreiben sollen:

|  |  |
| --- | --- |
| Datei:Externe Firewall.jpg | Datei:Personal Firewall.jpg |

Quellen: http://de.wikipedia.org/w/index.php?title=Datei:Externe\_Firewall.jpg&filetimestamp=20101006072345 und http://de.wikipedia.org/w/index.php?title=Datei:Personal\_Firewall.jpg&filetimestamp=20100913193539; aufgerufen am 16.07.2012

**Aufgabe 3**

Beschreiben Sie anhand der Abbildungen (M 3) die Wirkungsweise der beiden Firewall-Systeme!

Finden Sie Argumente, warum die Firewall kein Anti-Viren-Programm ersetzen kann!

**M 4**

Ihre Firewall lässt sich so konfigurieren, dass bestimmte Ports freigegeben werden können. Doch was sind Ports und wieso sollten Sie Ports freigeben?

Tauschen Computer untereinander Daten aus, so werden unterschiedliche Datenströme durch Ports voneinander getrennt. Ein Port ist auch ein prozessspezifisches Softwarekonstrukt, das einen Kommunikationsendpunkt zur Verfügung stellt. Man kann sich einen Port also vorstellen wie eine Tür zwischen Rechner und Netzwerk.

Eine Portsperre ist das Sperren oder Drosseln eines bestimmten Portes bzw. des darauf zugreifenden Dienstes. Das Sperren von Ports wird von einigen Internet Service Providern eingesetzt, um unerwünschte Dienste zu blockieren. Bei Providern können Dienste beispielsweise unerwünscht sein, weil sie sehr viel Datenverkehr verursachen, wie beispielsweise beim Filesharing in Tauschbörsen. Aber auch Messenger nutzen bestimmte Ports für ein- und ausgehende Nachrichten.

Ports können auch mit einer Firewall gesperrt werden. Bei einer lokalen Firewall wird normalerweise andersherum vorgegangen: Nur die tatsächlich benötigten Ports werden freigegeben und alle anderen Ports bleiben gesperrt. Somit werden die Angriffspunkte auf das geschützte Netz bzw. den PC reduziert. Portscanner werden von Angreifern verwendet, um einen oder mehrere Zielrechner nach offenen Ports und damit möglichen Einfalltoren zu untersuchen.

**Aufgabe 4**

Anhand der auf der nächsten Seite folgenden Liste können Sie erkennen, welche bekannten Ports in ihrer Firewall möglicherweise geöffnet sein sollten. Recherchieren Sie Ihnen unbekannte Dienste im Internet und geben Sie eine Verwendungsbeschreibung an:

|  |  |  |
| --- | --- | --- |
| Port | Dienst | Beschreibung |
| 20 | [FTP-Data](http://de.wikipedia.org/wiki/File_Transfer_Protocol) | Dateitransfer (Datentransfer vom Server zum Client) |
| 21 | [FTP](http://de.wikipedia.org/wiki/File_Transfer_Protocol) | Dateitransfer (Initiierung der Session und Senden der FTP-Steuerbefehle durch den Client) |
| 25 | [SMTP](http://de.wikipedia.org/wiki/Simple_Mail_Transfer_Protocol) |  |
| 53 | [DNS](http://de.wikipedia.org/wiki/Domain_Name_System) |  |
| 67 | [DHCP](http://de.wikipedia.org/wiki/DHCP) |  |
| 80 | [HTTP](http://de.wikipedia.org/wiki/Hypertext_Transfer_Protocol) |  |
| 110 | [POP3](http://de.wikipedia.org/wiki/Post_Office_Protocol) |  |
| 143 | [IMAP](http://de.wikipedia.org/wiki/Internet_Message_Access_Protocol) |  |
| 443 | [HTTPS](http://de.wikipedia.org/wiki/Hypertext_Transfer_Protocol_Secure) |  |
| 843 | [Flash](http://de.wikipedia.org/wiki/Adobe_Flash) |  |
| 993 | [IMAPS](http://de.wikipedia.org/wiki/Internet_Message_Access_Protocol) (verschlüsselt) |  |
| 995 | [POP3S](http://de.wikipedia.org/wiki/Post_Office_Protocol) (verschlüsselt) |  |
| 1433 | [Microsoft SQL Server](http://de.wikipedia.org/wiki/Microsoft_SQL_Server) |  |
| 1723 | VPN |  |
| 3306 | [MySQL](http://de.wikipedia.org/wiki/MySQL) |  |
| 3389 | [Remote](http://de.wikipedia.org/wiki/Remote_Desktop_Protocol) Desktop |  |
| 5190 | [ICQ](http://de.wikipedia.org/wiki/ICQ) |  |
| 8080 | [alternativer HTTP Port](http://de.wikipedia.org/wiki/Hypertext_Transfer_Protocol) |  |

**Lösungsvorschlag zu Aufgabe 1**

|  |  |
| --- | --- |
| Infrastruktur | Erläuterung |
| Router / Switch / Modem | Der Switch bietet die Möglichkeit, mehrere Rechner gleichzeitig mit demselben Internetzugang zu betreiben. Die Aufgabe des Switches, der in einem Router integriert ist, ist es, die Kommunikation unter den Rechnern und die gemeinsame Internetnutzung zu regeln. Das ebenfalls im Router integrierte Modem verbindet das häusliche Netzwerk mit dem Einwahlknoten des Internetproviders. |
| LAN-Kabel | Die kabelgebundene Anschlusslösung zeichnet sich dadurch aus, dass ein Netzwerkkabel vom PC bis zum Router gelegt werden muss. An Türdurchlässen oder Bodenschwellen wird sich das Kabel schnell aufscheuern. Spezielle Flachbandlösungen sind eher kostspielig. |
| Drahtlosnetzwerk (WLAN) | Viele Router bieten gleichzeitig die Möglichkeit, ein Drahtlosnetzwerk zu betreiben. Dabei bildet der Router den drahtlosen Zugriffspunkt (Access­point) und der Rechner den Client, der sich am Accesspoint anmeldet. Je nach Netzwerkkarten und Router gibt es unterschiedliche Übertragungsgeschwindigkeiten, Reichweiten und Verschlüsselungsmethoden. |
| PowerLAN | PowerLAN, auch dLAN (direct LAN) oder Powerline Communication (PLC) genannt, bezeichnet eine Technik, die vorhandene Stromleitungen zum Aufbau eines Netzwerks zur Datenübertragung mit nutzt, so dass keine zusätzliche Verkabelung notwendig ist. Innerhalb der Stromverteilung sind die Daten frei zugänglich, daher ist auch hier eine Verschlüsselung angebracht. Je nach Netzwerkkarten und Router gibt es unterschiedliche Übertragungsgeschwindigkeiten, Reichweiten und Verschlüsselungsmethoden. Für PowerLAN wird ein spezieller Router benötigt. Die Verbindung von Steckdose zum PC oder Router erfolgt dann kabelgebunden |



PowerLAN-Adapter

Quelle: http://de.wikipedia.org/w/index.php?title=Datei:Devolo.JPG&filetimestamp=20060719150417, aufgerufen am 16.07.2012

**Lösungsvorschlag zu Aufgabe 2**

Eine unbefugte Nutzung des WLAN ist möglich, wenn sich zum Beispiel ein Laptop-Nutzer in der Reichweite des ungeschützten häuslichen Drahtlosnetzwerkes befindet. Dieser kann jederzeit nach solchen verfügbaren Netzwerken suchen und sich anmelden. Da die Reichweite eines WLANs auf wenige hundert Meter begrenzt ist, muss sich dieser Nutzer nahe beim Accesspoint aufhalten, zum Beispiel auf der Straße vor der Wohnung.

Die schriftliche Abmahnung hat die Funktion, Streitigkeiten auf direktem und kostengünstigem Weg ohne Einschaltung eines Gerichts beizulegen. Die Abmahnung im Urheberrecht muss eine Schilderung des beanstandeten Sachverhalts, einen damit verbundenen Hinweis auf einen Rechtsverstoß, eine Aufforderung zur Unterlassung innerhalb angemessener Frist und die Androhung rechtlicher Schritte enthalten. Üblicherweise ist der Abmahnung eine vorformulierte Unterlassungserklärung beigefügt. Diese Erklärung wirkt als Vertrag und erhält in der Regel eine hohe Vertragsstrafe, die im Wiederholungsfalle zu bezahlen ist. Der berechtigt Abgemahnte hat die Kosten der Abmahnung zu tragen, bei minderschweren Erstfällen im nichtgewerblichen Bereich gilt im Bereich des Urheberrechts eine Obergrenze der zu erstatteten Anwaltskosten von 100 Euro.

Mögliche Situationen sind in Bereich der Urheberrechtsverletzungen zu suchen, z. B. das Herunterladen oder Anbieten geschützter Musiktitel oder Filme und die Veröffentlichung von geschützten Bildern in sozialen Netzwerken oder der eigenen Homepage, ebenso die Benutzung fremder Werke in eigenen Arbeiten ohne sauberes Zitieren.

Checkliste zur Sicherung des eigenen Drahtlosnetzwerkes

|  |  |
| --- | --- |
| Methode | Erläuterung |
| SSID verbergen | Die Kennung des eigenen Drahtlosnetzwerkes ist die SSID (Service Set Identifier), die frei wählbar ist. Um sich bei einem drahtlosen Netzwerk anzumelden, muss die SSID bekannt sein. |
| Verschlüsselung | Eine möglichst hohe Verschlüsselungstechnologie (WPA2) verwenden. Damit ist ein Zugriff nur bei bekanntem Netzwerkschlüsselwort möglich und der Datenverkehr kann nicht abgehört werden. Der Schlüssel sollte möglichst lang sein und eine breite Zeichenstreuung beinhalten. |
| MAC-Filterung | Ein MAC-Filter ist ein Netzwerk-Zugangsschutz, der nur Geräten mit bestimmter MAC-Adresse (eindeutige Hardwareadresse) Zugang zum Netzwerk gestattet. Typischerweise wird ein MAC-Filter in einem LAN oder WLAN angewendet und in Form einer Tabelle im Router (Firewall) abgelegt. Somit dürfen sich am Router nur bereits bekannte Netzwerkkarten anmelden. Zwar lassen sich MAC-Adressen manipulieren, dennoch stellt der MAC-Filter eine weitere Hürde für unbefugte Nutzer dar. |

**Lösungsvorschlag zu Aufgabe 3**

Eine externe Firewall (auch Netzwerk- oder Hardware-Firewall genannt) beschränkt die Verbindung zwischen zwei Netzen. Das könnten beispielsweise ein Heimnetzwerk und das Internet sein.

Sie kann dank der physischen Trennung zu dem zu schützenden Computersystem nicht so einfach manipuliert werden. Die externe Firewall ist dafür prädestiniert, unerlaubte Zugriffe von außen (in der Abbildung das WAN) auf das interne System zu unterbinden. Im Unterschied zur Personal Firewall besteht das interne System hier nicht zwangsläufig aus nur einem einzigen Computer, sondern kann sich auf einen Verbund mehrerer Computer beziehen, die das interne Netz (LAN) bilden und die alle gleichermaßen geschützt werden.

Als Personal Firewall oder Desktop Firewall wird eine lokal auf dem Computer installierte Firewall-Software bezeichnet. Zu ihrer Aufgabe gehört es, ungewollte Zugriffe von außen auf Netzwerkdienste des Computers zu unterbinden. Abhängig vom Produkt kann sie zudem versuchen, Anwendungen davon abzuhalten, ohne das Einverständnis des Anwenders mit der Außenwelt zu kommunizieren. Die Personal Firewall filtert zusätzlich auch die Verbindungen des PCs von und zu dem privaten lokalen Netz.

Durch Überwachung des Netzwerkverkehrs kann die Firewall zwar verhindern, dass Würmer selbständig vom Internet auf Netzwerkdienste des Rechners zugreifen. Sie unterscheidet aber nicht zwischen Schadprogrammen und vom Nutzer gewünschte Zugriffe. Sie kann lediglich erkennen, ob ein Datenpaket von außen ein aus dem Netzwerk angefordertes Antwortpaket ist. Anti-Viren-Software erkennt Schadprogramme anhand von Virendefinitionsdateien und typischem Programmcode und blockiert deren Ausführung.

**Lösungsvorschlag zu Aufgabe 4**

|  |  |  |
| --- | --- | --- |
| Port | Dienst | Beschreibung |
| 20 | [FTP-Data](http://de.wikipedia.org/wiki/File_Transfer_Protocol) | Dateitransfer (Datentransfer vom Server zum Client) |
| 21 | [FTP](http://de.wikipedia.org/wiki/File_Transfer_Protocol) | Dateitransfer (Initiierung der Session und Senden der FTP-Steuerbefehle durch den Client) |
| 25 | [SMTP](http://de.wikipedia.org/wiki/Simple_Mail_Transfer_Protocol) | [E-Mail](http://de.wikipedia.org/wiki/E-Mail)-Versand |
| 53 | [DNS](http://de.wikipedia.org/wiki/Domain_Name_System) | Auflösung von Domainnamen in [IP-Adressen](http://de.wikipedia.org/wiki/IP-Adresse) |
| 67 | [DHCP](http://de.wikipedia.org/wiki/DHCP) | Zuweisung der Netzwerkkonfiguration an Clients |
| 80 | [HTTP](http://de.wikipedia.org/wiki/Hypertext_Transfer_Protocol) | [Webserver](http://de.wikipedia.org/wiki/Webserver) |
| 110 | [POP3](http://de.wikipedia.org/wiki/Post_Office_Protocol) | [Client](http://de.wikipedia.org/wiki/Client)-Zugriff für [E-Mail-Server](http://de.wikipedia.org/wiki/E-Mail-Server) |
| 143 | [IMAP](http://de.wikipedia.org/wiki/Internet_Message_Access_Protocol) | Client-Zugriff für E-Mail-Server |
| 443 | [HTTPS](http://de.wikipedia.org/wiki/Hypertext_Transfer_Protocol_Secure) | sicherer Webserver (via [SSL](http://de.wikipedia.org/wiki/Transport_Layer_Security) verschlüsselt) |
| 843 | [Flash](http://de.wikipedia.org/wiki/Adobe_Flash) | Datenaustausch von Flashprogrammen via [ActionScript](http://de.wikipedia.org/wiki/ActionScript) |
| 993 | [IMAPS](http://de.wikipedia.org/wiki/Internet_Message_Access_Protocol) (verschlüsselt) | sicherer [Client](http://de.wikipedia.org/wiki/Client)-Zugriff für [E-Mail-Server](http://de.wikipedia.org/wiki/E-Mail-Server)  |
| 995 | [POP3S](http://de.wikipedia.org/wiki/Post_Office_Protocol) (verschlüsselt) | sicherer Client-Zugriff für E-Mail-Server |
| 1433 | [Microsoft SQL Server](http://de.wikipedia.org/wiki/Microsoft_SQL_Server) | Zugriff auf SQL-Server-Datenbanken |
| 1723 | VPN | Aufbau von [VPN](http://de.wikipedia.org/wiki/Virtual_Private_Network)-Verbindungen |
| 3306 | [MySQL](http://de.wikipedia.org/wiki/MySQL) | Zugriff auf MySQL-Datenbanken |
| 3389 | [Remote](http://de.wikipedia.org/wiki/Remote_Desktop_Protocol) Desktop | Windows Remotedesktopzugriff, Windows Terminal Services |
| 5190 | [ICQ](http://de.wikipedia.org/wiki/ICQ) | Instant-Messaging-Programm ICQ |
| 8080 | [alternativer HTTP Port](http://de.wikipedia.org/wiki/Hypertext_Transfer_Protocol) | [Webserver](http://de.wikipedia.org/wiki/Webserver) (Standardport bei [Apache Tomcat](http://de.wikipedia.org/wiki/Apache_Tomcat)) |